The State of Data Rights

By IAPP Research Manager Margaret Honda
and IAPP Market Research Specialist Christelle Kamaliza, CIPP/E, CIPM

BigID iapp REPORT

Content

Research Objectives and Methodology

The **IAPP**, in partnership with **BigID**, set out to gain insight into the landscape of individual data rights, and how organizations provide data transparency to their employees and consumers. This report explores components of a framework for processing data access requests, deletion requests, and data transparency - including understanding the demand for data rights and its relationship to building brand trust.

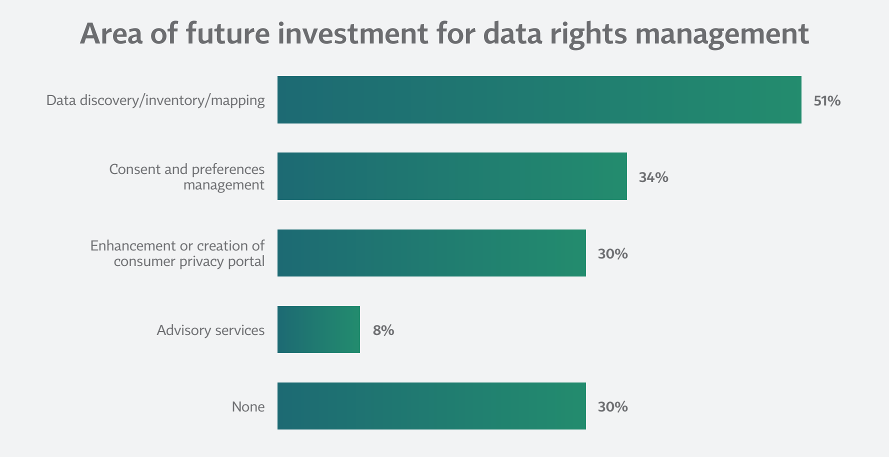
To drive this survey, we asked more than **475 privacy professionals** — in-house privacy professionals and in-house IT professionals — from around the world to examine current data rights practices through the organizational structure lens and how these practices may shift in the future.

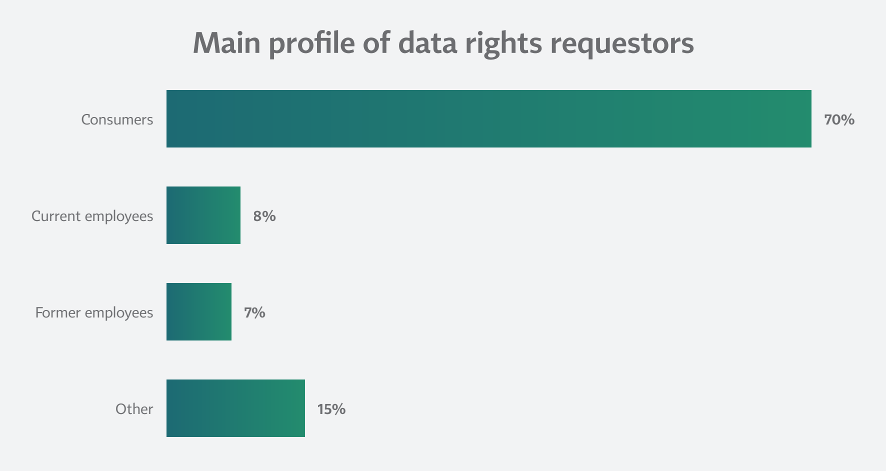
Executive Summary

Privacy and data protection laws around the world increasingly grant individuals the right to access, correct, restrict or delete their personal data. Article 15 of the EU General Data Protection Regulation and Sections 999.312 and 313 of the California Consumer Privacy Act, in particular, have prompted companies to develop more effective means of means of managing data rights and fulfilling data subject access requests, while prioritizing data transparency to their employees and consumers. To better understand these trends, the IAPP partnered with BigID to survey privacy professionals around the world on their DSAR practices and processes. This report summarizes the findings focusing on how companies approach data rights, how they currently track, process, and fulfill requests, and in which areas they intend to invest.

As companies look to the future, most respondents plan to invest in data rights tools and capabilities. Because personal and sensitive data is everywhere — in databases, file servers, mainframes, the cloud and data-in-motion applications — a strategic driver behind data rights investment is often integration with other business functions, including data governance, security, risk, compliance and legal processes.

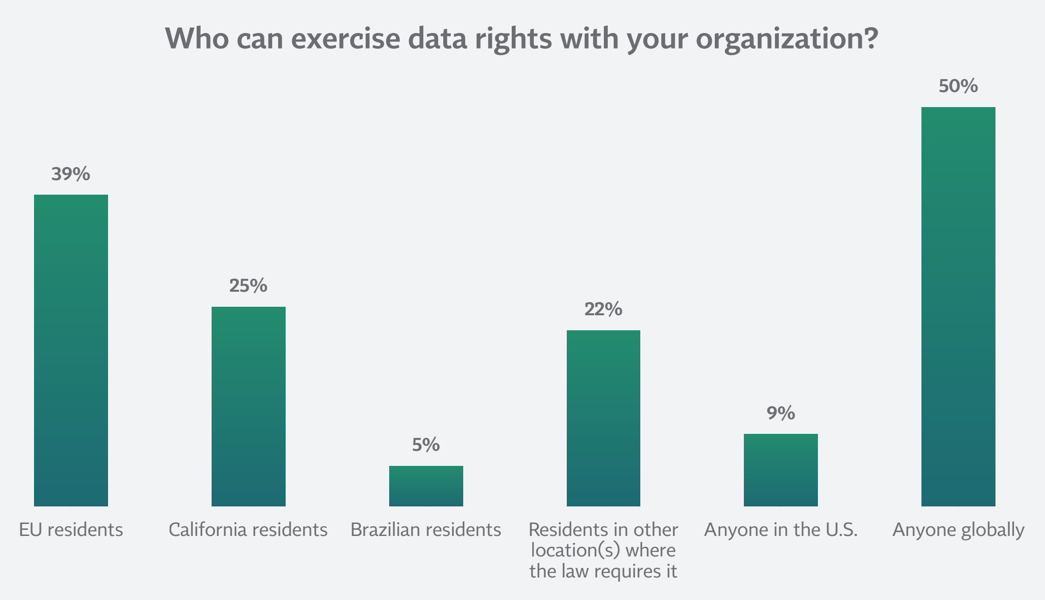
More than half of the respondents said they plan to invest in data discovery, including inventory and mapping. Other areas of planned investment include consent and preferences management capabilities and enhanced consumer privacy portals. Overall, companies in the U.S. plan to invest in data rights management resources more than those located in the rest of the world. This may reflect the relatively recent adoption of the CCPA, which brought with it new data rights obligations for companies and rights for consumers. If this is the main investment driver, we can expect similar investment around the world as many countries adopt or update data protection laws.

