

UNPREPARED FOR GDPR?

A Research Report on the State of Enterprise Readiness for the EU's New PII Mandates



Compuware

| The Mainframe Software Partner For The Next 50 Years

Key Takeaways

- The EU General Data Protection Regulation (GDPR) requires enterprises to track all instances of customer PII across the organization, to obtain customer consent for the use of their PII (including the “right to be forgotten”) and to document the efficacy of this data governance to auditors.
- Two-thirds (68%) of enterprises risk failure to comply with GDPR due to increasing data collection, growing IT complexity, proliferating applications, outsourcing and mobile—as well as lax policies in regards to data masking and getting explicit data-related permissions from customers.
- EU and US enterprises alike must therefore adopt a variety of best practices— including more rigorous masking of test data and better customer consent practices—to avoid the financial penalties and potential damage to brand reputation that can result from non-compliance.

GDPR and Its Implications

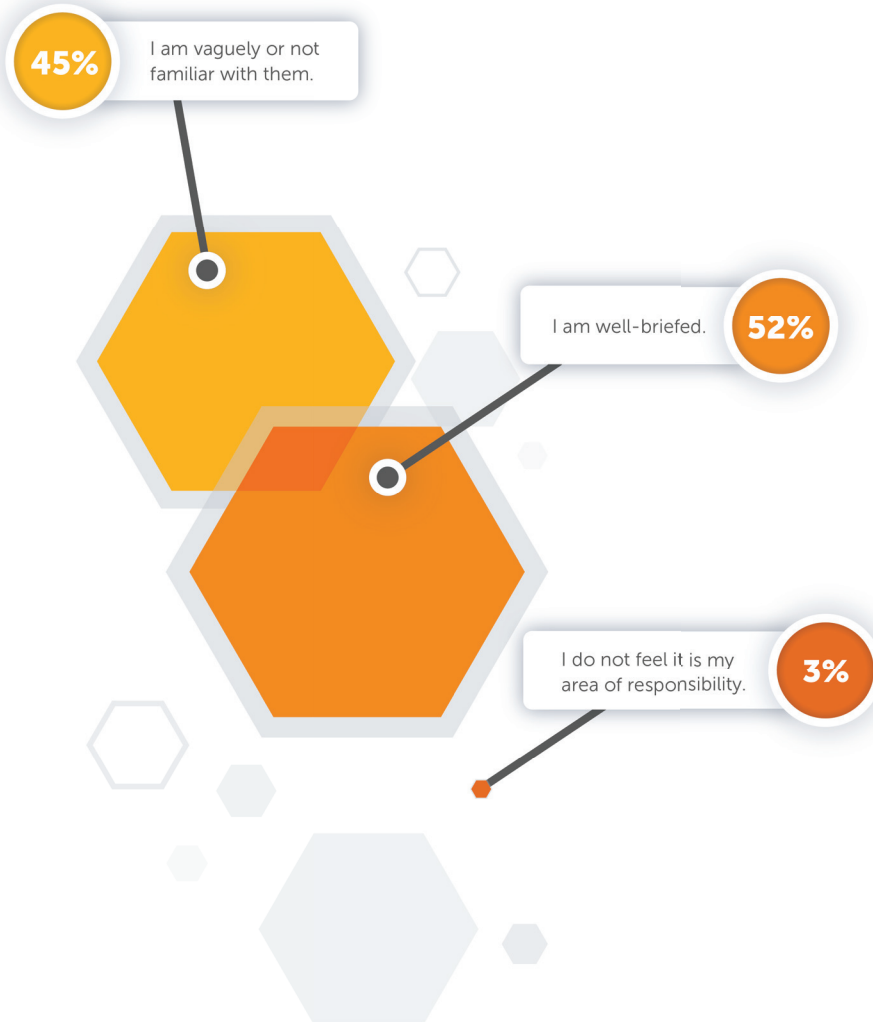
The EU General Data Protection Regulation (GDPR) was adopted in April 2016 to unify previously fragmented mandates across EU jurisdictions regarding how enterprises use, manage and delete customers’ Personally Identifiable Information (PII). All enterprises in the EU, the US and elsewhere that capture PII relating to EU citizens must comply with its provisions by May 2018. Any failure to comply with GDPR exposes enterprises to fines of as much as €20 million or 4% of global turnover— whichever is higher.

The GDPR presents significant challenges to enterprises when it comes to data governance. Of particular note are GDPR provisions that:

- Rigorously and expansively define PII to include everything from customer email addresses and tax IDs to their hobbies and social media posts.
- Require enterprises to obtain specific and explicit permissions for PII use.
- Mandate credible documentation to auditors of the specific mechanisms used by the enterprise to track and appropriately control PII use across all systems and platforms.
- Assert an EU citizen’s legal “right to be forgotten”—i.e., that enterprises be demonstrably capable of removing every instance of a customer’s PII across all systems and platforms at the customer’s request.

