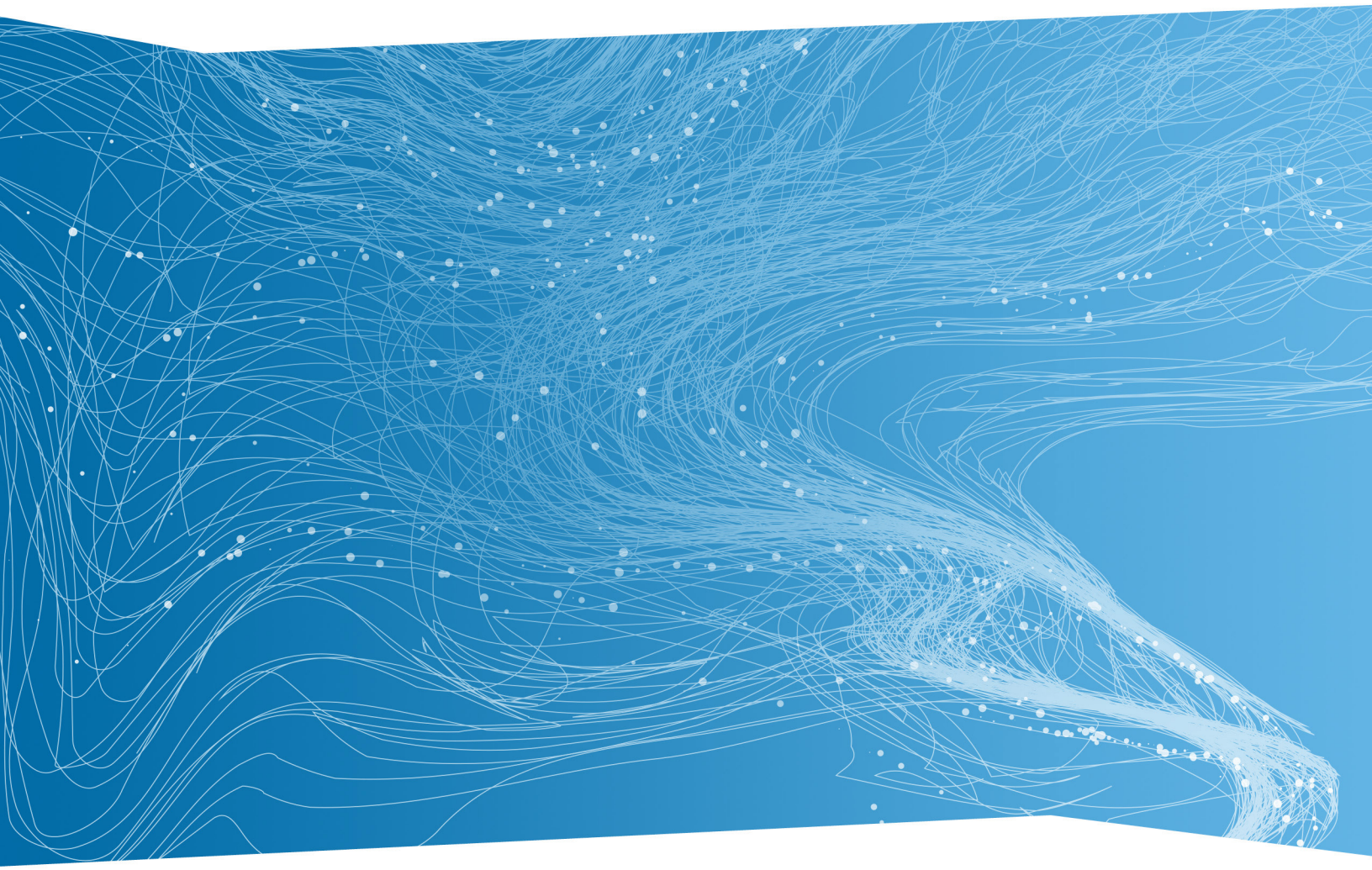
RSA



WHITE PAPER

# GDPR: RETHINKING HOW YOU THINK ABOUT PERSONAL DATA

RSA

Complying with the General Data Protection Regulation (GDPR) can seem an overwhelming challenge to organizations that control and process personal data belonging to residents of the European Union (EU). From retailers and others that keep track of customer preferences, to healthcare providers and insurers that maintain medical records, to financial services companies entrusted with data about income and other personal financial information, organizations bound by the provisions of GDPR will face a stringent set of requirements for protecting data privacy beginning May 25, 2018. And while many of the principles underlying the regulation are not new, at least some of the requirements—such as data subjects' right to be forgotten—will be unfamiliar, if not unprecedented. A complete understanding of what's going to be required demands thinking about data's journey through an organization—from data collection through disposal—in new and different ways.

By using existing beliefs about personal data and its role and purpose as starting points, organizations can begin to see where and how their current thinking about the data journey may need to shift in light of GDPR. This paper examines three sets of beliefs that are likely to currently characterize the beginning, middle and end of the data lifecycle in many organizations. It explores how a fundamental yet simple shift in the thinking surrounding each one may help bring about a better understanding of the regulation.

The context for this discussion is the overall goal of GDPR: to protect the personal data of an EU resident. Everything the regulation provides for is in the service of that goal. It expands data subjects' control over how their personal data is collected and used, and it expands the responsibilities of data controllers and processors to protect the data through its lifecycle, starting with data collection.