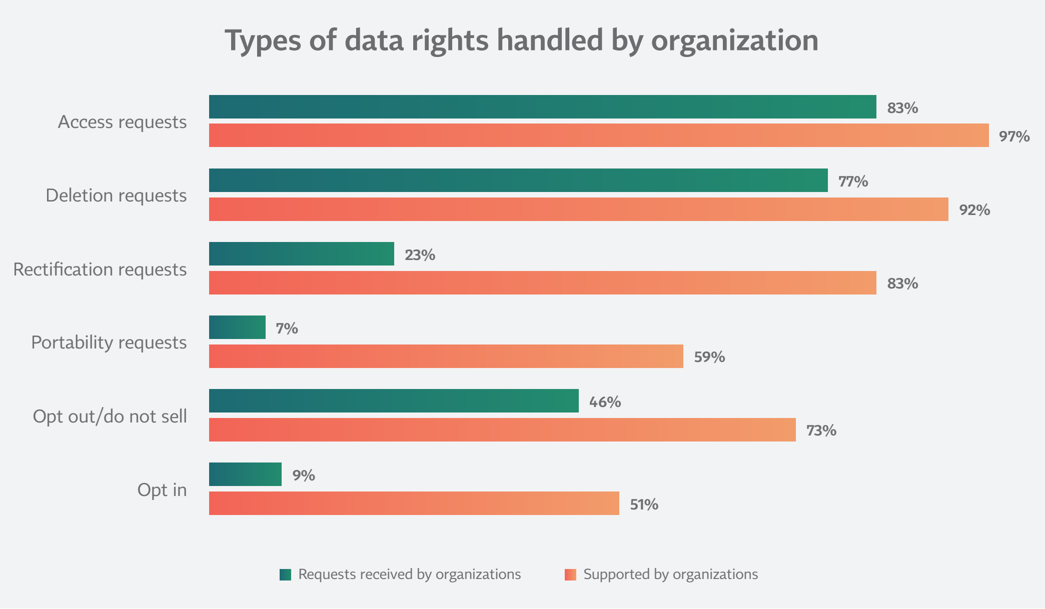




Companies most often refer to the action of consumers/data subjects exercising their rights for data/information as either "data subject access requests" or "data subject rights requests." While the specific terminology might seem insignificant, it points to different legal underpinnings across jurisdictions. Most of the organizations that responded using "data subject rights requests" are headquartered in the EU. **For the purposes of this report, we will use the term DSARs when talking about the broader practice of excercising and fulfilling data rights.**

Respondents reported the number of DSAR requests received in 2020 is either in line with or fewer than what companies expected. **The requests they receive overwhelmingly originated with consumers rather than employees.** This is especially true in the U.S. Employees of companies headquartered in the EU request personal data at a significantly higher rate than those employees of companies headquartered in other parts of the world.


Who can exercise data rights with your organization?


Types of data rights handled by organization

For nearly half of companies across the globe, DSAR management budgets are typically held by privacy departments, and most (70%) respondents reported having fewer than six personnel dedicated to the DSAR function.

Global companies receive DSARs from around the world and must decide whether to grant equivalent data rights — including access requests, deletion, and more — across the board or respond according to the rules in each jurisdiction. **Half of the respondents stated anyone globally can exercise data subject rights with their organizations.** Organizations headquartered outside of the U.S. were more likely to adopt this global approach than their U.S. counterparts. Companies in the U.S. focus significantly more on requests from California residents.

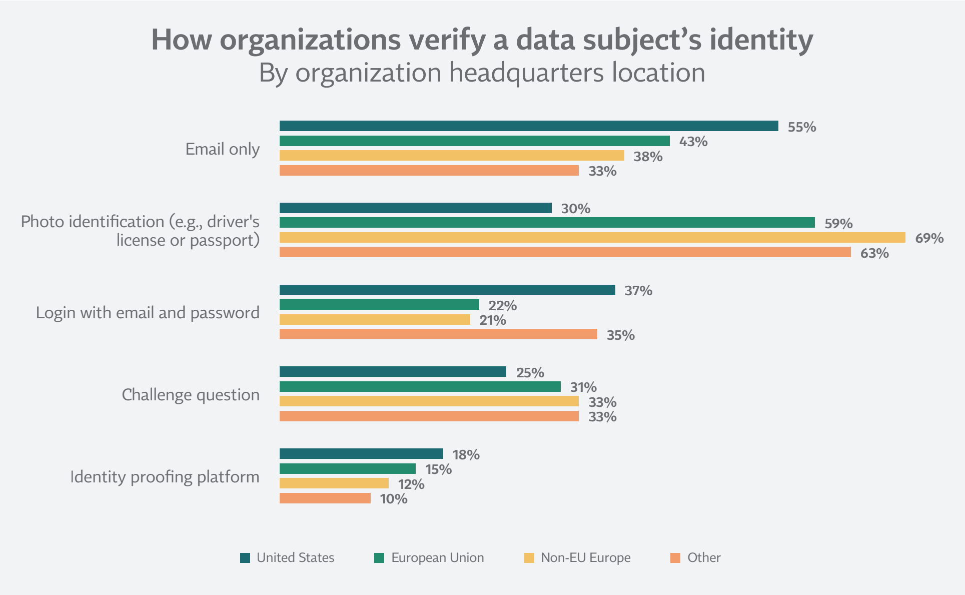
Organizations receive and support all types of DSARs — access, deletion, rectification, portability, opt in, and opt out/do not sell. **Companies reported access and deletion requests are the most common type of requests received, while opt-in requests are the least common.**

Most organizations continue to manage data rights manually and via a front-end portal or similar submission form. Nearly half of organizations process requests by phone or via email. In the U.S., companies process requests more often through either an in-house self-service online portal or a third-party privacy portal.

