AN A.S. PRATT PUBLICATION
NOVEMBER – DECEMBER 2017
VOL. 3 • NO. 9

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 3 NUMBER 9 NOVEMBER/DECEMBER 2017

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*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [303] (LexisNexis A.S. Pratt)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

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

(2017–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. Copyright 2017 Reed Elsevier Properties SA, used under license by Matthew Bender & Company, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires 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, 718.224.2258. 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.

GDPR Contracts and Liabilities Between Controllers and Processors

By Joshua Gray [*]

This article summarizes the key aspects of the UK's Information Commissioner's recently published draft guidance on General Data Protection Regulation contracts and liabilities on contracts between controllers and processors under the Regulation.

The Information Commissioner's Office ("ICO") recently published draft guidance[1]on General Data Protection Regulation ("GDPR") contracts and liabilities on contracts between controllers and processors under the GDPR (the "Guidance"). The ICO consulted on the Guidance until October 10. The article summarizes the key aspects of the Guidance.

GDPR CONTRACTS

Under the GDPR, whenever a controller uses a processor it needs to have a written contract in place. This is important so the parties understand their responsibilities and liabilities. The mandatory requirements of the data processing agreements are set out in Article 28 of the GDPR. The requirements under the GDPR build upon the general requirements under the Data Protection Directive that (i) a processor act only upon a controller's instructions and (ii) to take appropriate measures to keep the personal data secure. Any contracts in place on May 25, 2018 must meet the new GDPR requirements, and the ICO recommends that existing contracts and template terms are reviewed and amended to comply with the GDPR.

The key requirements of the GDPR in respect of data processing terms are:

- to have a written contract in place when appointing a processor (whether as a controller or a processor appointing a sub-processor);
- the contract must set out:
    - the subject matter and duration of the processing;
    - the nature and purpose of the processing;
    - the type of personal data and categories of data subject; and
    - the obligations and rights of the controller.
- the contract must contain the following minimum terms, requiring the processor to:

[*] Joshua Gray is a technology and IP transactions lawyer in the London office of Covington & Burling LLP. He may be contacted at jgray@cov.com.

[1] https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf.

  - only act on the written instructions of the controller;
  - ensure that people processing the data are subject to a duty of confidence;
  - take appropriate measures to ensure the security of processing;
  - only engage sub-processors with the prior consent of the controller and under a written contract;
  - assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
  - assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
  - delete or return all personal data to the controller as requested at the end of the contract; and
  - submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a Member State.

Much of the ICO's guidance on the above mirrors the GDPR itself, controllers and processors should note the following matters from the ICO:

- The ICO recommends setting specific details of processing as listed in the second bulled above, noting that controllers need to be very clear from the outset and cannot rely upon general catch-all terms. This approach could be seen to be somewhat heavy handed, particularly if the nature of the processing is self-evident from the nature of the services.
- A processor's obligation to keep personal data confidential extends to all employees, temporary workers and agency workers.
- The processor's obligations to ensure adequate security under Article 32 of the GDPR will be subject to separate guidance on security matters, and for now the ICO's existing guidance under the Data Protection Act is sufficient.
- A processor's obligations to assist the controller under Article 28(3)(f) are "not infinite" and are limited by taking into account the nature of the processing and information available to the processor.

The ICO does not provide any material guidance on the following matters which are often contentious during the negotiation of GDPR-compliant data-processing terms:

- How should a right to object to a change in subcontractors manifest? Termination?
- Is it possible to limit a controller's right to audit a data processor? What pragmatic controls may be used by a processor to comply with this requirement (e.g. limiting the duration and scope of audits, whether third party certifications are a

permissible substitute for third party certifications and so on). The Guidance appears to suggest that the processor may be able to provide information or submit to audits to satisfy the requirements under Article 28(3)(h).

The GDPR allows the use of standard contractual clauses for data processing issued by the European Commission or a Supervisory Authority (such as the ICO), although none have been issued as yet.

CONTROLLER RESPONSIBILITIES AND LIABILITIES

Under the GDPR, controllers may only use processors who provide sufficient guarantees that they will meet the requirements of the GDPR — with such guarantees typically being put in place by way of a contract. An approved code of conduct or certification scheme may also be available to help a controller demonstrate that it has chosen a processor who provides sufficient guarantees to process the person's data in accordance with the GDPR, although again, no such schemes have been approved so far.

The Guidance notes that controllers are ultimately responsible for ensuring that personal data is processed in accordance with the GDPR. Unless a controller can demonstrate that it is "not in any way responsible for the event giving rise to the damage" it will be fully liable for any damage caused by non-compliant processing to ensure a data subject receives effective compensation.

Again, the Guidance avoids some of the more challenging aspects of implementing risk allocation provisions relating to joint and several liability under the GDPR such as:

- Whether limitations and exclusions of liability could operate to prevent a party "claiming back" losses under the joint and several liability regime.
- What control of defense and related provisions may be permissible under the GDPR?

PROCESSOR RESPONSIBILITIES AND LIABILITIES

The Guidance provides a helpful summary of processors' responsibilities and liabilities in their own right:

- A processor must only act on the documented instructions of a controller.
- If a processor determines the purpose and means of processing (rather than acting only on the instructions of the controller) then it will be considered to be a controller and will have the same liability as a controller.
- In addition to its contractual obligations to the controller, under the GDPR a processor also has the following direct responsibilities:

  - not to use a sub-processor without the prior written authorization of the data controller;
  - to co-operate with supervisory authorities (such as the ICO);
  - to ensure the security of its processing;
  - to keep records of processing activities;
  - to notify any personal data breaches to the data controller;
  - to employ a data protection officer; and
  - to appoint (in writing) a representative within the European Union if needed.
- If a processor fails to meet any of these obligations, or acts outside or against the instructions of the controller, then it may be liable to pay damages in legal proceedings, or be subject to fines or other penalties or corrective measures.
- If a processor uses a sub-processor then it will, as the original processor, remain directly liable to the controller for the performance of the sub-processor's obligations.

On contract liabilities, the ICO notes that:

- Contracts could specify indemnities in respect of data processing and that professional advice should be obtained on this point.
- Under contract a processor may be directly liable for any failure to meet the terms of the relevant agreement with a controller.
- Where a sub-processor is used, there are potentially three parties liable under the GDPR toward a data subject (controller, processor and sub-processor).

While the above is a helpful start, data controllers and processors need to assess how the data processing terms fit within the wider risk allocation framework in their agreement including representations, warranties, indemnities, limitations, and exclusions of liability and insurance.