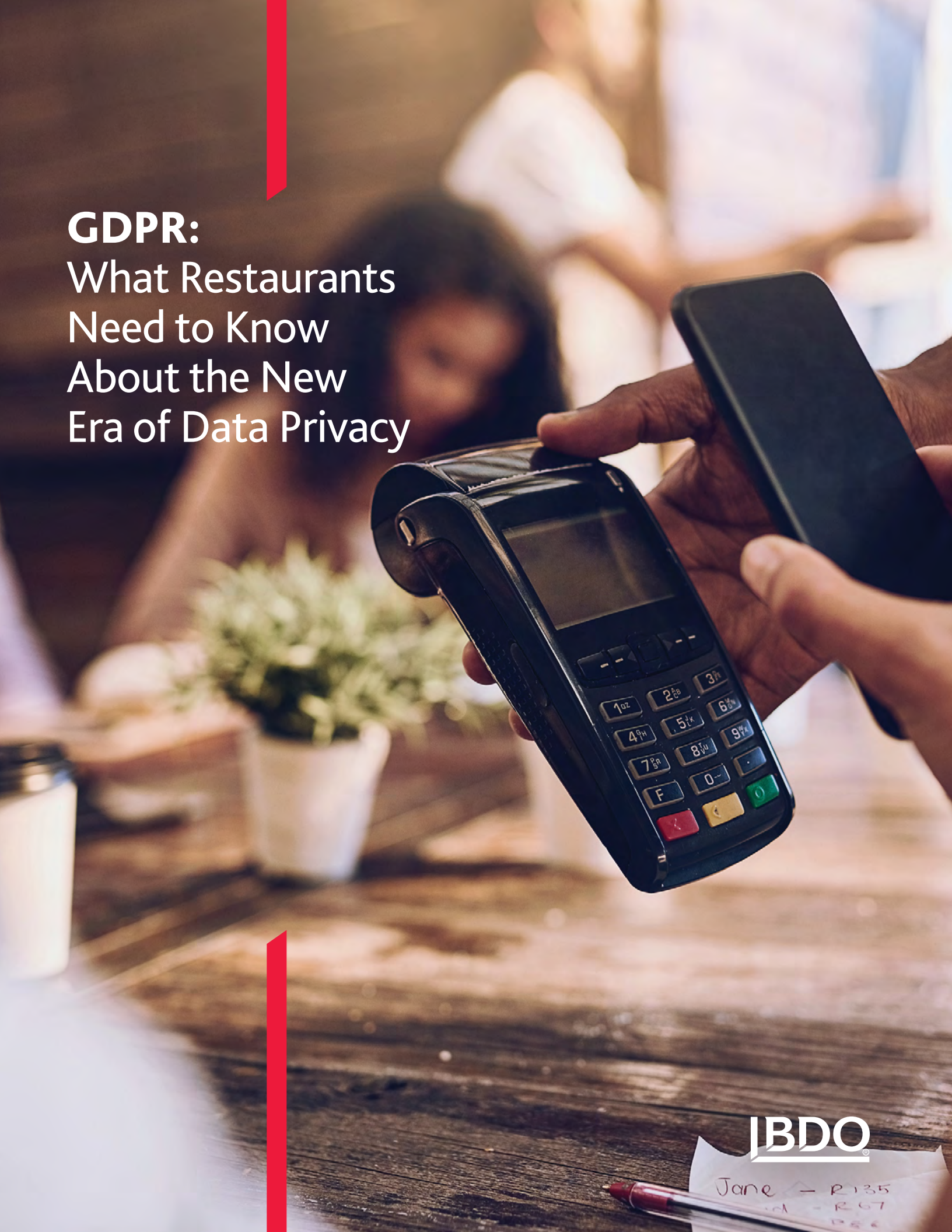
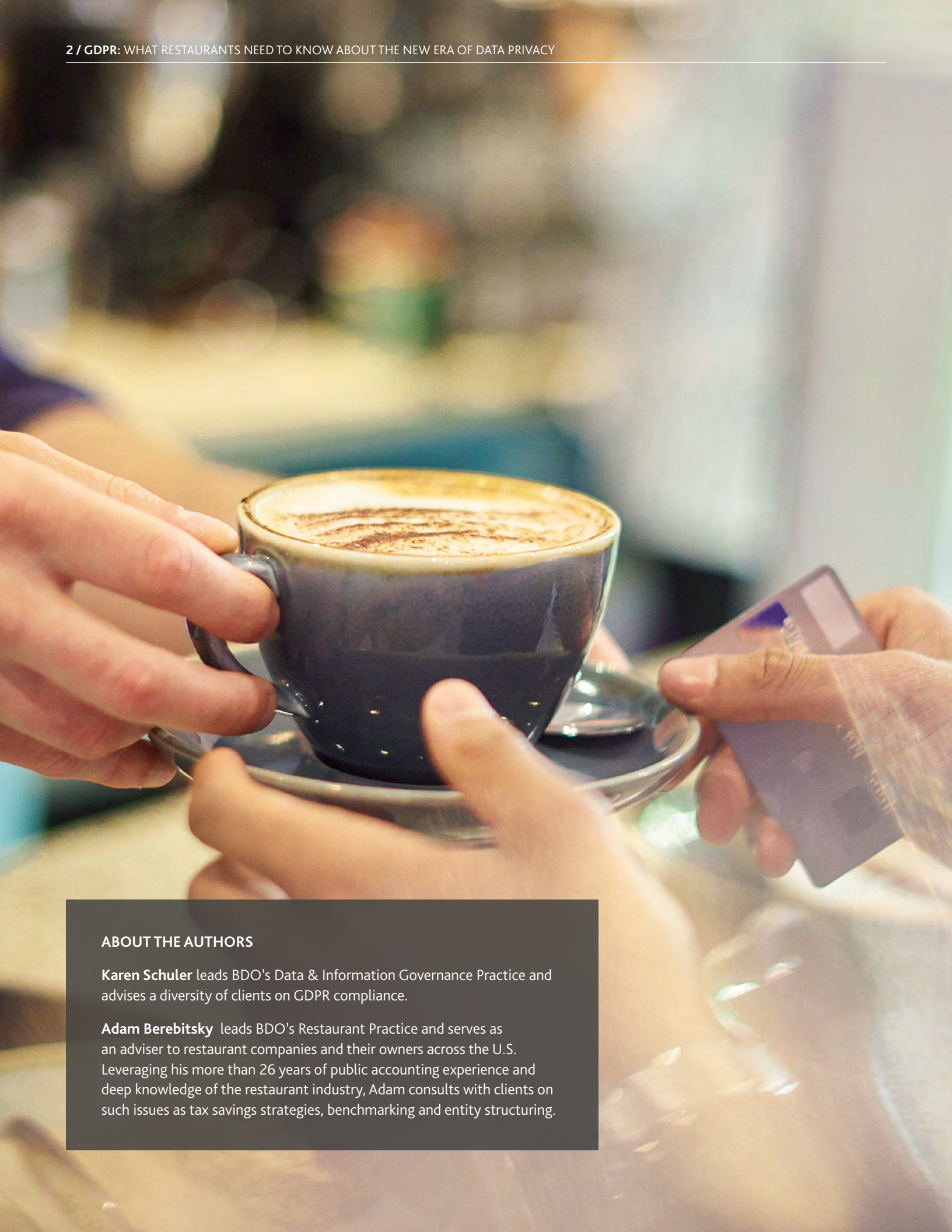
GDPR:
What Restaurants Need to Know About the New Era of Data Privacy