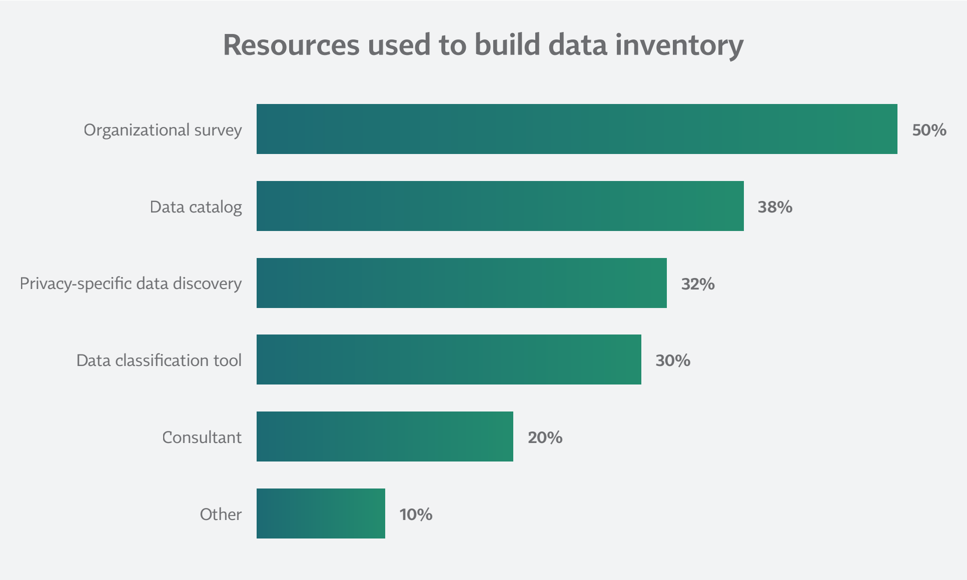
Companies have adopted a variety of different approaches to verify a data subject's identity. No single method rose to the top of the list. Confirming an email account or requesting a photo identification are common tactics. **Companies located outside of the U.S. use photo identification significantly more often. U.S.-based companies frequently rely on either email or login information.**

When responding to individuals, more than 60% of the respondents provide the requestor a summary report illustrating the type of data the organizations holds, and 57% provide the actual records. A lower percentage of respondents provide the requestor proof of deletion, detailed reports of data type, and location and consent summaries. When asked about the type of information included in the summary reports companies provide, respondents indicated basic personally identifiable information is included most often. Those companies located in the EU report official documents, like health and financial data, significantly more often than those companies in the U.S.

To locate data responsive to an individual request, companies typically search databases, applications and cloud storage systems. **Half of respondents indicated they use surveys to build their data inventories, while about 30% use data catalogs, privacy specific data discovery or data classification tools either together or separately.** Organizations deploy a combination of approaches to correlate this data to a certain identity, including manually searching for a keyword (email or name), performing a targeted query on a table or application programming interface, or using a privacy tool that was built for this purpose.


How organizations verify a data subject's identity

By organization headquarters location

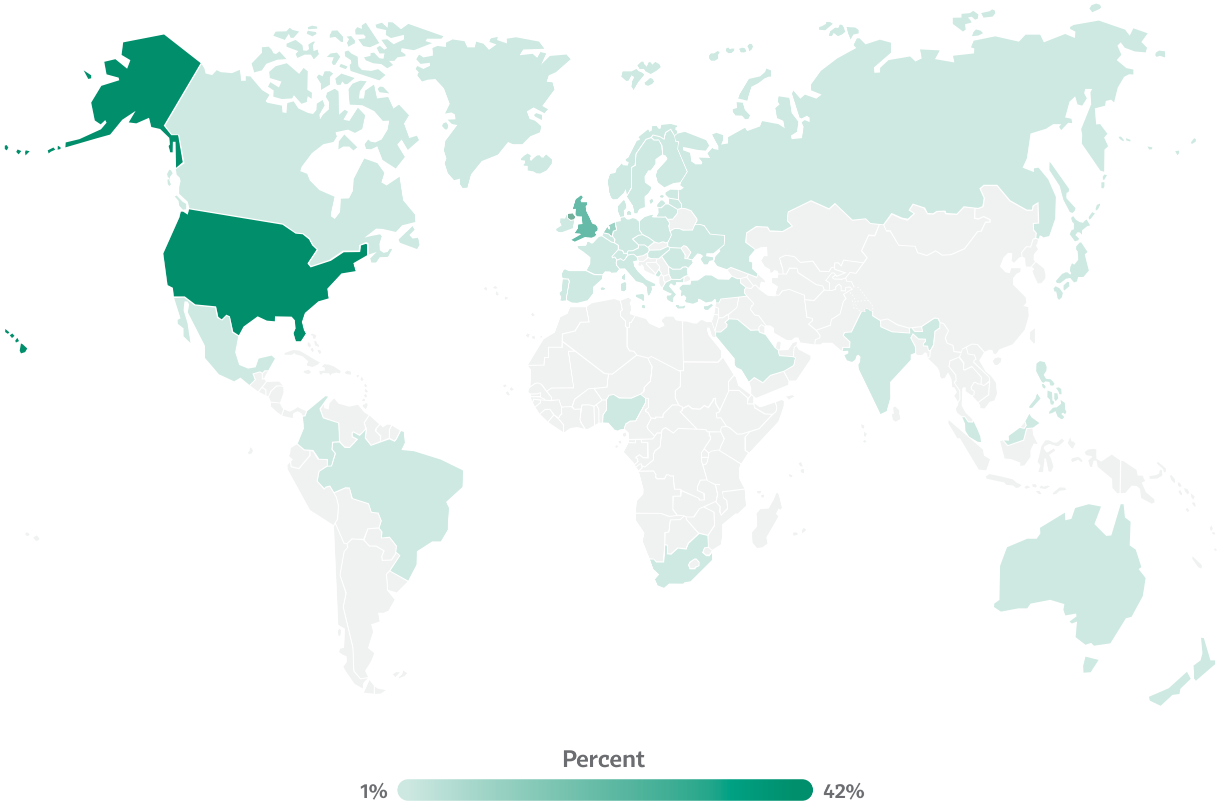

Resources used to build data inventory

Companies must be ready to effectively process and manage data rights as new privacy and data protection laws are enacted around the globe and individuals become more educated on their rights to access, delete and correct their personal data. The findings from this survey will help companies prepare for this potential increase in demand by understanding common data rights management practices today and future investment strategies.

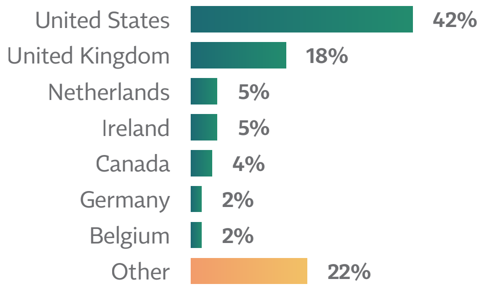
Respondent Demographics

Nearly half of the respondents are from North America and work for organizations located in the U.S. A third of the respondents work for organizations headquartered in the EU.