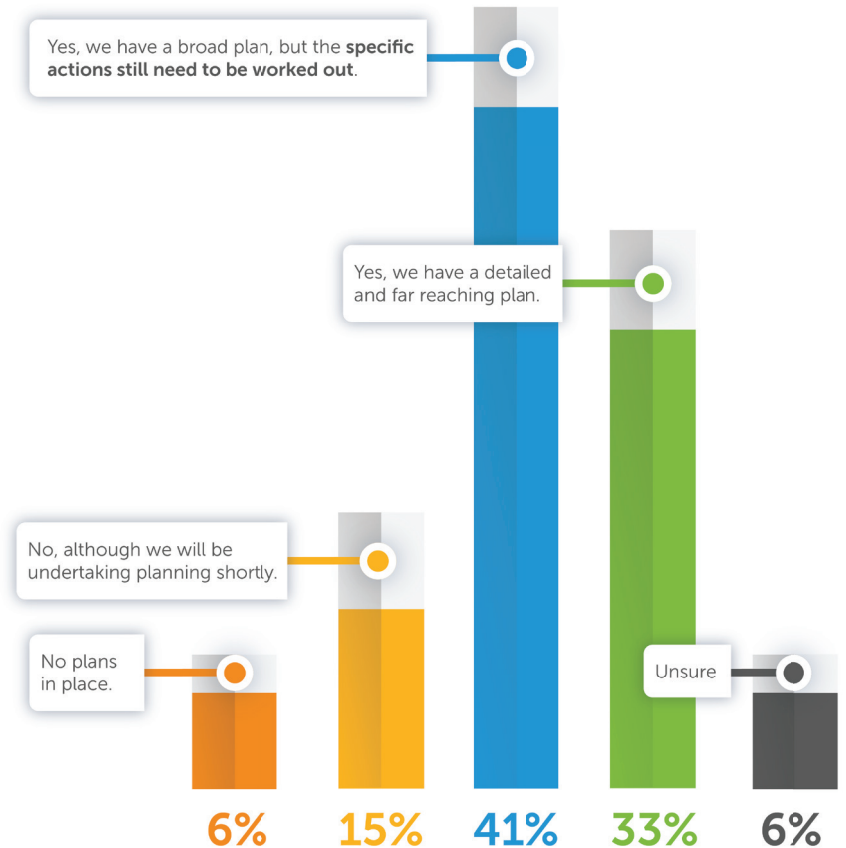
Just over half (52%) of survey respondents claimed to be well-briefed on the GDPR and its impact on the handling of European customer data. However, almost as many (45%) said instead that they were only ‘vaguely’ familiar or unfamiliar with GDPR provisions.

What is your familiarity with the European General Data Protection Regulation (EU GDPR) and its impact on the way that businesses handle European customer data?



Knowledge about GDPR does not correlate with preparedness. A full two-thirds (68%) of survey respondents said either that their companies do not currently have a comprehensive GDPR compliance or that they are unsure about the existence of such plans.

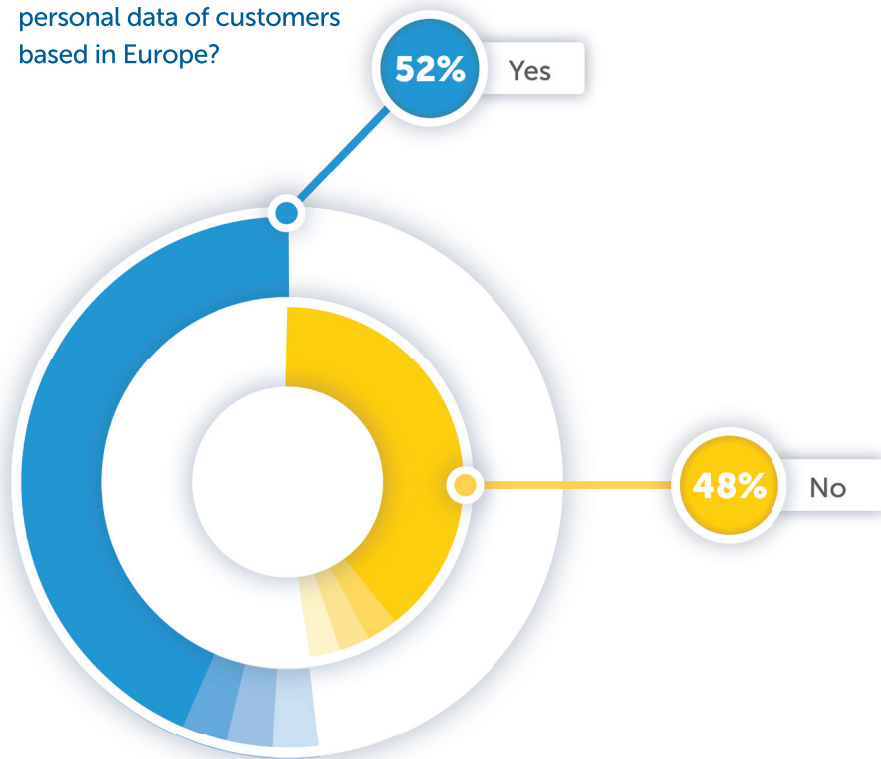
Has your organization put plans in place for how it will respond to the customer data implications of the GDPR?



Results have been rounded to the nearest whole number.

GDPR awareness was somewhat lower among US respondents (43%). That lack of awareness could prove problematic for many US companies, since 52% acknowledge that they possess EU customer data—which means that they will in fact need to comply with GDPR even though they are US-based.

Does your organization possess or process any personal data of customers based in Europe?



