

AN A.S. PRATT PUBLICATION

OCTOBER 2018

VOL. 4 • NO. 8

PRATT'S
**PRIVACY &
CYBERSECURITY
LAW
REPORT**



EDITOR'S NOTE: INTERSECTING REGULATIONS

Victoria Prussen Spears

SWEEPING CALIFORNIA CONSUMER PRIVACY PROTECTION ACT REACHES UNSUSPECTING BUSINESSES AND REQUIRES PROMPT FOCUS

To-Quyen Truong

EU-REGULATED COMPANIES FACED WITH PERSONAL DATA BREACH - RECONCILING OBLIGATIONS UNDER GDPR AND MAR

Jan-Frederik Keustermans, Frederic Peeters, Natascha Gerlach, Géraldine Bourguignon, and Laurent Legein

CCPs AS THIRD PARTY SERVICE PROVIDERS: BREACH NOTIFICATION ISSUES

Douglas Landy, John Williams, Nicholas Smith, Joel Harrison, and James Kong

BEST PRACTICES TO DETECT AND PREVENT FILE-LESS AND CLICK-LESS MALWARE

Fob H. James

Pratt's Privacy & Cybersecurity Law Report

VOLUME 4

NUMBER 8

OCTOBER 2018

Editor's Note: Intersecting Regulations

Victoria Prussen Spears

247

**Sweeping California Consumer Privacy Protection Act Reaches Unsuspecting
Businesses and Requires Prompt Focus**

To-Quyen Truong

249

**EU-Regulated Companies Faced with Personal Data Breach – Reconciling
Obligations Under GDPR and MAR**

Jan-Frederik Keustermans, Frederic Peeters, Natascha Gerlach,
Géraldine Bourguignon, and Laurent Legein

261

CCPs as Third Party Service Providers: Breach Notification Issues

Douglas Landy, John Williams, Nicholas Smith,
Joel Harrison, and James Kong

269

Best Practices to Detect and Prevent File-Less and Click-Less Malware

Fob H. James

276

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*, [4] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [247] (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.

LexisNexis and the Knowledge Burst logo are registered trademarks of Reed Elsevier Properties Inc., used under license. A.S. Pratt is a trademark of Reed Elsevier Properties SA, used under license.

Copyright © 2018 Reed Elsevier Properties SA, used under license by Matthew Bender & Company, Inc. All Rights Reserved.

No copyright is claimed by LexisNexis, Matthew Bender & Company, Inc., or Reed Elsevier Properties SA, in the text of statutes, regulations, and excerpts from court opinions quoted within this work. Permission to copy material may be licensed for a fee from the Copyright Clearance Center, 222 Rosewood Drive, Danvers, Mass. 01923, telephone (978) 750-8400.

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

(2018-Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

EDITOR-IN-CHIEF

STEVEN A. MEYEROWITZ

President, Meyerowitz Communications Inc.

EDITOR

VICTORIA PRUSSEN SPEARS

Senior Vice President, Meyerowitz Communications Inc.

BOARD OF EDITORS

EMILIO W. CIVIDANES

Partner, Venable LLP

CHRISTOPHER G. CWALINA

Partner, Holland & Knight LLP

RICHARD D. HARRIS

Partner, Day Pitney LLP

DAVID C. LASHWAY

Partner, Baker & McKenzie LLP

CRAIG A. NEWMAN

Partner, Patterson Belknap Webb & Tyler LLP

ALAN CHARLES RAUL

Partner, Sidley Austin LLP

RANDI SINGER

Partner, Weil, Gotshal & Manges LLP

JOHN P. TOMASZEWSKI

Senior Counsel, Seyfarth Shaw LLP

TODD G. VARE

Partner, Barnes & Thornburg LLP

THOMAS F. ZYCH

Partner, Thompson Hine

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 2018 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, 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.