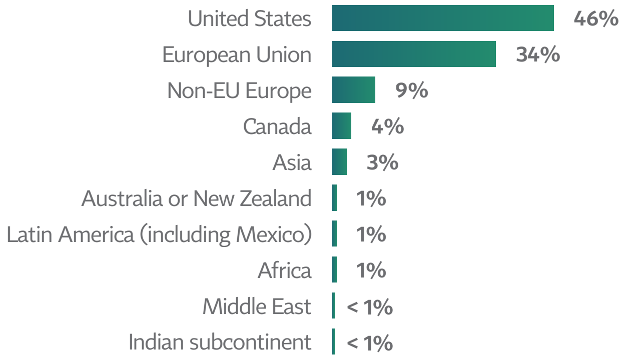
Global distribution of survey respondents



Distribution of respondents' location

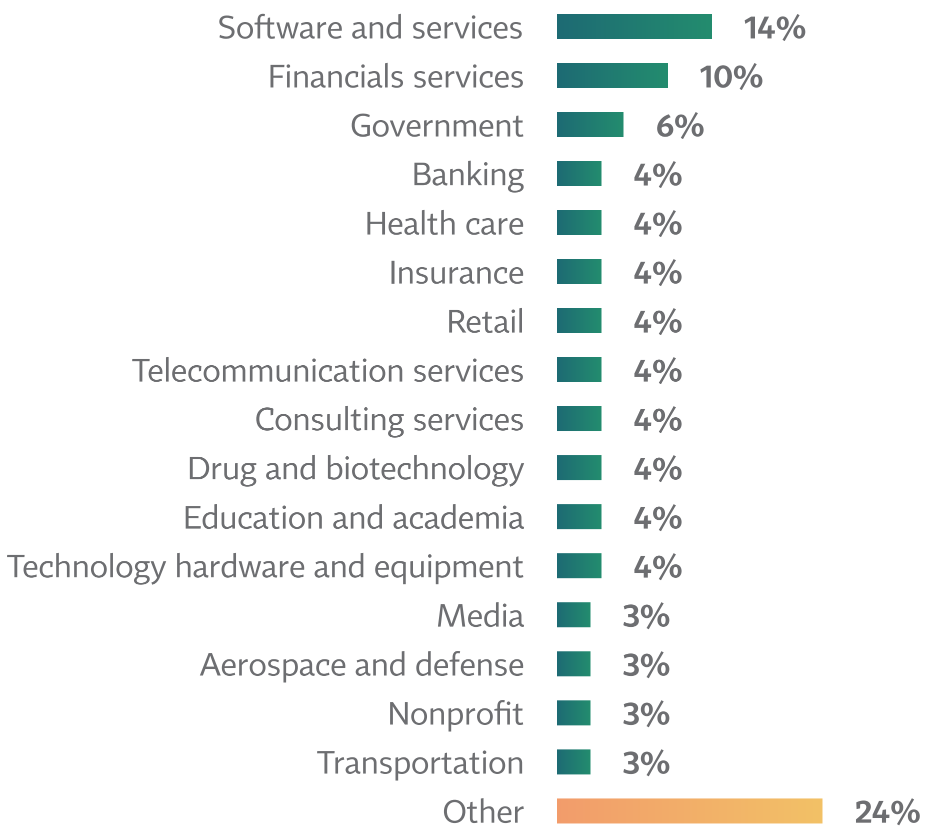


Distribution of organization HQ

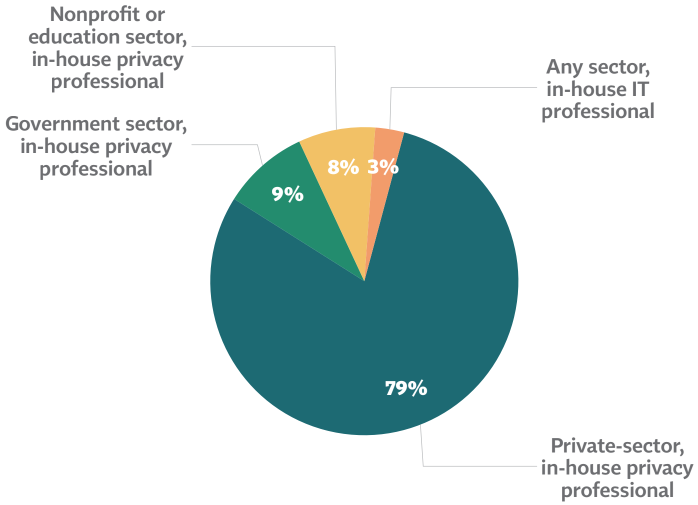


Most respondents are in-house privacy professionals in the private sector, from a balanced mix of industries and organizations of all sizes.