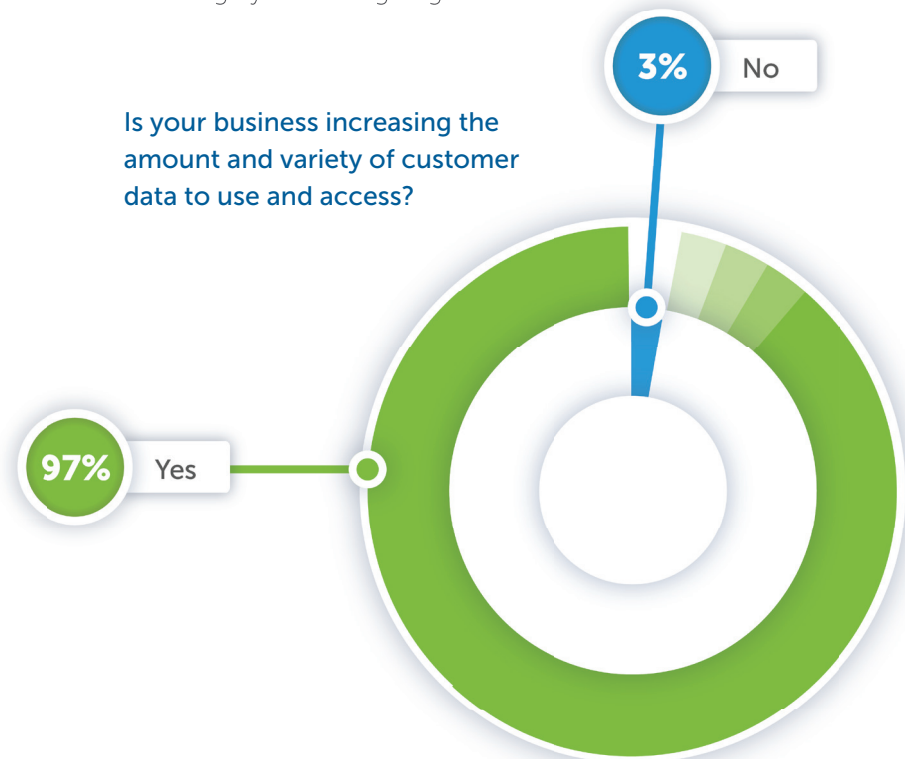
Compliance Challenges for the App-intensive Enterprise

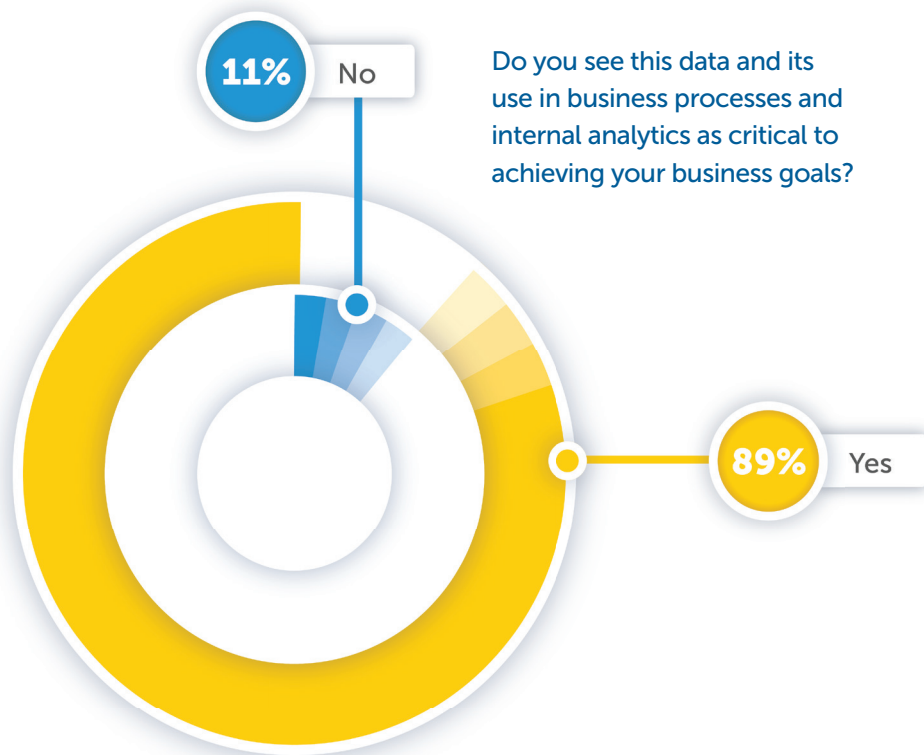
Compliance with GDPR mandates won't be easy. The increasingly digital nature of business inherently makes it more difficult to monitor every instance of an individual customer's PII everywhere across an enterprise IT environment comprised of multiple systems and platforms.

More specifically, survey respondents cited four key factors exacerbating the difficulty of GDPR compliance:

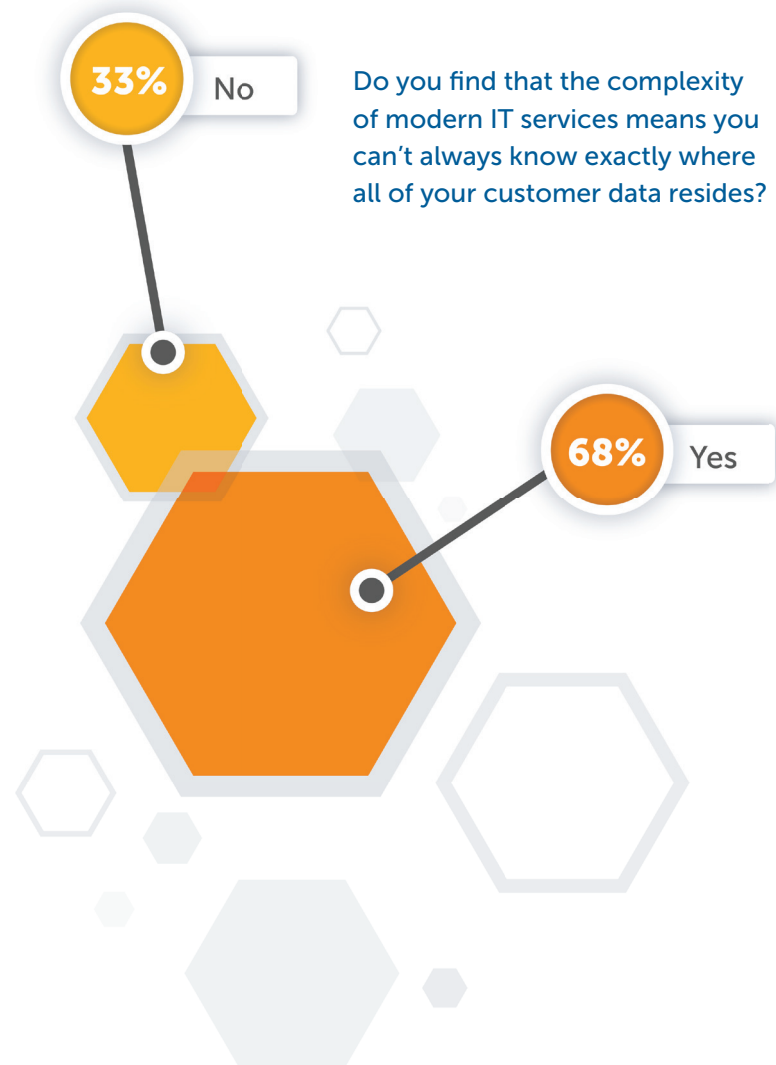
Increasing data collection. The more data an enterprise possesses, the more challenging it can be to keep track of it all—and to perform specific operations such as PII deletion for individual customers. Yet enterprises are almost universally (97%) working to collect even more customer data. And they almost universally (89%) view that data as critical to achieving their business goals. So any GDPR compliance measures they adopt will have to be highly scalable going forward.