EU-Regulated Companies Faced with Personal Data Breach – Reconciling Obligations Under GDPR and MAR

*Jan-Frederik Keustermans, Frederic Peeters, Natascha Gerlach,
Géraldine Bourguignon, and Laurent Legein**

Although there are no insurmountable conflicts between the General Data Protection Regulation and the Market Abuse Regulation, ensuring compliance with both regulations in the often tense circumstances and short time span between the internal discovery of a mass data breach and its disclosure to the public can be challenging and will require proper coordination among all actors involved within the company's organizational structure. The authors of this article discuss the obligations under both regulations.

Personal data breaches at EU-regulated issuers can lead to an interesting interplay between the disclosure obligations under the General Data Protection Regulation (“GDPR”) and the Market Abuse Regulation (“MAR”). Both regulations share a few common characteristics, at least formally: they are new binding rules leaving no room for national implementation, mainly codify prior rules but increase accountability and sanctions, are extremely detailed and are further supplemented by implementing measures as well as guidance from the European administrative authorities. But on substance, each follows its own imperatives: where MAR principally requires immediate disclosure to the public of inside information and prohibits selective disclosure of such information, GDPR focuses in the context of a personal data breach on the obligation to notify the competent data protection authority and subsequent or coinciding notifications specifically targeted at the affected individuals, preferably before the data breach becomes public knowledge. Therefore, even though there is no insurmountable conflict between the two regulations, ensuring compliance with both in the often tense circumstances and short time span between the internal discovery of a mass data breach and its disclosure to the public can be challenging and will require proper coordination among all actors involved within the company's organizational structure.

* Jan-Frederik Keustermans (jkeustermans@cgsh.com) and Frederic Peeters (fpeeters@cgsh.com) are associates at Cleary Gottlieb Steen & Hamilton LLP focusing on corporate and financial transactions. Natascha Gerlach (ngerlach@cgsh.com) is a senior attorney at the firm practicing in the areas of electronic discovery and European data protection law. Géraldine Bourguignon (gbourguignon@cgsh.com) is counsel at the firm concentrating on corporate law, capital markets, financial regulation, and litigation. Laurent Legein (llegein@cgsh.com), a partner at the firm, concentrates his practice in mergers and acquisitions, private equity, and equity capital markets transactions.

WHERE MAR AND GDPR INTERSECT

High profile personal data breaches are increasingly dominating the business news cycle. Well-known examples include Facebook's current data crisis, the 2017 data breach at Equifax and recent breaches at Uber and Yahoo. In that context, companies across the globe are faced with mounting cyber security threats and a heightened risk of public backlash when information about data breaches is made public.

For listed issuers in particular, the timing and content of any public communication about a (suspected) personal data breach can have a significant impact on the trading price of the issuer's securities.¹ This is especially the case for issuers with a specific business interest in personal data (such as online search engines or social network providers) or with reputational risks due to the sensitivity of personal data (such as financial institutions, credit reporting agencies or companies handling health care data).²

Regulators have also taken notice and have been increasingly scrutinizing the issue. In the United States, public prosecutors have already gone after companies allegedly trying to cover up data breaches (or purposefully delaying their disclosure to the public) and criminal charges for alleged insider trading in violation of federal securities laws were recently brought against a former Equifax executive who is alleged to have traded in Equifax securities using information pertaining directly to a data breach that was at the time not yet known to the public.

In the European Union, it is at this juncture, between the potential privacy implications of personal data breaches and the insider trading risks they may entail when listed issuers are involved, that an interesting interplay exists between market abuse rules (regulated in the EU by MAR and its implementing legislation) and data protection rules (primarily regulated in the EU, as from May 25, 2018, by the GDPR).

Just like MAR compliance is a key area of focus for any EU-listed issuer subject to its rules, data breach management should be a priority in the area of GDPR compliance for any company active in Europe that is processing significant amounts of personal data.