ABOUT THE AUTHORS

Karen Schuler leads BDO's Data & Information Governance Practice and advises a diversity of clients on GDPR compliance.

Adam Berebitsky leads BDO's Restaurant Practice and serves as an adviser to restaurant companies and their owners across the U.S. Leveraging his more than 26 years of public accounting experience and deep knowledge of the restaurant industry, Adam consults with clients on such issues as tax savings strategies, benchmarking and entity structuring.

For U.S.-based restaurants, the European Union's recent enactment of the General Data Protection Regulation (GDPR) means navigating unexpected compliance hurdles. As the most significant change to EU data privacy policy in more than two decades and the most comprehensive data privacy law that American businesses have ever faced, restaurants are obliged to safeguard the personal data of individuals in the EU—regardless of where they're headquartered.

Say a U.S. based quick-serve restaurant opens a new location in France. That restaurant is now held to the policies set forth in the GDPR, despite it being headquartered in the United States. In fact, many restaurants operating in both the U.S. and the EU are working towards universal privacy compliance, given impending new domestic privacy regulations and on-going requirements of the GDPR.

But what about restaurants operating outside of the 28 EU member states? It may be assumed that U.S. restaurants without stores in the EU, especially those operating out of a single location, can simply disregard the GDPR entirely—but this may not be the case. Because the GDPR aims to protect the data of EU individuals, regardless of where they are, U.S. restaurants that regularly serve individuals from the EU may be required to comply if they are collecting personal information. This is particularly relevant to restaurants that operate out of tourism hotspots across America, such as New York City or Las Vegas. Those that regularly retain the personal data of EU individuals, through things like credit card payments and loyalty programs, must handle that data with a process that aligns with GDPR standards.