Is your business increasing the amount and variety of customer data to use and access?





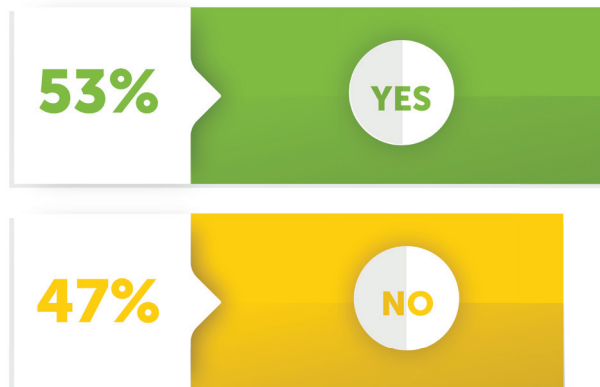
Growing IT complexity. Today's enterprise has typically accumulated multiple generations of technology—including mainframe, distributed and cloud-based platforms running various types of databases and applications. That's why 68% of survey respondents said the complexity of their IT services significantly inhibits their ability to know where all their customer data is at all times.



Results have been rounded to the nearest whole number.

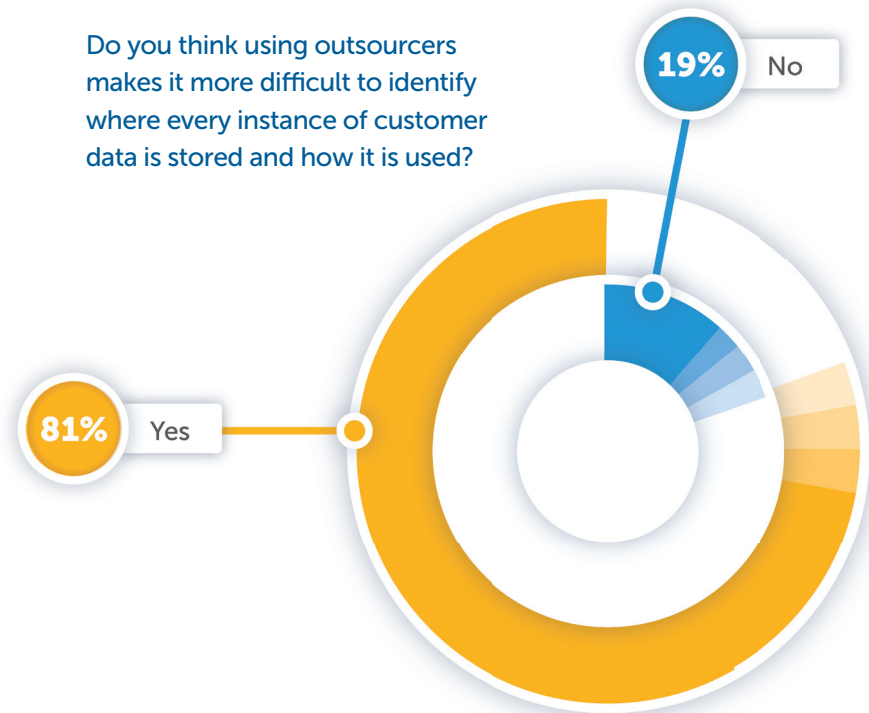
Agile and DevOps. In addition to scale and complexity, enterprises are also challenged by the speed and relentlessness with which their digital environments are undergoing change and expansion. The adoption of Agile Development and DevOps culture are driving this rapid, continuous change and expansion as enterprises seek to continually bring new, competitively differentiated value propositions to market—which, in turn, makes GDPR compliance an ever-moving target according to 53% of respondents.

Do you find that it is especially difficult to know where your organization's test data is at any one time?

