AN A.S. PRATT PUBLICATION
SEPTEMBER 2017
VOL. 3 • NO. 7

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 3 NUMBER 7 SEPTEMBER 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 [233] (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

(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. 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.

Data Protection, Privacy, and the Hospitality and Leisure Industry: Preparing for the EU GDPR

By Gretchen Scott, Campbell Featherstone, and Federica De Santis*

This article explores key changes particularly relevant to hospitality businesses that will be introduced under the General Data Protection Regulation.

Guest data is an increasingly important arsenal for hospitality brands to personalize the guest experience, build customer loyalty and differentiate themselves from Online Travel Agencies. As such, the ability to collect data and maximize its use is now a strategic imperative. Technology has enabled the mass collection of personal data, which offers unprecedented and exciting opportunities for businesses to understand and drive customer behavior.

At the same time, regulation of customer data is increasing, with the European Union ("EU") leading the charge in imposing controls around the processing of personal data. Customers are now more wary of data exploitation and savvy as to their legal rights, whilst data security breaches regularly make lurid headlines and can be incredibly damaging to corporate reputations. In the age of technology and intense competition for customers, businesses must be aware of regulatory regimes affecting their processing of customer data and vigilant as to ongoing compliance.

THE GENERAL DATA PROTECTION REGULATION

In one of the most significant global privacy developments of the past 20 years, the EU has adopted the General Data Protection Regulation 2016/679 ("GDPR"). The GDPR will come into effect on May 25, 2018, replacing the existing privacy regime (EU Directive 95/46/EC ("Directive")) and introducing sweeping and significant new obligations regarding personal data. This article explores key changes particularly relevant to hospitality businesses that will be introduced under the GDPR.

Broader Territorial Scope

Many global hospitality businesses have significant operations in the EU and are already subject to the Directive on the basis they are "established" within a member state. The GDPR extends the reach of the Directive with two additional limbs

* Gretchen Scott (gscott@goodwinlaw.com) is a partner in Goodwin Procter LLP's Business Law Department and a member of the Hospitality and Leisure Group, Strategic Technology Transactions and Licensing Group, Life Sciences Group and Privacy and Cybersecurity Group. Campbell Featherstone (cfeatherstone@goodwinlaw.com) is an associate in the firm's Business Law Department. Federica De Santis (fdesantis@goodwinlaw.com) is an associate in the firm's Business Litigation group and a member of its Privacy and Cybersecurity practice.

designed to capture foreign businesses that target data subjects in the EU: (1) offering goods or services to individuals in the EU, and (2) monitoring their behavior (for example, through online tracking) so far as it takes place within the EU.

The territorial scope reflects efforts by the European Commission to export its data protection laws around the globe. Targeting the EU market will now bring your business and company within the ambit of the GDPR, notwithstanding that the offer of goods or services may be made from afar and the goods or services themselves (for example, hotel accommodation) are located outside the EU. This extended reach is likely to catch off-guard those businesses not established in the EU that target EU customers. Mere access to a website or a "general" offer of goods or services should not in itself suffice. But hospitality businesses with tailored EU or Member State-specific sites – or even those that simply accept payments in Euros – are at a particular risk of finding themselves directly subject to the GDPR.

The second limb is triggered by "monitoring" the behavior of data subjects in the EU, through the use of website cookies that track personal data or, for example, through customized "user accounts" requiring a login. For those businesses that avoid the first limb, this second limb may yet bring them within the jurisdictional reach of the GDPR.

If subject to the GDPR, a non-European business will need to appoint an EU-based representative to act as a point of contact for EU data protection authorities ("DPAs") and individuals on all issues related to compliance with the GDPR.

Higher Fines

The potential financial ramifications of a failure to comply with data protection laws will increase markedly, with potential for substantial fines (up to €20 million or four percent of an infringer's global revenues, whichever is higher, for more serious breaches). While fines at the upper end of the scale are likely to only be levied in instances of the most egregious breaches of data protection law, the sheer magnitude of the potential fines (which evoke the penalties under the EU competition law regime) is indicative of the shift in attitude towards the importance of data protection and data security within the EU.

Consent

Many hospitality businesses rely on the "consent" of the data subject as the legal basis for various processing activities, for example, to enable data to be transferred to a third party (such as a marketing partner). Establishing "consent" is tougher under the GDPR than under the Directive: businesses will not be able to rely on silence, inactivity or a pre-ticked box; nor may consent be buried within general terms and conditions – it must be obtained in a manner that is distinguishable from consent given when entering other written agreements. Where consent has previously been relied upon to justify processing activities, businesses will need to carefully assess whether their existing

consents meet the new conditions and, if they do not, fresh consent will need to be obtained (unless another legal basis for processing can be established). Businesses will also need to ensure that processes are in place to enable customers to withdraw consent as easily as they give it.