The GDPR's impact was felt around the world, and lawmakers everywhere are considering how they can modernize their data protection practices. Noncompliance with policies, procedures or misuse of personal data can have hefty legal, reputational and financial consequences. With such stiff penalties—four percent of annual revenue or €20 million, whichever is greater—restaurant operators will need to go beyond simply checking the box and truly make an overall commitment to responsible information governance and data privacy.

At the same time, balancing EU and U.S. data privacy regulations could prove challenging for restaurants, particularly as regulations continue to evolve. For example, the California Consumer Privacy Act will become effective in 2020, requiring Californian restaurants to provide information on how customer data is being used and imposing restrictions on data sharing for commercial purposes. A thorough assessment of risk exposure to current and upcoming data privacy laws can help restaurants be prepared to implement necessary changes.

How can restaurants implement an effective GDPR program?

The GDPR seeks to enforce the expanded data privacy rights of individuals in the EU and in doing so requires adequate protection from businesses both within and outside of its borders. In other words, if your restaurant deals with the personal data of individuals in the EU in any way, then the GDPR likely applies to you.

How it applies to you depends on whether you are a "controller" or "processor" of EU personal data. Controllers determine data processing goals and make decisions on how personal data will be used, while Processors collect, store and process personal data based on instructions from the Controller. In many cases, restaurants act as both. See below for more details on the obligations of both role under GDPR.

PRINCIPLES

DATA SUBJECT RIGHTS

CONTROLLER OBLIGATIONS

MEMBER STATE DEROGATIONS

OPERATIONS (PROCESSOR) AREAS

- Policies and procedures
- Technology
- Information security
- Third-party risk management
- Website activity
- Information governance/record retention
- Contract requirements
- Documentation of processing activites
- Breach notifications
- Data Protection Impact Assessment (DPIA)
- Data trasfer mechanisms

CONTROLLER OBLIGATIONS

- Identification of personal data and special categories/sensitive data
- Accountability – Documentation on compliance
- Notice
- Consent documentation and withdrawal mechanism
- Special categories of data
- Constraints and requirements for autmated decisioning
- Legitimate basis for processing
- Cross-border transfers
- Security obligations
- Data Protection Officer (DPO)
- Representatives

PRINCIPLES

- Fair, lawful, and transparent
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

RIGHTS OF THE DATA SUBJECT

- Right of access
- Rectification and erasure
- Data portability
- Right to restriction/restriction of processing
- Right to object
- Transparency
- Right to erasure

GDPR compliance needs will vary between restaurants, based on how well their business activities support the expanded personal data privacy rights of individuals in the EU. Enacting an effective GDPR program could prove to be particularly complicated for franchised restaurants, especially those who have an array of customer touchpoints across channels. These multiple touch points range from point-of-sales, to e-commerce and loyalty programs, as well as mobile applications, kiosks, ERP systems and even e-mail.