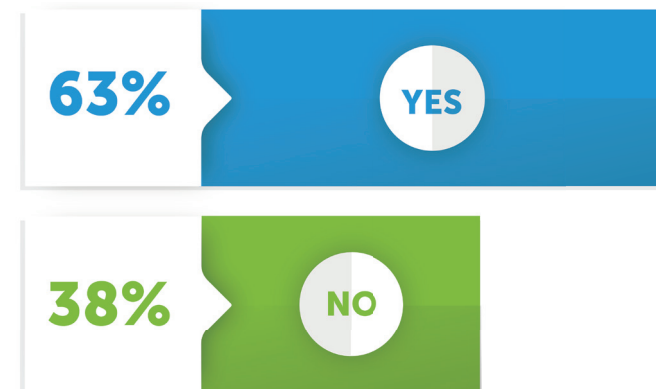


Outsourcing and mobility. GDPR compliance is further complicated by the fact that customer data does not always remain within the “four walls” of the enterprise. Data can be shipped to outsourcers who support application development efforts—and can wind up on users’ mobile devices. These two issues were cited by 81% and 63% of respondents, respectively. The cloud also makes it increasingly likely that instances of customer data will reside outside the enterprise data center.

Do you think using outsourcers makes it more difficult to identify where every instance of customer data is stored and how it is used?



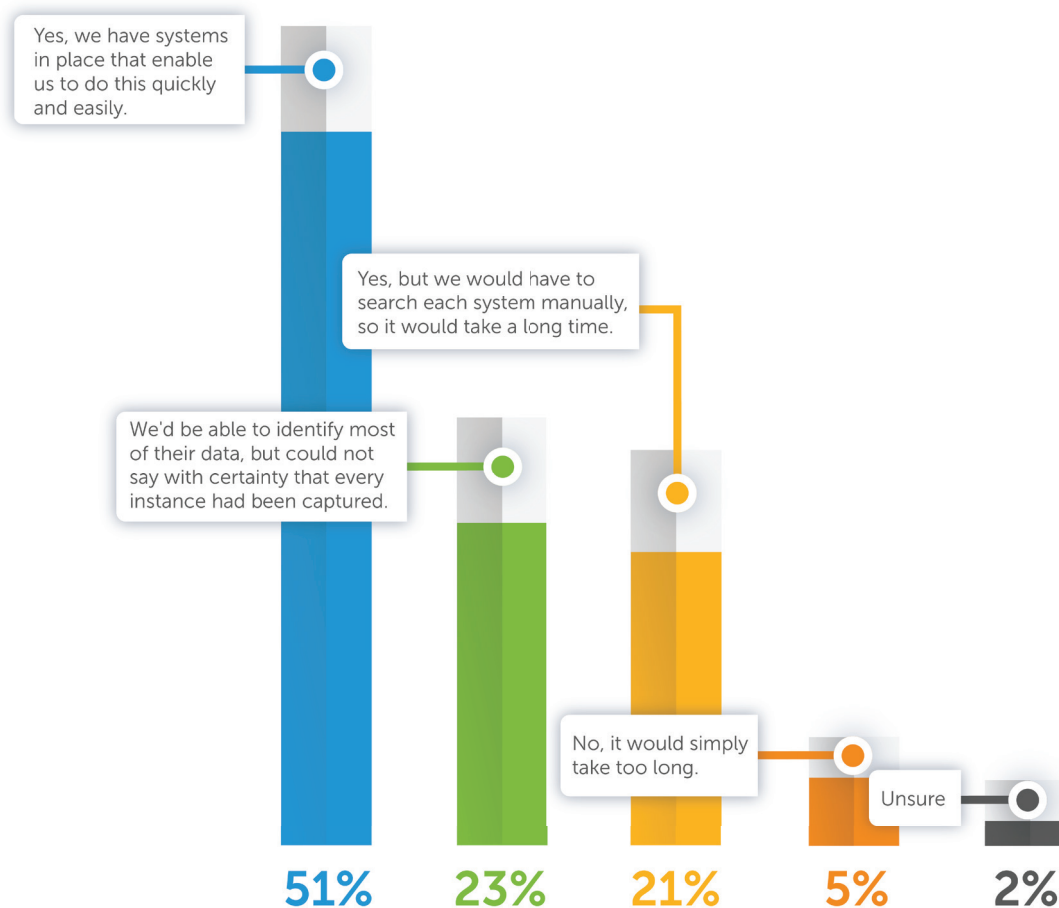
Do you think mobile technology has made it more difficult to keep track of where your customer data is at all times?



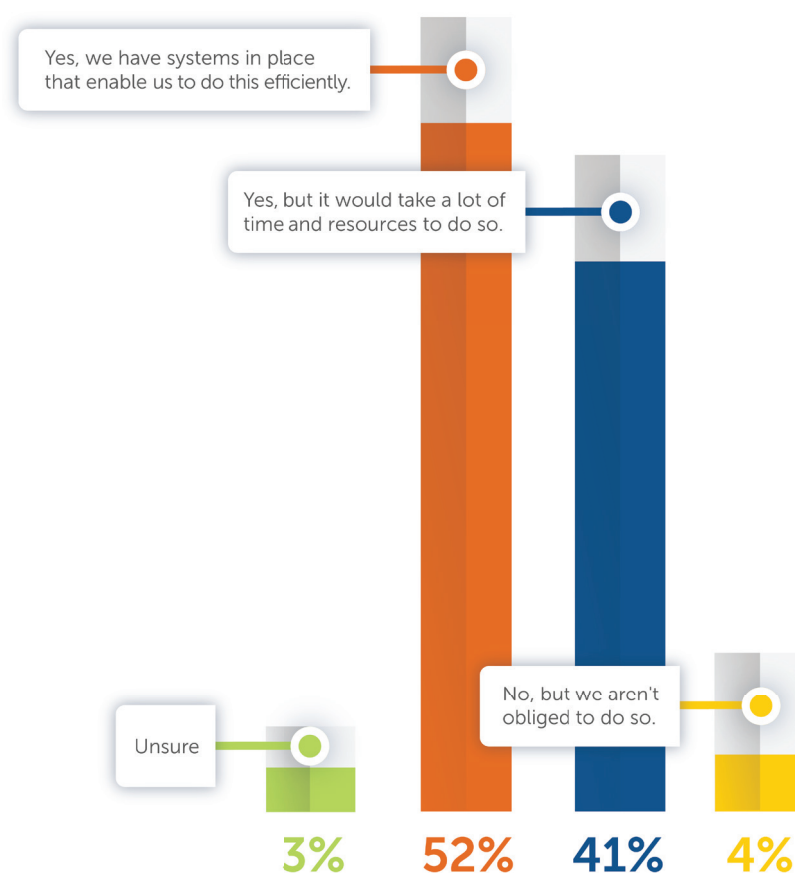
Results have been rounded to the nearest whole number.