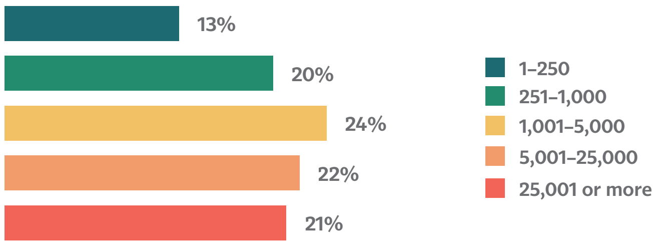
Industry



Current position



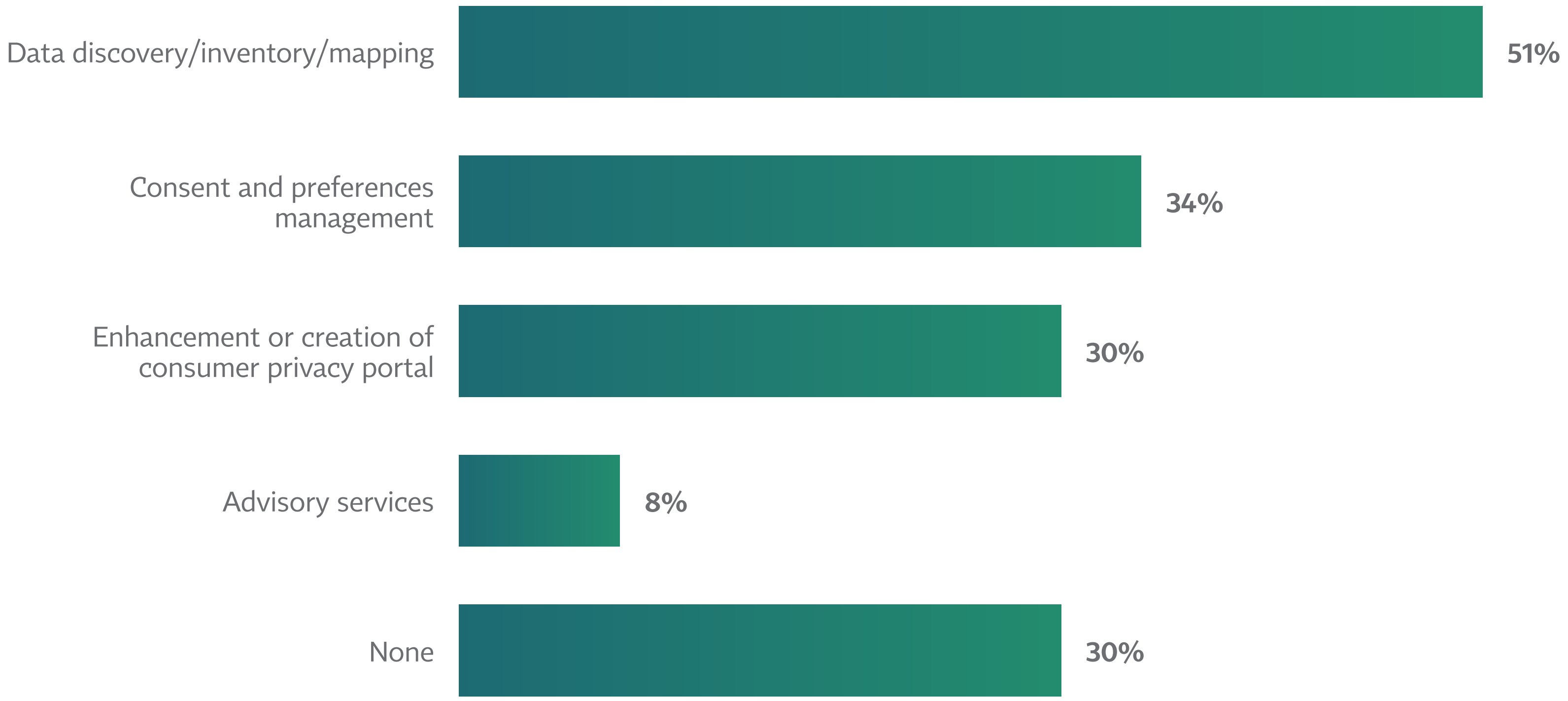
Size of organization



Survey Findings: Data rights investment priorities and metrics

Half of the respondents indicated that data discovery/inventory/mapping is the top area for additional future data rights investments. A third of the companies also plan to invest in consent and preferences management and enhancement of a consumer privacy portal.

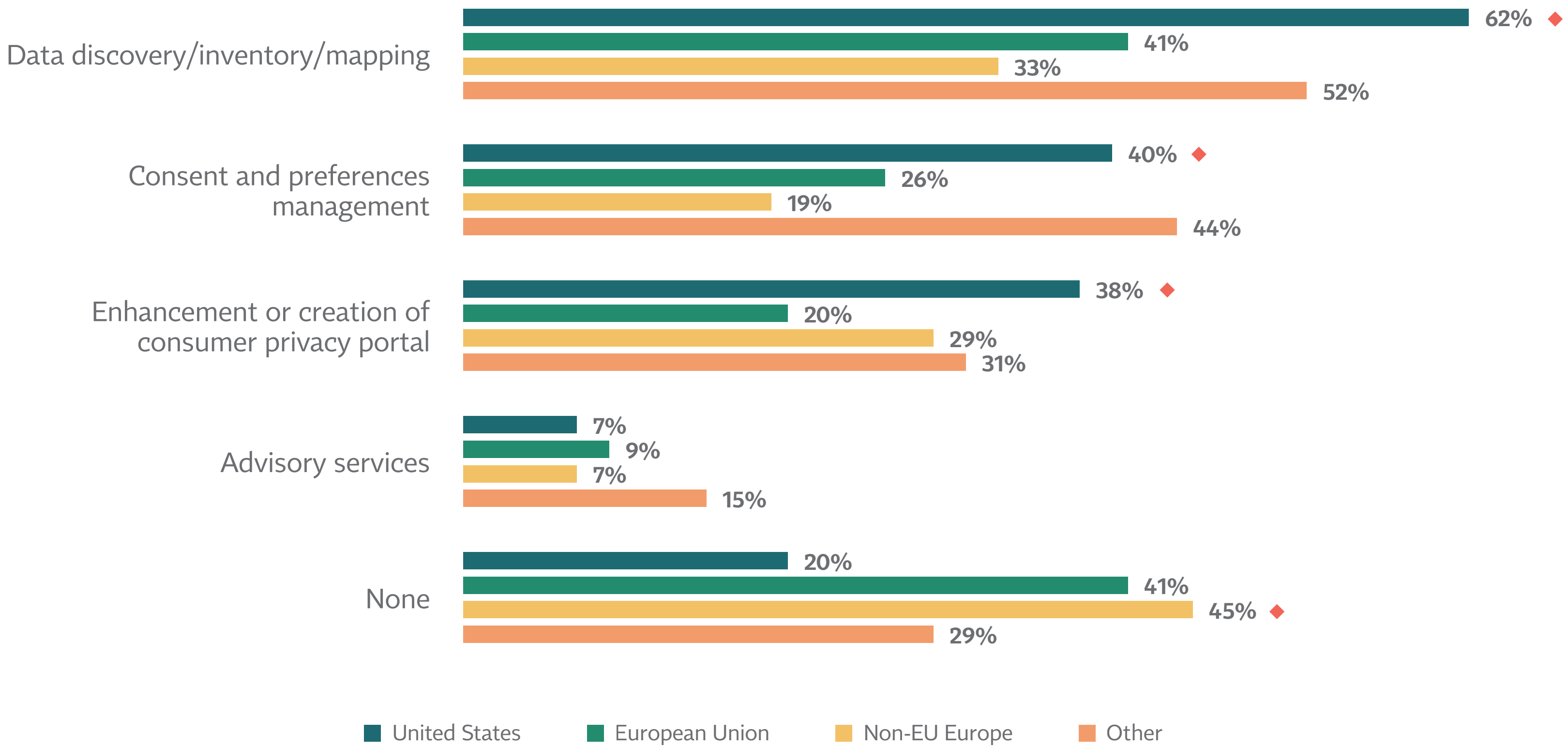
Areas of future investment for data rights management resources



Overall, U.S.-based companies are more likely to be investing in data rights management resources in the future.

