AN A.S. PRATT PUBLICATION
OCTOBER 2019
VOL. 5 • NO. 8

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 5 | NUMBER 8 | OCTOBER 2019

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [5] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [245] (LexisNexis A.S. Pratt)

An A.S. Pratt™ Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2019–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquiries and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 646.539.8300. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report,* LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

European Commission Q&A on the Interplay Between the Clinical Trials Regulation and GDPR

Ronan Tigner and Alex van der Wolk*

The European Commission has issued questions and answers on the interplay between the Clinical Trials Regulation and the General Data Protection Regulation. The authors of this article explain the Q&A, which offers some additional clarifications for data processing within clinical trials, but falls short in other respects.

In response to the opinion of European Data Protection Board ("EDPB"), the European Commission has issued question and answers on the interplay between the Clinical Trials Regulation ("CTR") and the General Data Protection Regulation ("GDPR") ("Q&A").[1] The non-binding Q&A offers some additional clarifications for data processing within clinical trials. However, the Q&A also falls short in other respects. In particular, it omits some core issues, deferring to national data protection authorities instead.

KEY TAKEAWAYS

The Q&A aligns with the opinion that the EDPB issued on the Q&A ahead of its publication on:

- *The legal justification within clinical trials and deterrent on using consent* – Under the GDPR, the processing of personal data must be tied to one of the legal justifications/derogations (for sensitive data such as health data) listed in the GDPR. One of those justifications/derogations is consent, but there are also others, such as public interest or scientific research. In parallel, EU clinical trial rules generally require that clinical trial participants provide their informed consent to participate in a clinical trial.

  The Q&A confirms that consent *under the GDPR* (protecting privacy) should be distinguished from *clinical trial* informed consent (protecting ethics), and that *consent is generally not the appropriate justification* under the GDPR.

* Ronan Tigner is an associate at Morrison & Foerster LLP focusing his practice on a broad range of privacy and data security matters. Alex van der Wolk is a partner at the firm and the co-chair of its Global Privacy & Data Security Practice advising companies on data protection strategy and compliance governing all aspects of information management. The authors may be reached at rtigner@mofo.com and avanderwolk@mofo.com, respectively.

[1] https://ec.europa.eu/health/sites/health/files/files/documents/qa_clinicaltrials_gdpr_en.pdf.

- This is the case in particular, given the potential imbalance of power between participants and clinical trial investigators (so that consent would not be freely given) and because if a participant withdraws consent, personal data collected prior to the withdrawal may have to be deleted, which can lead to a host of issues, and threaten the quality and credibility of the clinical trial.
- As a result, the Q&A recommends other legal justifications than consent, which it allocates depending on some core activities identified within clinical trials, namely "reliability and safety purposes" and "research activities" as the EDPB had suggested (see the table below). As we identified in our previous alert, while clarifying the absence of the need for consent under the GDPR is helpful, it can also cause tension where local privacy laws prescribe consent for reliance on scientific research,[2] as in Ireland[3] or the Netherlands.[4]

- *Secondary use* – The Q&A also confirms the existence of a "presumption of compatibility" under the GDPR for further scientific research outside the study protocol. Within clinical trials, a "protocol" must be drafted to describe the clinical trial objectives among other details. Those objectives are then built into clinical trial documentation that is provided to the participants. That said, clinical trials may last several years and discoveries may prompt the need for research beyond the protocol. Under clinical trial rules, such prolonged use is allowed[5] under certain conditions. The question therefore arises as to whether such prolonged use is also possible under the GDPR without having to obtain a new legal justification (or whether, conversely, a separate justification is required, which may require taking additional steps, such as re-notice/re-consent with individuals). The EDPB confirms that it is possible to rely on the initial justification for the scientific research also for the prolonged use. It should be noted, however, that secondary use is a complex issue under the GDPR, and that the EDPB already announced, in its opinion, that it will devote further attention and guidance to it in the future. There will, therefore, be additional considerations to look out for in the future.

[2] Although one could argue in that case that the GDPR's legal basis is scientific research and additional consent is being sought only as a safeguard under GDPR Art. 89(1), and not as standalone GDPR consent.