## COLLECTING PERSONAL DATA: IT'S NOT HOW MUCH YOU HAVE. IT'S HOW LITTLE.

Back in 2012, the rule for customer data collection seemed to be "the more, the merrier." In an article in the *Harvard Business Review* that year, a software executive reported that "We believe that any business should gather as much data from their customers as they possibly can get."[1] In 2015, a researcher reported in Forbes: "Retailers are in the midst of a data land grab. They are trying to collect all of the consumer data they can possibly get their hands on. Why? Because they're hoping that some of it will prove to be valuable."[2]

Fast-forward to 2017, and customer data collection is still a critical part of doing business; GDPR doesn't change that. It does, however, address the *indiscriminate* collection of personal data. Organizations that want to continue to think of data collection as an exercise in gathering as much as possible will find that line of thinking at odds with the requirements of GDPR. The regulation requires that personal data be collected for specified purposes only

RSA

and for that data to be "adequate, relevant and limited to what is necessary in relation to the purposes for which they [the data] are processed."[3]

In other words, it's time to stop thinking about how much data is enough and start thinking about how personal data should be used for a legitimate business purpose, which was disclosed to the data subject at the point of collection.

## USING PERSONAL DATA: IT'S NOT "WE'LL SEE HOW LATER." IT'S "WE NEED TO KNOW NOW."

One of the GDPR stipulations for obtaining consent from data subjects to collect their personal information is that the consent cannot be "bundled"—rather, it has to be given individually for each specific data processing activity and business purpose. This spells the end of the aforementioned once-common practice of collecting data in hopes that it will prove valuable in some way at some future time. When someone gives consent to use their personal data for a particular purpose, it's no longer okay to keep it and use it for other things that come up. This requires organizations to think of personal data as something whose purpose they need to carefully shape and determine before data collection, rather than after the fact.

In thinking through how to use the personal data they collect, organizations also need to think about some specific areas of caution under GDPR. For example, the profiling of data subjects based on their personal data, and decision-making based on that profiling, are restricted by GDPR.[4] Another area that requires careful thinking through in light of GDPR is sharing of personal data with third parties like contractors and vendors.[5] For example, under GDPR, a company that outsources HR functions is responsible for what happens to employees' personal data that's shared in the process. Complicating the challenge is the dynamic nature of third-party relationships; vendors and contractors come and go, and you need to stay a step ahead of those changes. Once you and your GDPR compliance advisors have established a strategy for managing this third-party risk, a robust third-party governance solution can be invaluable for documenting and monitoring relevant changes on an ongoing basis.

## RETAINING PERSONAL DATA: IT'S NOT "KEEP IT TILL YOU NEED IT." IT'S "KEEP IT TILL YOU DON'T."

Until now, it may not have been that unusual for an organization to have personal data on hand that has long ceased to be useful. From years-old job applications that lie forgotten in a file to product registrations submitted by people who've gone a decade without buying anything else, personal data may sometimes simply be the product of benign neglect. Or it's part of the "maybe I'll need it someday" thinking that has also led to organizations collecting personal data without attaching a purpose to it—a practice that is no longer acceptable under GDPR.

While GDPR doesn't mandate deleting personal data after a specific amount of time, it does state that the data must be kept "in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed," unless it's for certain specific types of archiving.[6] So if it's not going to be deleted, it will have to be pseudonymized. There's also another good reason for organizations to go ahead and delete personal data they no longer need—and that's the "right to be forgotten"[7] rule of GDPR. That provision gives data subjects the right to request that an organization delete all the personal data it maintains on them, subject to certain exceptions as specified under applicable laws. Obviously, the fewer records the organization keeps over the long term, the less onerous it will be to comply with such requests.

## CREATING AN ADVANTAGE FOR COMPLIANCE

GDPR isn't just a new set of rules for protecting personal data; for many organizations, it's a whole new way of thinking about personal data—especially for those based in some non-EU countries where data privacy laws may not be as strict as they have historically been in the EU. Adopting a new perspective on the journey that personal data takes through the organization may be a challenge, but having that understanding of the larger context for GDPR can provide an advantage to organizations moving through their own journey to achieve GDPR compliance. The regulation will likely evolve and change over time, but the fundamental ways of thinking about personal data that underpin it will remain. Understanding those perspectives can only help.

Learn more about RSA Archer® governance, risk and compliance (GRC) solutions and other RSA solutions to help with GDPR compliance at rsa.com/gdpr.

[1] David K. Williams and Mary Michelle Scott, "How One Company Uses Customer Data to Drive Sales," *Harvard Business Review* (September 6, 2012)

[2] Nikki Baird, "How Much Customer Data Do Retailers Really Need?" *Forbes* (October 27, 2015)

[3] Article 5, EU GDPR, "Principles relating to processing of personal data"

[4] Rita Heimes, "Top 10 operational impacts of the GDPR: Part 5—Profiling," International Association of Privacy Professionals (January 20, 2016)

[5] Alexandra Ross, "A strategic approach to vendor-management under the GDPR," International Association of Privacy Professionals (February 28, 2017)

[6] Article 5, EU GDPR, "Principles relating to processing of personal data"

[7] Article 17, EU GDPR, "Right to erasure ('right to be forgotten')"

RSA and the RSA logo, are registered trademarks or trademarks of Dell Technologies in the United States and other countries. © Copyright 2018 Dell Technologies. All rights reserved. Published in the USA. 02/18 White Paper H16993.

RSA believes the information in this document is accurate as of its publication date. The information is subject to change without notice.