Areas of future investment for data rights management resources

By organization HQ location

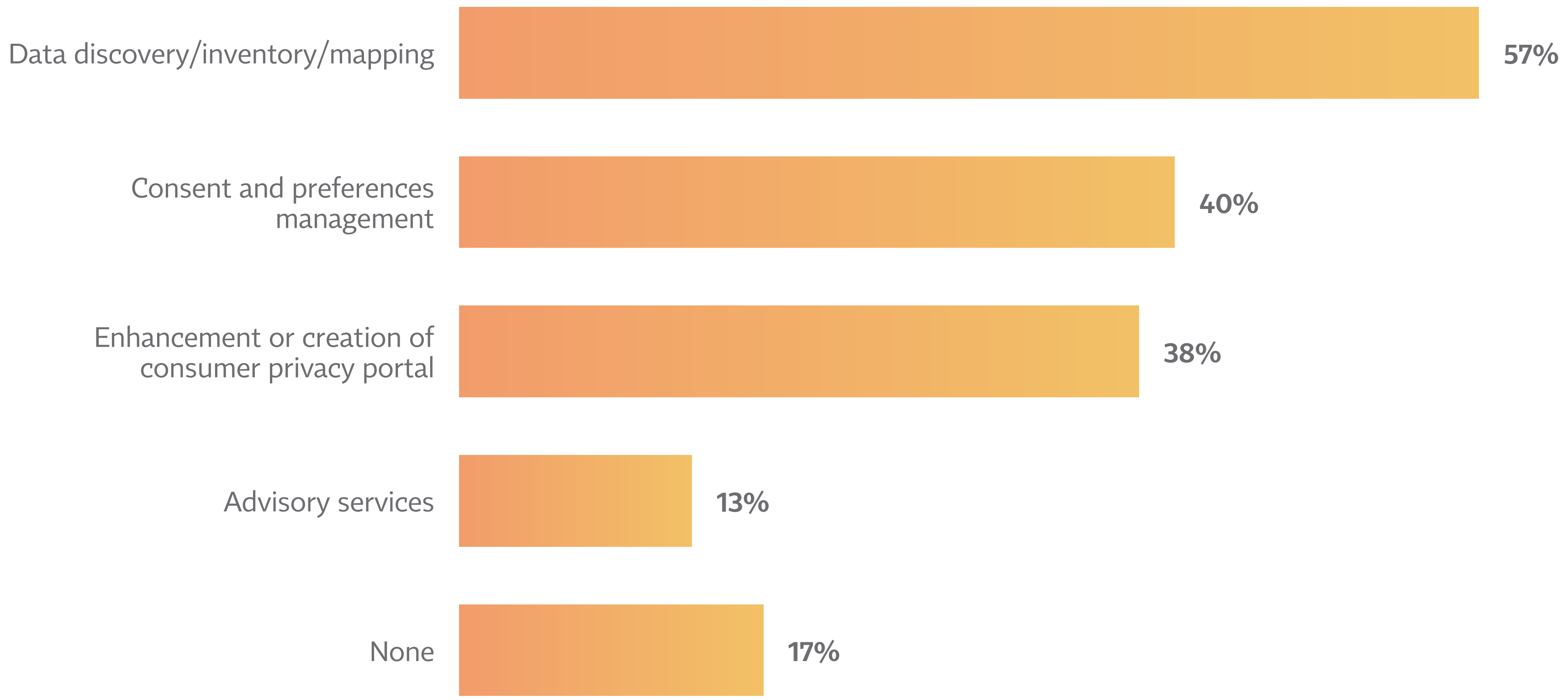


◆ *Indicates a statistically signigicant difference.*

Nearly 60% of organizations in the financial services sector are prioritizing data discovery, inventory and mapping as an area of future data rights management investment.

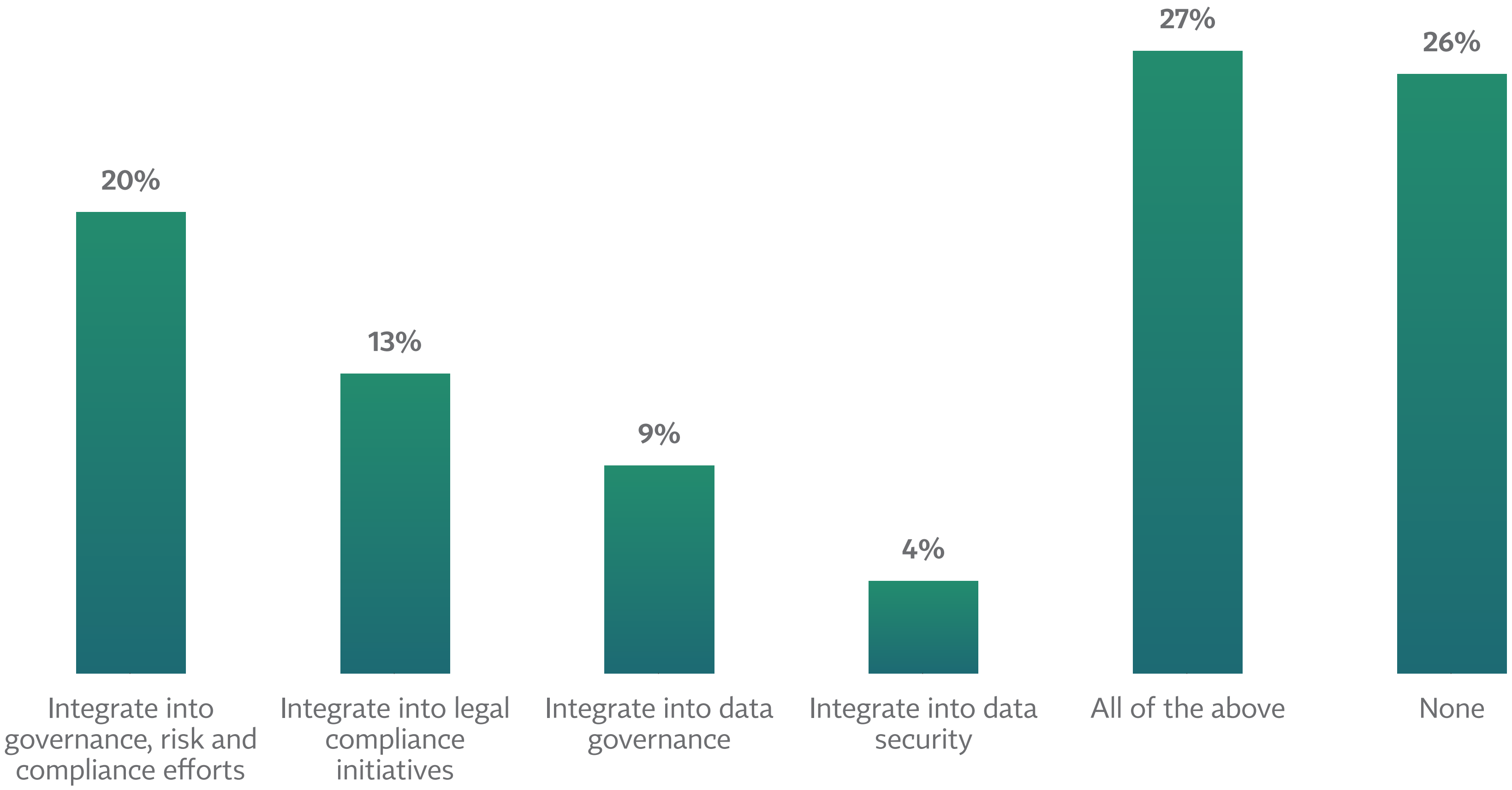
Areas of future investment for data rights management resources