[3] Section 3.e of the Data Protection Act 2018 (Section 36(2)) (Health Research) Regulations 2018, *available at* http://www.irishstatutebook.ie/eli/2018/si/314/made/en/pdf.

[4] Article 24.c of the Dutch Data Protection Act, *available at* https://wetten.overheid.nl/BWBR0040940/2018-05-25.

[5] CTR Art. 28.2.

The Q&A also provides some additional insights, for example:

- *Withdrawal of consent* – Where privacy consent is nevertheless used as a legal basis for processing data (alongside clinical trial consent), and a participant withdraws consent, it is up to the investigator to determine whether the withdrawal relates only to participation in the clinical trial or also to the processing of personal data. In other words, there is no automatic withdrawal of both consents. It is therefore useful to clearly split out the requests for privacy and clinical trial consent in participant documentation (e.g., separate document or section in the Informed Consent Forms), so as not to conflate both consents and risk losing the possibility of arguing that a participant only withdrew from the trial but not also from the processing of personal data (which as explained, may entail deleting the personal data).
- *Transfers* – When it comes to cross-border transfers, the Q&A indicates that companies may "*adopt the approach that is most suitable for their specific* situation," which suggests there is no prescribed or favored transfer mechanism. The Q&A also explicitly mentions "public interest" as a transfer mechanism, which aligns with the legal basis for reliability and safety (see the Table below) and may prove useful (e.g., for reporting to foreign public authorities where the public interest is shared between the EU and the foreign country's legislation).

WHERE THE Q&A FALLS SHORT

- *Limited scope* – There are a number of core issues which the EDPB opinion did not address and that unfortunately are also not clarified by the Q&A. For example, it is known that there are local disparities amongst EU Member States as to what the qualifications of the investigator and the sponsor should be (e.g., joint controllers, independent controllers, or investigator as processor and sponsor as controller). The Q&A would have been a good opportunity for the European Commission to promote a harmonized approach, but the Q&A remains silent about this issue. Likewise, it is not clear how the territorial criteria of the GDPR apply to foreign-sponsored trials (e.g., where a non-EU sponsor uses an EU-based investigator to run a clinical trial using personal data from EU individuals). The Q&A only restates the general criteria for GDPR applicability without specifically clarifying them in the context of clinical trials and recommends that companies consult with data protection authorities for further details (which means that consistency should be promoted at the EDPB level).
- *Consent for ongoing trials* – The Q&A also states that if privacy consent is requested from participants under the predecessor to the Clinical Trial Directive (Directive 2001/20), this legal basis cannot be changed into another legal basis (see question 11 of the Q&A) (and that if consent for ongoing trials does

not meet the GDPR threshold, re-consent may be required). This interpretation seems to depart from guidance[6] provided by the Article 29 Working Party and endorsed by the EDPB regarding consent that suggested that controllers may, as a one-off situation, be able to make the transition to another GDPR-compliant legal basis.

CONCLUSION

Although the European Commission's Q&A offers some clarifications on personal data processing within clinical trials, especially in confirming that consent is not the appropriate justification for processing personal data, it nevertheless omits some core issues for which guidance would be useful. As a result, disparities are likely to remain and should be taken into account when implementing a clinical trial across various EU jurisdictions (e.g., additional time will be necessary to negotiate and adapt local agreements and notices). The EDPB intends to opine further on the issue of secondary use, and this may be an opportunity to advocate for further consistency for other issues. Finally, for additional details, see the table showing the GDPR legal bases in the Q&A below.

Processing	Legal Basis (GDPR Art. 6)	Derogation (GDPR Art. 9)
Reliability and Safety (safety, disclosures, archiving)	Legal obligation (6.1(c))	Public interest in the area of health (9.2(i))
Research Activities	Consent (6.1(a)) (*under specific circumstances*)	Explicit consent (9.2(a)) (*under specific circumstances*)
	Public interest (6.1(e))	Public interest in the area of health (9.2(i))
		Scientific research (9.2(j))
	Legitimate interest (6.1(f)) (*if public interest does not work*)	Scientific research (9.2(j))
Emergencies (new compared to EDPB opinion)	Vital interests (6.1(c))	Vital interests (9.2(c))

[6] https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51030.