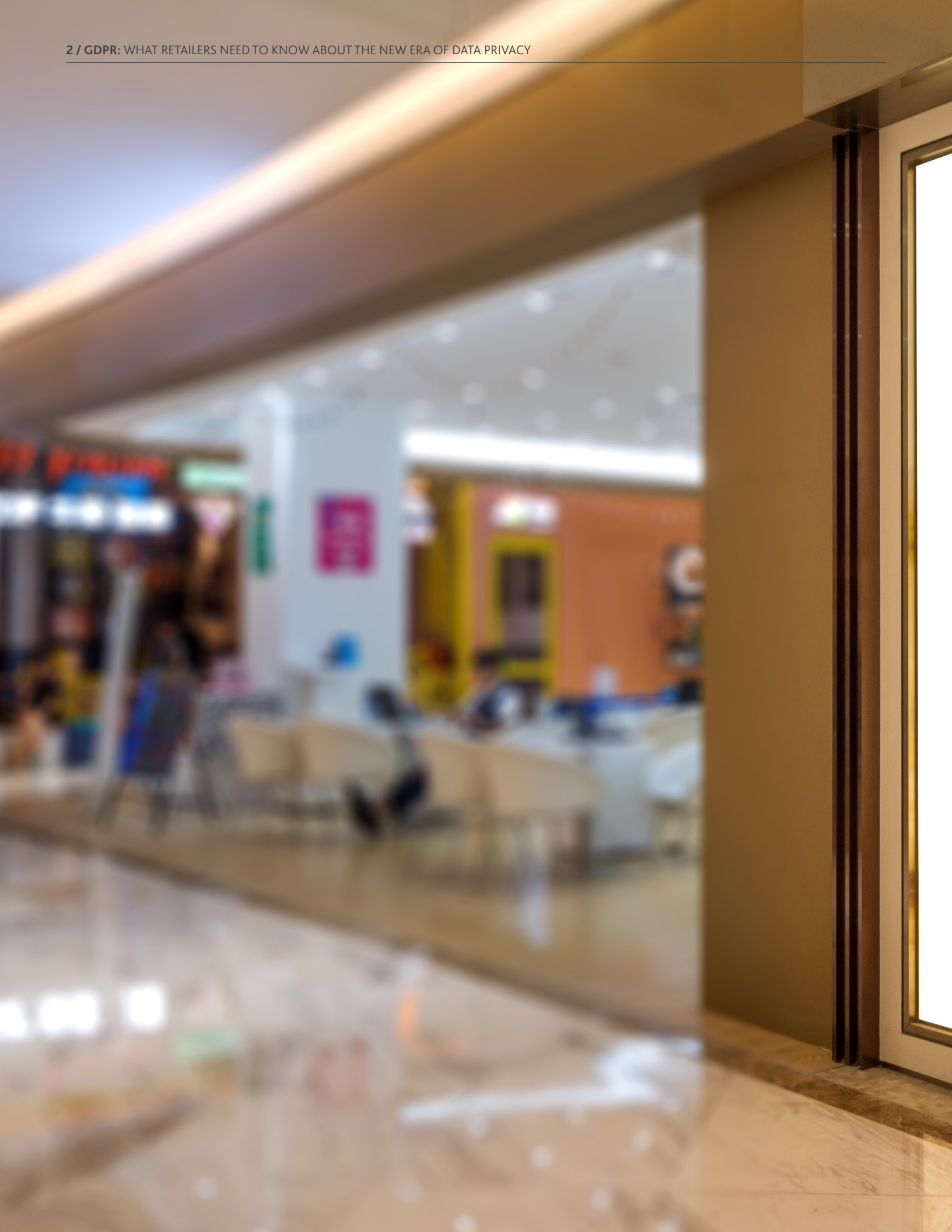
GDPR: What Retailers Need to Know About the New Era of Data Privacy



It's no secret that the role of data in the retail industry has grown considerably with the rise of global e-commerce and mobile commerce. Therefore, retailers are heavily impacted by international data privacy regulations.

In part, this is why it's critical for retailers to understand the General Data Protection Regulation (GDPR)—the most significant change to European Union (EU) data privacy policy in more than two decades and the most comprehensive data privacy law that American retailers have ever faced. Officially implemented on May 25, 2018, the regulation aims to safeguard personal data of individuals in the EU, applying to companies that process their personal data—regardless of where the retailer is headquartered.

In this fast-paced, constantly-evolving digital landscape, information governance has become a prominent topic, with lawmakers around the world considering how they can modernize their data protection policies. Noncompliance with those policies or misuse of individuals' personal data can have hefty legal, reputational and financial consequences. Consider that under GDPR, the fine for Facebook's Cambridge Analytica data breach could have been up to $1.5 billion, according to TechRadar.

Savvy retailers who wish to avoid such penalties—which could be four percent of annual revenue or €20 million, whichever is greater—will go beyond checking the box by making an overall commitment to responsible information governance and data privacy. This starts with an understanding of differences in privacy regulations, the various components of GDPR and what readiness and maintenance looks like for retailers.

HOW DO U.S. AND EU DATA PRIVACY LAWS COMPARE?