In the financial services industry



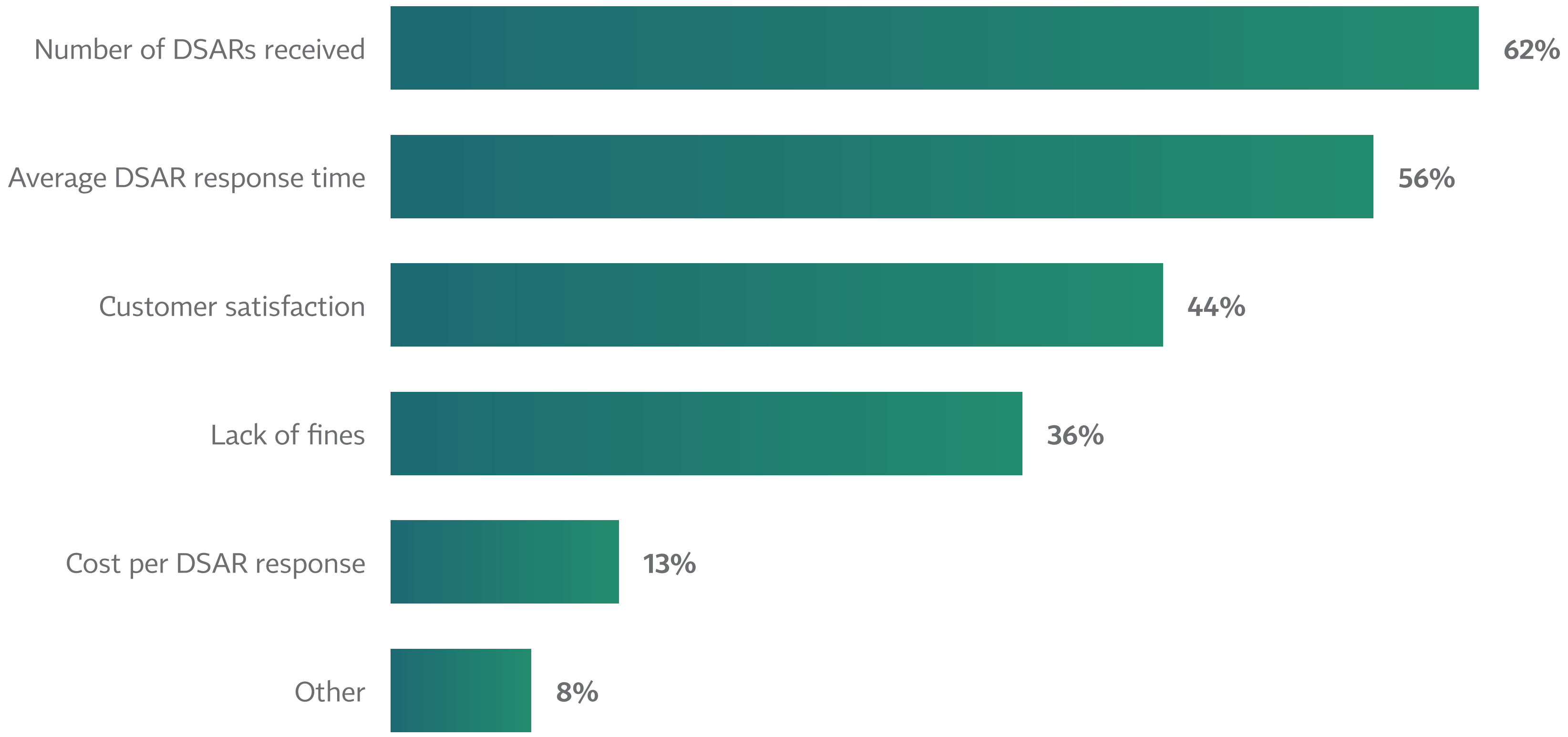
Organizations reported that data rights investments will support a wide range of initiatives, including governance, risk, compliance and security efforts.

Strategic drivers behind planned data rights management investment



The number of requests received and average response time are the top metrics companies use when measuring the success of their data rights strategy investments.

Metrics used to measure the success of data rights strategy investments



Organizations with more than 600 requests in the past year responded they also use customer satisfaction and the lack of fines to measure success.