¹ For example, Facebook's share price fell by almost seven percent on March 19, 2018 (the biggest one-day drop in Facebook's share price since March 2014) in relation to the disclosure to the public of Cambridge Analytica's apparent unsanctioned access to personal data of about 50 million Facebook users (this estimate was subsequently revised to 87 million Facebook users).

² Personal data breach reporting and notification requirements also exist under sector specific European legislation, such as the eIDAS Regulation (EU) 910/2014, the Payment Services Directive (EU) 2015/2366 and the Network and Information Security Directive (EU) 2016/1148 (NISD). GDPR expands on these existing sector specific requirements and similar recommendations.

MAR's DISCLOSURE REQUIREMENTS

Scope of Application

The disclosure requirements under MAR generally apply to companies with debt, equity or other securities admitted to trading on EU regulated markets or multilateral trading facilities or for which a request for admission to trading has been made, or traded on an EU organized trading facility.³

Inside Information?

Under MAR, EU-listed issuers are under an obligation to disclose to the public as soon as possible any inside information which directly concerns them (*i.e.*, non-public information of a *precise* nature, relating directly or indirectly to the issuer or its securities, which, if disclosed, would be likely to have a *significant effect* on the price of the issuer's securities).⁴ Although assessing when inside information arises is fact-driven and issuer-specific, information about a serious data breach may significantly impact the share price, in particular of issuers with a data driven business model.

Listed issuers will need to assess carefully whether and when inside information arises, mostly focusing on the "precise nature" and "price sensitivity" of the data breach. Considering the increasing importance of data across industries, serious data breaches involving personal data will often qualify as "inside information." The fact that a company having suffered a security breach has not yet been able to map the full extent and scale of the breach does not necessarily mean that there is no inside information.⁵

However, if and when disclosure is made, it must be done in a manner "*which enables fast access and complete, correct and timely assessment of the information by the public*" as required by Article 17(1) MAR. In the context of a data breach, the requirement to disseminate complete and correct information will need to be carefully balanced against the possible remaining uncertainties about the scope and nature of the breach at the time of disclosure and possible adverse effects for affected individuals in case of a publication of too many specificities of the breach.

Possible Deferral?

An EU-listed issuer may, under MAR, decide to defer the disclosure of inside information provided that (i) the immediate disclosure is likely to prejudice its legitimate interests, (ii) the deferral is not likely to mislead the public, and (iii) confidentiality can be ensured.⁶ In many cases, immediate public disclosure of a mass data

³ Article 2 MAR.

⁴ Article 17(1) MAR.

⁵ In light of the *Geltl* judgement, a mere "realistic prospect" that a set of circumstances may come into existence, or that an event may occur, is enough (ECJ, June 28, 2012 (*Geltl v. Daimler*), C-19/11).

⁶ Article 17(4) MAR; See ESMA Guidelines of October 20, 2016.

breach will be likely to prejudice the issuer's legitimate interests, not only by hampering its ability to map the scale of a data breach, identify the nature, sensitivity and volume of the affected personal data and the number of affected individuals, but also by prejudicing its ability to take effective measures to contain the breach and prevent further breaches and dissemination of the affected personal data. Whether the deferral is likely to mislead the public will depend on the relevant facts and circumstances. If there have been rumors in the press about a possible data breach or statements by the CEO regarding the robustness of the company's security systems, these circumstances may be relevant factors to consider in determining whether deferral would be likely to mislead the public. In such case the confidentiality may also be compromised.⁷ Whether confidentiality can be ensured will also partly depend on the notification obligations under GDPR.

Selective Disclosure?

If disclosure is deferred, any further selective disclosure of the information is prohibited, except within the normal course of professional duties and always subject to a (contractual or legal) confidentiality obligation.⁸ The issuer must be able to ensure the confidentiality of the relevant information at all times. If confidentiality can no longer be ensured, Article 17(7) MAR requires immediate public disclosure.