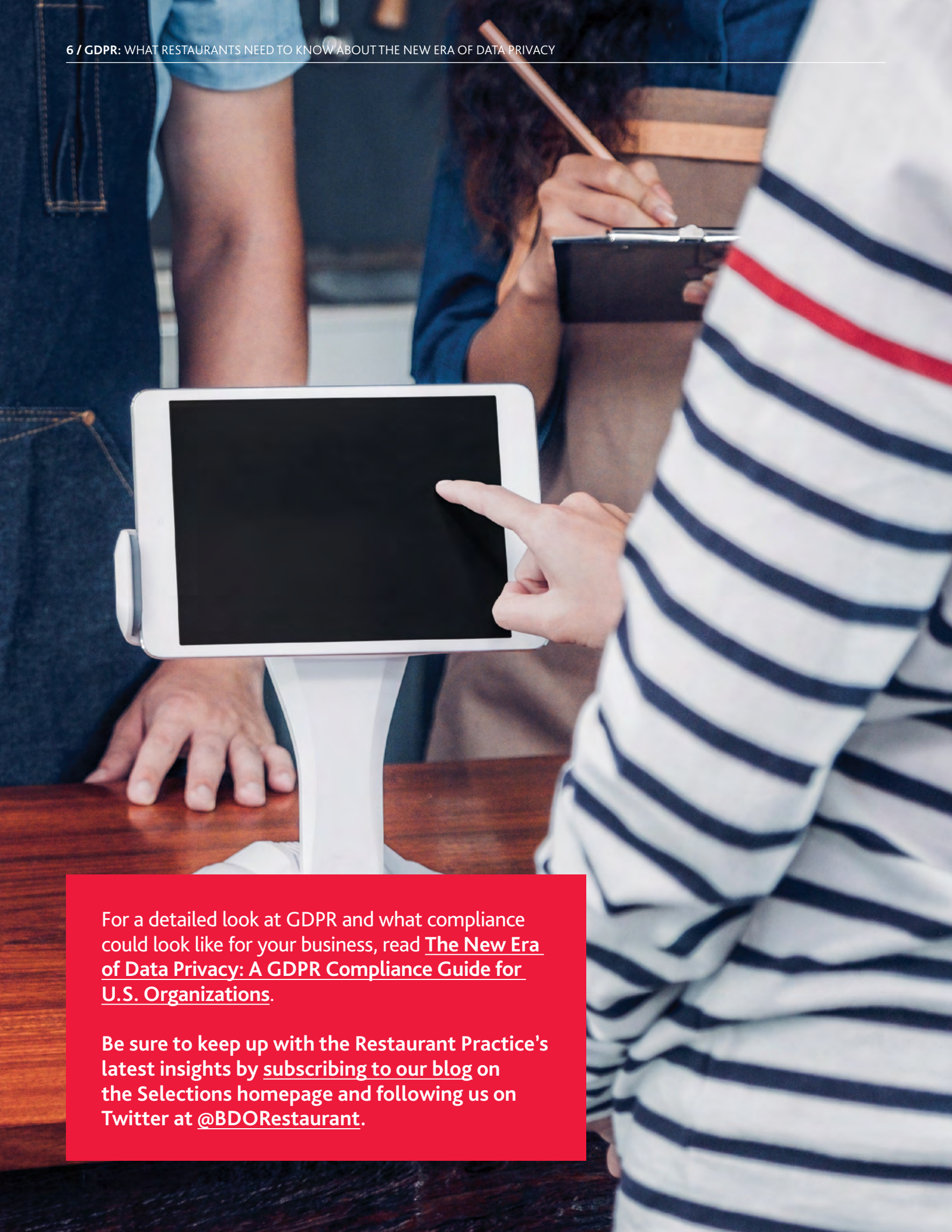
For starters, restaurants should consider some common questions when it comes to implementing their data privacy program, including:

- If a data subject wishes to delete their data, how will I locate their personal data? How will the company decide what can be deleted and what is required for regulatory or legal retention purposes?
- If a consumer data subject wishes to gain access to their personal data, what can the company provide to them? What format will it be delivered?
- What personal data does the company retain and for how long?
- Do we work with vendors that are provided access to consumer data?
- Do we have employees that may make data subject requests and does the company understand how to address those requests?
- Can the company meet the 30-day deadline? Will 60-day extensions be requested?

Data subject requests are by far one of the most complicated aspects of complying with the GDPR because consumers want to know:

- How their personal data is protected.
- Where their data is located, and who has access to it.
- How to correct personal information.
- Whether the company has consent to use or share their personal data.

Overall, GDPR requires that businesses, including restaurants, take a holistic approach to privacy governance. Keep in mind that GDPR was established with the understanding that data privacy will continue to evolve, and the enforcement of personal data privacy rights will need to change accordingly. Even U.S. -based restaurants without EU locations must be prepared to protect customer data through comprehensive privacy programs, with the goal of driving a culture of data privacy and protection throughout the company. Restaurants who both confirm their current policies address GDPR requirements and establish robust, responsive data privacy philosophies will be best equipped for the new era of data privacy.



For a detailed look at GDPR and what compliance could look like for your business, read **The New Era of Data Privacy: A GDPR Compliance Guide for U.S. Organizations**.

Be sure to keep up with the Restaurant Practice's latest insights by subscribing to our blog on the Selections homepage and following us on Twitter at @BDORestaurant.

People who know Restaurants, know BDO.

www.bdo.com/**restaurants**

CONTACT

KAREN SCHULER
National Data & Information Governance Leader
kschuler@bdo.com

ADAM BEREBITSKY
National Restaurant Practice Leader
aberebitsky@bdo.com

BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, and advisory services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through more than 60 offices and over 650 independent alliance firm locations nationwide. As an independent Member Firm of BDO International Limited, BDO serves multi-national clients through a global network of more than 73,800 people working out of 1,500 offices across 162 countries.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. For more information please visit: www.bdo.com.

Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your needs.

© 2018 BDO USA, LLP. All rights reserved.