Notification of Data Breach

Data controllers – including hospitality businesses – will be expressly required to notify the relevant DPA of certain "personal data breaches," unless they can show the breach is unlikely to result in a risk to the rights and freedoms of individuals. Likewise, affected individuals must also be notified if the breach is likely to result in a "high risk" to their rights and freedoms. Businesses will need to assess their internal processes to ensure that appropriate procedures are in place to detect, investigate, report and document data breaches and to manage the fall-out from such reporting.

Data Processors

Whereas the Directive regulates only the entity controlling personal data, the GDPR imposes direct obligations on third parties ("data processors") that process data on behalf of the data controller (for example, suppliers in the GDS network, third-party support service providers and cloud hosting providers). New obligations include maintaining written records of processing for the data controller, appointing a representative (if the data processor is based outside the EU) and notifying the data controller of a breach "without undue delay." We expect significant changes to the contractual obligations negotiated between controllers and processors as a result.

No Notification

The obligation to register with the local DPA has been abandoned. In its place is a requirement to carry out an internal data risk impact assessment and implement procedures focusing on high risk operations. The DPA must be consulted if the assessment shows that processing would result in a high risk which is not possible to mitigate. The DPA may then use its enforcement powers to intervene if it is concerned the processing may breach the GDPR.

Data Protection Officer

Data protection officers are already a feature of the data protection regime of certain member states (e.g., Germany). The GDPR introduces a uniform requirement for certain controllers and processors to designate a data protection officer, notably (for the hospitality industry) if their core activities consist of processing which, by its nature, scope or purpose, requires regular and systematic monitoring of data subjects on a large scale. The data processing activities of the hotel brands, including their membership programs, are likely to trigger the requirement to appoint appropriately qualified data protection officers. Businesses need to be assessing whether they will be subject to this additional administrative requirement.

International Data Transfers

The GDPR, like the Directive, restricts and regulates data transfers to countries outside the European Economic Area (the EEA, comprising the EU member states, Norway, Iceland, and Lichtenstein) that do not ensure an adequate level of data protection. The permitted methods of transferring data outside the EEA remain broadly in place, with some improvements. Given the increased penalties that will apply under the GDPR, it is particularly important for hospitality businesses to consider the extent to which they transfer personal data elsewhere – both intra-group and to service providers – and to ensure that the correct arrangements are in place to ensure lawful transfers of personal data. Notably, transfers which are currently undertaken on the basis of consent should be reconsidered in light of the fact that, under the GDPR, a data controller may only rely on consent as a basis for exporting personal data outside the EEA where such consent is explicit (especially given that consent may be withdrawn at any time). Accordingly, reliance on consent is unlikely to be practical for systematic transfers of personal data; as such, data controllers should look to have robust, permanent arrangements in place to underpin any transfers.

One-Stop Shop

A business with multiple establishments in the EU (or whose sole EU establishment substantially affects individuals in multiple member states) may now benefit from the new "one-stop shop" approach to enforcement under which the DPA of the business' main establishment acts as the lead authority to coordinate investigations and enforcement actions concerning the business' compliance with the GDPR, thus avoiding having to deal with all 28 DPAs.

TIME TO PREPARE?

The GDPR requires data controllers to implement data protection measures "by design" and "by default." This means that the measures put in place by data controllers to process personal data must "by design" implement data protection principles, and must "by default" only process that personal data which are necessary for the specific purpose of the processing. The sooner that a business turns its mind to the requirements of the GDPR, the sooner it can implement – by design – processes, protocols and documentation that facilitate its compliance with the GDPR.

Hospitality businesses that will be subject to the GDPR (particularly those not subject to the existing EU privacy regime) should take advantage of the lead time before the GDPR comes into force, and consider the following initial steps to prepare themselves:

- Conducting an audit of current data protection practices. This should involve mapping what personal data businesses hold about individuals in the EU, where it came from, with whom personal data is shared and to which countries it is transferred.
- Performing a gap analysis to identify the areas requiring changes to comply with the GDPR.
- Starting to implement the changes in time for the GDPR's implementation to test for and address compliance challenges.
- Revisiting processes for obtaining personal data from individuals (such as privacy policies and registration forms for loyalty programs) to ensure compliance with the GDPR.