GDPR's NOTIFICATION REQUIREMENTS

Scope of Application

GDPR applies to the processing of personal data either (i) in the context of the activities of a company's establishment in the EU (or in a place where EU law applies by virtue of public international law), regardless of whether the processing takes place in the EU or not and (ii) to any company that is not established in the EU, if the personal data processed relates to data subjects in the EU and where the processing activities relate to the offering of goods or services to those data subjects or to the monitoring of their behavior (where the behavior takes place within the EU).⁹ The definition of personal data applied by GDPR is extremely broad.¹⁰

Personal Data Breach?

GDPR defines a personal data breach quite broadly as "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.*"¹¹

⁷ Article 17(7) MAR.

⁸ See Articles 10(1) and 17(8) MAR.

⁹ Article 3 GDPR.

¹⁰ Article 4(1) GDPR.

¹¹ Article 4(12) GDPR.

Prompt DPA Notification

Article 33(1) GDPR requires a company subject to GDPR to notify a personal data breach to the competent national data protection authority (“DPA”) without undue delay (if feasible within 72 hours), unless the breach “*is unlikely to result in a risk to the rights and freedoms of natural persons.*”

Prompt notification is the default rule and companies need to be able to explain and justify any decision to delay notification beyond the initial 72 hours. A company having suffered the security breach must therefore assess risks for the affected individuals in a very short timeframe while taking into account complex factors such as the nature, sensitivity and volume of data affected and the number of affected individuals.

Mass data breaches resembling the ones that were front page news recently will almost always pose a risk for individuals, thus requiring notification to the DPA.

Notification to Affected Individuals

When a data breach is likely to result in a *high* risk to the rights and freedoms of natural persons, the company must also notify the affected individuals without undue delay.¹² The threshold for notification to individuals is therefore higher than that for a notification to the DPA. The DPA will in many cases be able to assist in assessing whether a notification to the individuals is necessary.

The individual notifications must be done in “*clear and plain language*”¹³ and must ensure that those notified understand the scope and significance of the breach and are informed about ways to protect their personal data from further unauthorized use.

If a high risk is identified, a company may forego directly notifying the affected individuals only if:

- (i) it implements or had already implemented appropriate technical and organizational protection measures (such as data encryption using state of the art algorithms) to ensure that affected personal data is protected and the risk for individuals is unlikely to materialize in practice,
- (ii) it has taken steps immediately following the breach effectively extinguishing the high risk, or
- (iii) notifying the affected individuals would involve a “*disproportionate effort*” by the company.

¹² Article 34(1) GDPR.

¹³ Article 34(2) GDPR.

In the latter situation, the company must however still issue a public statement (or take other equivalent measures) to ensure the affected individuals are made aware of the breach.¹⁴

In exceptional circumstances, it may even be necessary to notify the affected individuals before the competent DPA can be notified, for instance where an imminent threat of identity theft has been identified.

PRACTICAL GUIDANCE TO ENSURE COMPLIANCE

Ensuring compliance with MAR and GDPR when an EU-listed issuer is faced with a significant personal data breach that also gives rise to inside information requires a carefully managed communication process that must be timed and coordinated diligently between different actors within the issuer's organizational structure. The company's management, general counsel, data protection officer, and investor relations department will need to be attuned to their respective roles and responsibilities, and to coordinate with each other in developing an appropriate plan of action. A company's data incident response plan should ensure that the appropriate steps are taken to facilitate this coordination.

MAR and GDPR rules both require the company to assess any situation taking into account all specific factual circumstances of the case, and there is therefore no one-size-fits-all solution. But certain general considerations will likely be relevant in most situations.

- First, when a company becomes aware of a data breach, it must immediately start an internal investigation to map the scale of the breach, identify the nature, sensitivity and volume of the affected data and take measures to contain the breach. Although a personal data breach that is sufficiently serious can give rise to inside information, an EU-listed issuer may want to assess whether it complies with the conditions to defer disclosure. Among other things, the issuer should consider if the deferral could be likely to mislead the public (*e.g.*, if there have been rumors in the press or statements by the CEO in this respect), and the issuer may not be in a position to ensure confidentiality (*e.g.*, if affected individuals must be notified).
- If the conditions for deferral are not met, the company must immediately disclose the breach to the public as required by MAR. If the GDPR thresholds for notification are also crossed, the company will at that point be under a GDPR-specific obligation to simultaneously notify the DPA and/or the affected individuals directly as well.