Due to these factors and others, only about half (51%) of survey respondents believed they could quickly and easily find every instance of a customer's PII. About a quarter (23%) said this could not be done with certainty, and about one fifth (21%) said it would be a manual process requiring a lot of time and resources. And only about half (52%) felt comfortable claiming the ability to remove all of that data efficiently should they be required to do so under a "right to be forgotten" request.

Would you be able to identify and locate every instance of an individual's personal data within your systems?



Would you be able to remove all of the data that your organization has on a particular person if you were required to do so?



Results have been rounded to the nearest whole number.

Test Data and Customer Consent: Two Critical Vulnerabilities

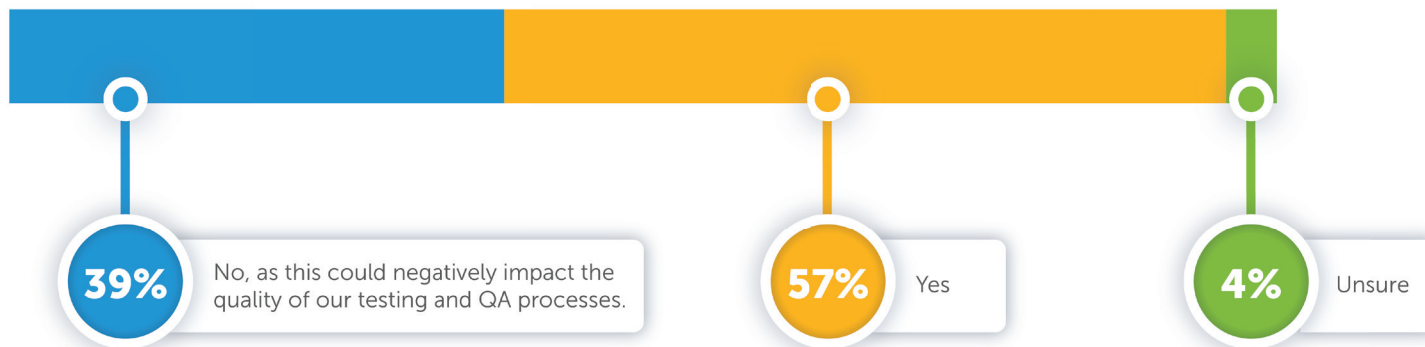
The survey also revealed two critical, pervasive and inter-related vulnerabilities when it comes to enterprise compliance with GDPR: test data and customer consent.

Test Data

Test data is a critical and pervasive compliance vulnerability, because it is one of the most common ways customer PII gets replicated and moved around (and beyond) the enterprise on an unplanned, ad hoc basis. Test data sets constantly need to be created as developers create new applications and enhance existing ones—and that developer work/product constantly has to be tested for functional and non-functional QA. If test data isn't properly masked and anonymized, every new test data set becomes a potential compliance problem down the road.

Yet, unfortunately, 43% of survey respondents admit to or are unsure of if they put customer PII at risk by failing to ensure that customer data is always anonymized before it is used for application testing purposes.

Does your company anonymize or use other techniques to depersonalize customer data before using it in application testing environments?



Failure to mask test data actually creates multiple compliance vulnerabilities, including

- An inability to pinpoint every instance of customer PII
- An inability to remove every instance of customer PII
- An inability to meet auditors' documentation requirements regarding these two mandates

Failure to mask customer data before sharing it with outsourcers—whether they're developers or testers—further exposes enterprises to risk by putting them at the mercy of the outsourcer's own security and compliance practices.