GDPR is the EU's overarching data protection law for all 28 EU member states, allowing only some differences in approach among those states. By contrast, the U.S. has no single comprehensive law equivalent to GDPR—rather, the U.S. has industry- and state-specific data privacy policies.

These opposing approaches correlate to differences in the way data privacy is viewed. In Europe, data privacy is defined as a right, and explicit consent must be provided for organizations to use individuals' personal data outside of the reason for which it was initially collected. Contrarily, in the U.S., the definition of data privacy has historically been flexible, including trade-offs for certain benefits and privileges.

Balancing EU and U.S. data privacy regulations could prove challenging for retailers, particularly as policies continue to evolve. For example, the California Consumer Privacy Act will become effective in 2020, requiring retailers 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 retailers be prepared to implement necessary changes.

What are the primary principles of GDPR that retailers should know?

Like its predecessor the Data Protection Directive of 1995 (DPD), GDPR includes several guiding principles. The seven key principles of GDPR, as found in Article 5 of the regulation, are:

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimization
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality
7. Accountability principle

Where GDPR principles differ from those of its predecessor is the new accountability principle, which holds retailers responsible for proactively complying with—and demonstrating compliance with—the regulation.

However, the biggest changes are in scope and enforcement—GDPR seeks to enforce the expanded data privacy rights of individuals in the EU and doing so requires adequate protection from businesses both within and outside of its borders.

In other words, if your retail business 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. Many retailers are both. See the next page for more details on the obligations of both roles 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

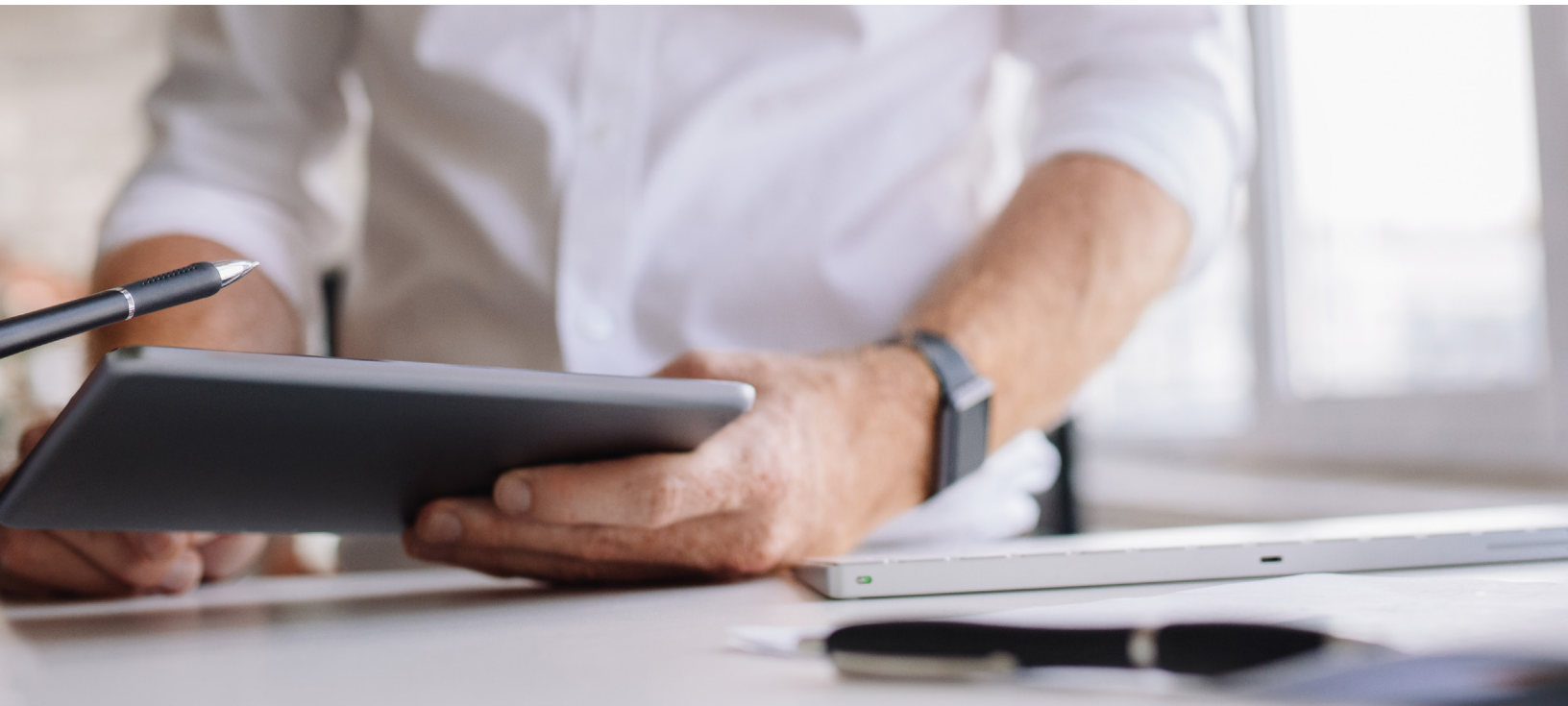
- Identification of personal data and special categories/sensitive data
- Accountability - Documentation on compliance
- Notice
- Consent documentation and withdrawal mechanism
- Special categories of data
- Constraints and requirements for autmated decisioning
- Legitimate basis for processing
- Cross-border 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



How can retailers implement an effective GDPR program?