¹⁴ Article 34(3) GDPR.

- But even if the conditions under MAR for deferral are met, a company having suffered a data breach may prefer to take the initiative and opt for full disclosure of the breach in a carefully crafted message, to remain in control of its communication and avoid the backlash of information surfacing through rumors which could then only be confirmed by it. At the same time, the company must consider whether and when it has sufficiently definite information to make a meaningful disclosure and should monitor whether any disclosure should be subsequently amended or corrected in light of newly discovered information. In the context of a personal data breach, experience shows that it is often difficult to get a clear grasp quickly about the scope, nature and severity of the breach.
- From a GDPR perspective, even if a decision is taken under MAR to defer disclosure, where personal data is affected and a risk to the rights and freedoms of the individuals whose personal data was breached exists, the competent DPA must be notified. This notification required by GDPR should fall within the “normal course of professional duties” exemption for selective disclosure of inside information of Article 10(1) MAR and relevant personnel of the DPA will be subject to a statutory confidentiality obligation¹⁵ as required under Article 17(8) MAR. However, since the DPA may not be as attuned to the intricacies of delayed disclosure of inside information under MAR, a listed issuer should still point those nuances out to the DPA specifically and make sure communication about the data breach is done in a coordinated manner. It may be prudent to caution a DPA not to communicate publicly about a data breach, contact affected individuals selectively or otherwise endanger the confidentiality of the selectively disclosed inside information without at least giving the company prior notice.
- The interplay between GDPR notifications and MAR disclosure becomes even trickier when dealing with the requirement to notify affected individuals selectively and directly. That notification cannot be made subject to a confidentiality requirement and, in any event, one must assume that confidentiality of the information can no longer be ensured once a significant number of affected individuals has been notified of the fact that their personal data has been breached. At that point, the issuer can therefore no longer defer public disclosure under MAR and will need to make the information public simultaneously with the GDPR notifications being sent to the directly affected individuals. The content of the disclosure and the level of detail to be provided to the public under MAR will however slightly differ on a number of points from what GDPR requires to be provided to directly affected individuals.¹⁶

¹⁵ See Article 54(2) GDPR.

¹⁶ For GDPR’s specific requirements in this respect, see also the Article 29 Working Party Guidelines on personal data breach notification under Regulation 2016/679, adopted on October 3, 2017, *available at* http://ec.europa.eu/newsroom/document.cfm?doc_id=47741.

- Finally, internal policies of EU-listed issuers, including incident response plans, should ensure that the relevant documentation requirements under MAR and the GDPR are complied with simultaneously. GDPR requires companies to document not just general measures implemented to ensure compliance with GDPR and prevent data breaches, but also specifically to “*document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken*”¹⁷ and, if applicable, to justify its decision to delay notification beyond the initial 72 hours after having become aware of the data breach.¹⁸ In addition, MAR requires EU-listed issuers, upon deferral of disclosure, to document the deferral decision, establish insider lists, declare a prohibited period and prepare leakage press releases. Upon disclosure, the issuer will need to inform the competent MAR authority and provide evidence of the initial fulfillment of the deferral conditions.

As the issues outlined above show, managing simultaneous MAR and GDPR compliance in case of a mass data breach is very challenging and will require coordination among various actors involved within the affected company's organizational structure and with external advisors. Yet, ensuring compliance at every turn is key, considering the severe sanctions a company may face for noncompliance with either GDPR or MAR.

¹⁷ Article 33(5) GDPR.

¹⁸ Article 33(1) GDPR.