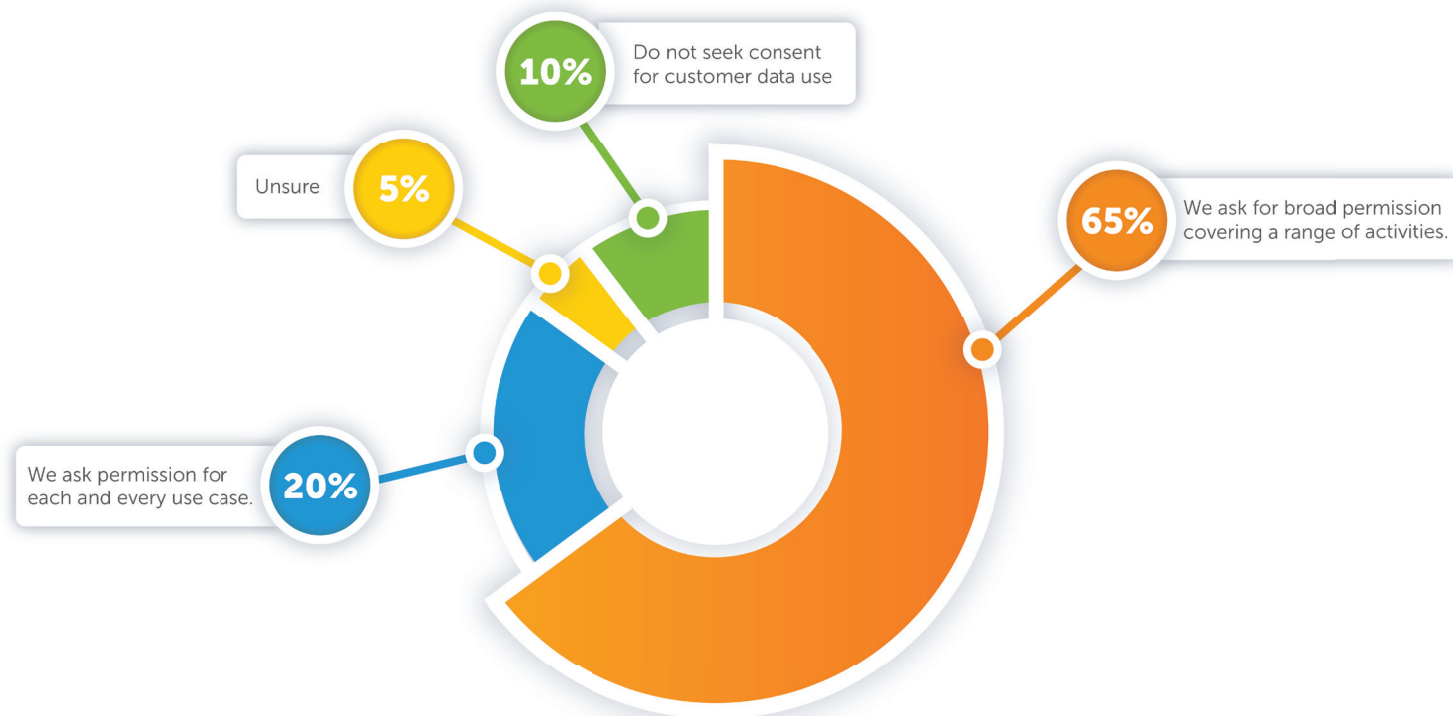
Customer Consent

The GDPR gives EU citizens more control over corporate use of their PII by requiring enterprises to gain explicit consent for specific uses of that PII, in addition to allowing them to request erasure of all instances of their personal data ("right to be forgotten").

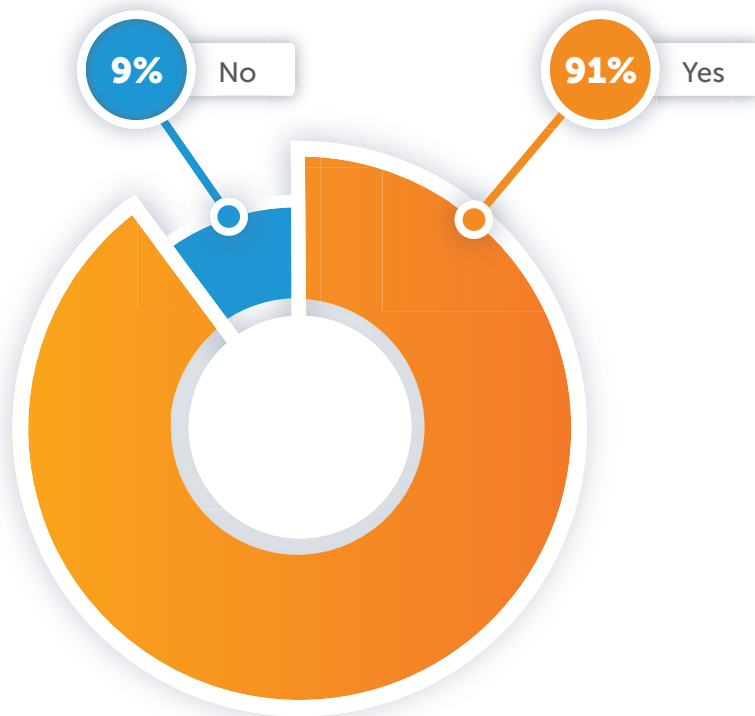
This presents a particular challenge for enterprises when it comes to test data, because 80% of survey respondents indicated that they either don't ask or aren't sure if they ask customers for explicit consent for their data to be used in application testing—making them currently non-compliant with the legislation.

Masking and anonymization of test data obviously solves the consent issue as well, since it exempts test data from the PII consent provisions of the GDPR. Test data masking is also a far better security measure than what the survey revealed 91% enterprises do at present—which is to rely on the terms of their employment contracts.

What is your approach for seeking customer permission to use their personal data for a variety of purposes?