GDPR compliance needs will vary from retailer to retailer, 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 retailers, particularly those who have an array of customer touchpoints across channels, as well as those that have franchises. These multiple touch points range from point-of-sales, to e-commerce and call centers, as well as mobile applications, kiosks, ERP systems and even email.

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

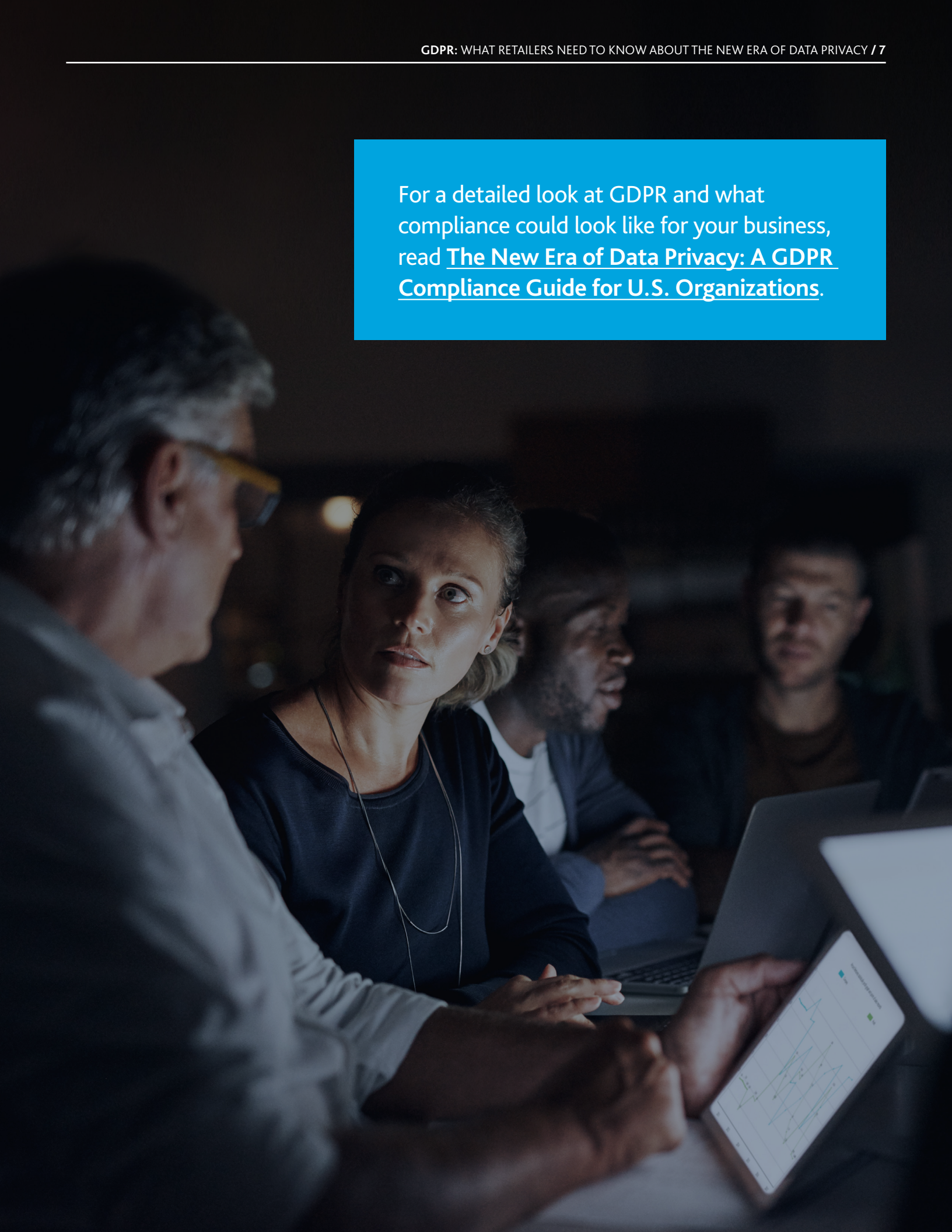
- If a data subject wishes to delete their data, how will I locate all of their information? How will the company make a determination of what can be deleted and what is required for regulatory or legal retention purposes?
- If a consumer data subject wishes to gain access to their personal data, what 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 need to work with third-party vendors to obtain copies of personal data?
- Do we have employees that may make similar 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 retailers take a holistic approach to data 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. Effective data privacy programs should align with retailers' business, operations, legal and technology functions, helping drive a culture of data privacy and protection throughout the company. Retailers who both confirm their current policies address GDPR requirements and establish robust, responsive data privacy corporate 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**.



CONTACT

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

NATALIE KOTLYAR
National Retail & Consumer Products Practice Leader
nkotlyar@bdo.com