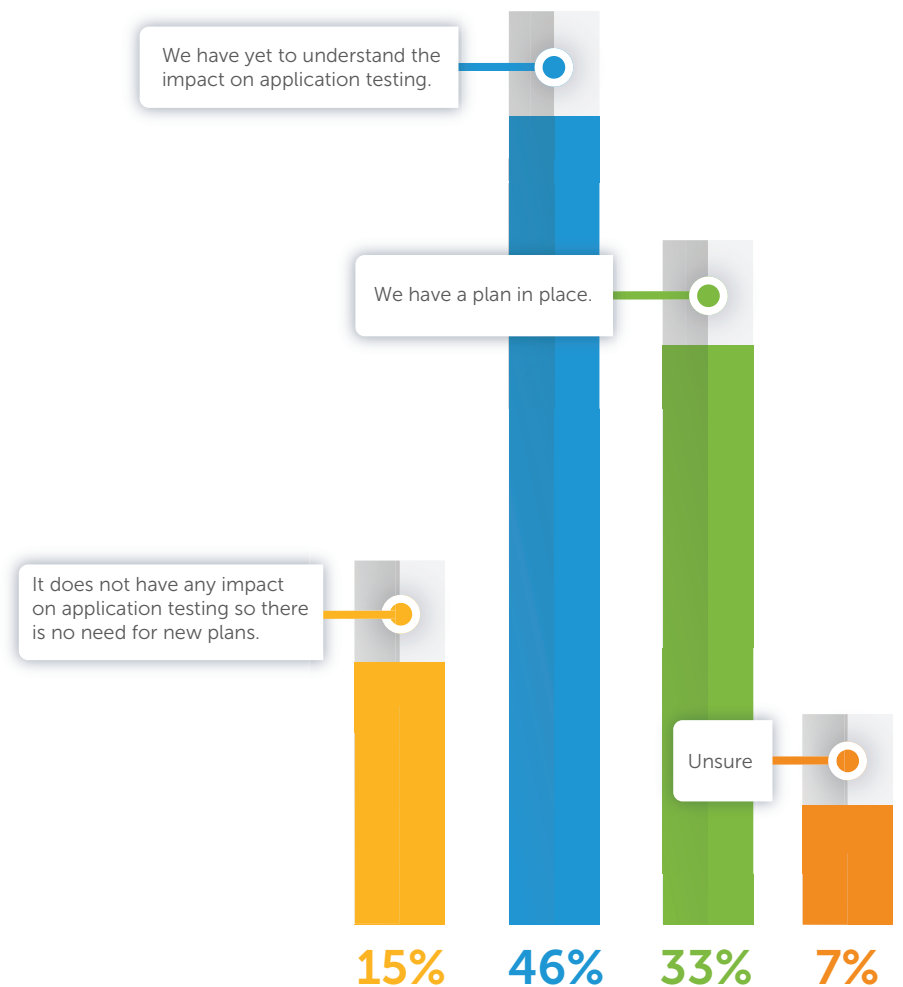


Does your organization rely on the terms and conditions laid out in its employment contracts to ensure its data policies are adhered to while using data to test applications?



The above issues would be less of a threat to GDPR compliance if enterprises were already taking appropriate steps to address their compliance shortfalls. But they're not. An overwhelming majority of respondents (68%) don't yet have a detailed plan in place for how they will address these issues. And 15% are still not even aware that there are issues to address.

Has your organization put plans in place for how it will respond to the impact that the EU GDPR will have on the way that it handles customer data in relation to application testing?



Results have been rounded to the nearest whole number.

Conclusion: Plan, Mask and Comply

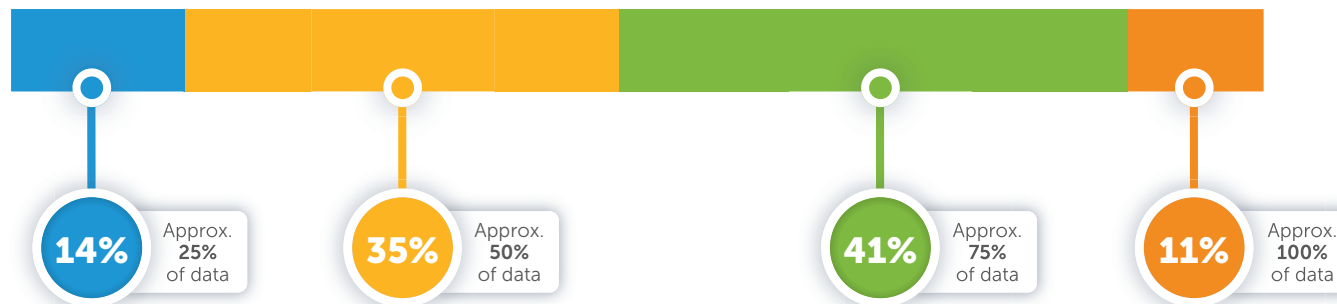
In addition to being descriptive, these study results also suggest a variety of prescriptive actions:

- 1. Stakeholder education regarding GDPR compliance.** Enterprises should take immediate steps to clarify their obligations under GDPR and educate all relevant stakeholders—including developers, QA staff and those managing outsourcer relationships—about their responsibilities for fulfilling those obligations.
- 2. Data governance process upgrade plan and execution.** Stakeholders should collaborate to determine where improvements need to be made in data governance—so instances of PII are reliably tracked and tight correlation is maintained between customer permission and actual PII use.
- 3. Implement masking technology.** It's not enough to mandate data masking. If masking isn't easy— and if it isn't sophisticated enough to fulfill the technical requirements of dev/QA teams—unmasked, untracked PII will continue to find itself into test environments. The right data masking technology is thus essential for GDPR compliance with confidence. Mainframe masking is particularly important, since that is where most enterprise data resides.

Deadline for compliance with GDPR is less than two years away. And while GDPR compliance is not extraordinarily difficult from a technical perspective, the results of this study clearly indicate that it will require significant changes from present enterprise practices.

Every enterprise technology and compliance manager should therefore help initiate the first steps towards GDPR best practices immediately, so that the final steps can be completed before auditors start assessing compliance—and before customers start demanding better control over their PII.

How much of your customer data is stored on a mainframe?



Results have been rounded to the nearest whole number.

Methodology

Conducted by independent research company Vanson Bourne and commissioned by Compuware, this survey was administered to 400 CIOs at large companies across vertical markets in both Europe and the United States in June 2016.

The Mainframe Software Partner For The Next 50 Years

Compuware empowers the world's largest companies to excel in the digital economy by fully leveraging their high-value mainframe investments. We do this by delivering highly innovative solutions that uniquely enable IT professionals with mainstream skills to manage mainframe applications, data and platform operations.

[Learn more at Compuware.com.](https://www.compuware.com)