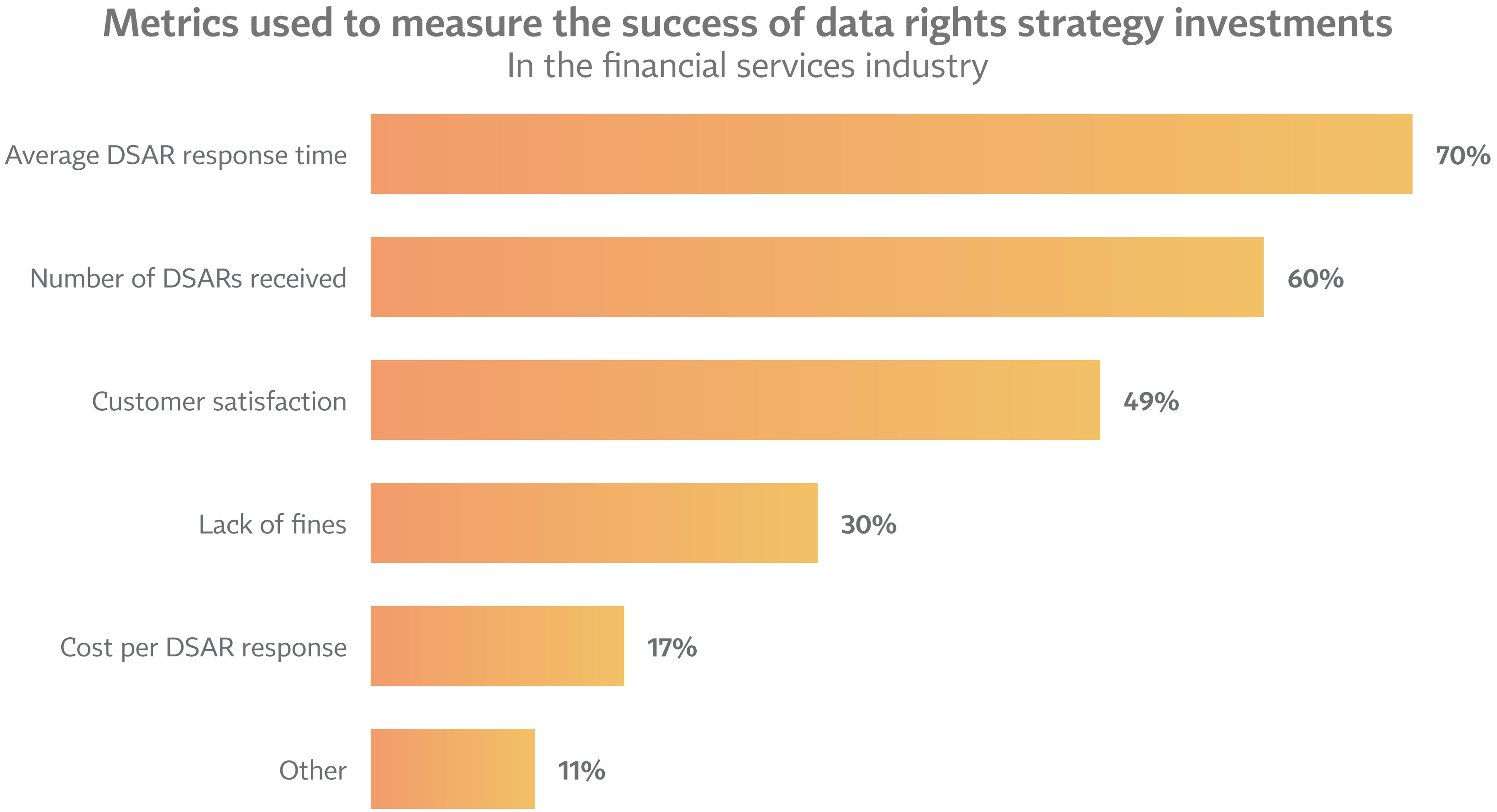
Metrics used to measure the success of data rights strategy investments

By number of requests

METRICS TO MEASURE SUCCESS OF DSAR STRATEGY INVESTMENTS	NUMBER OF DSARS RECEIVED OVER THE PAST YEAR						
	0	**1–25**	**26–75**	**76–300**	**301–600**	**601–1,000**	**More than 1,000**
Number of DSARs received	58%	59%	62%	60%	78%	68%	61%
Average DSAR response time	26%	49%	51%	**62%**	**75%**	**75%**	**64%**
Customer satisfaction	58%	37%	43%	46%	28%	61%	**58%**
Lack of fines	26%	30%	34%	35%	36%	**57%**	48%
Cost per DSAR response	11%	13%	15%	17%	3%	18%	13%
Other	0%	11%	10%	7%	11%	0%	3%

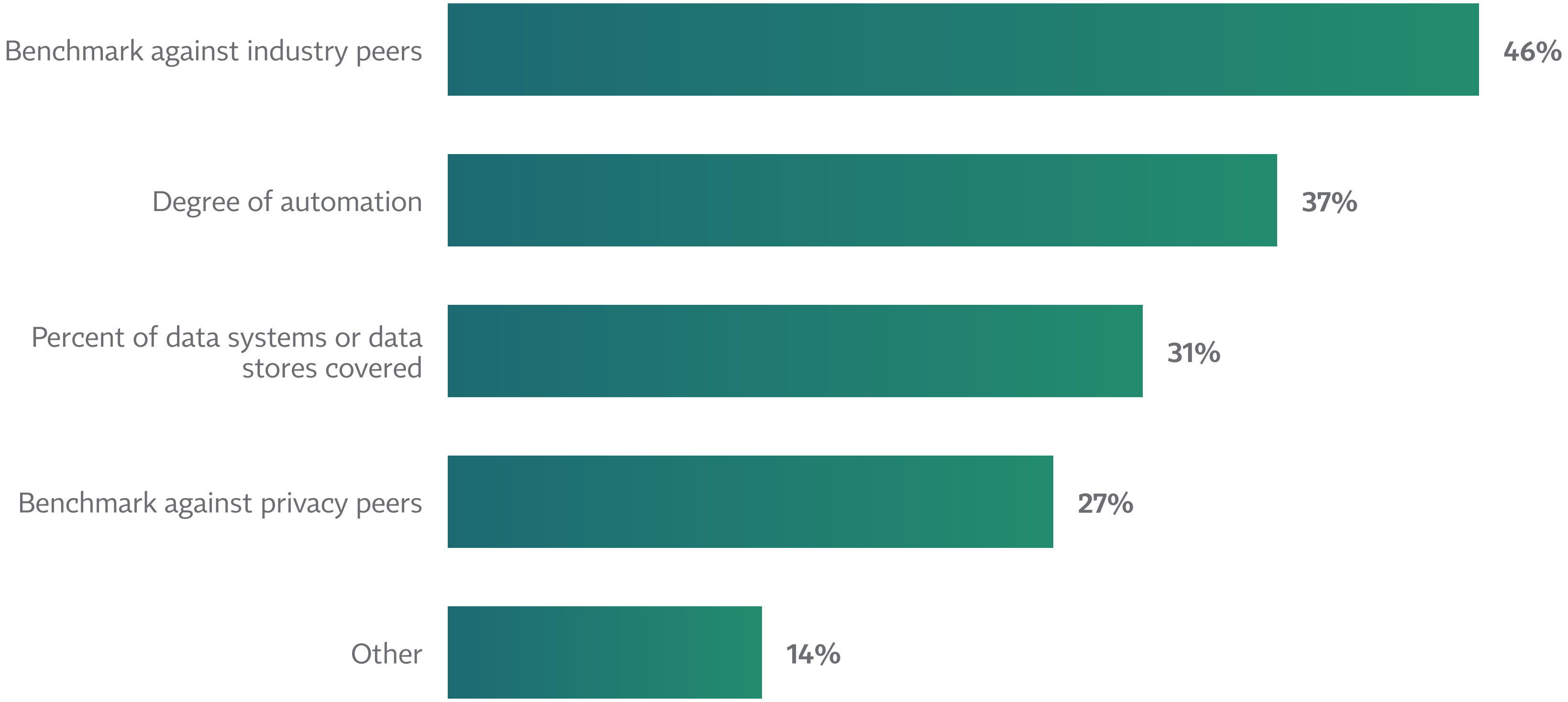
Statistically significant difference.

Most organizations in the financial services sector place DSAR response time as their top measure of success of their data rights investment, more than the number of DSARs received — a reverse from the overall trend.



Nearly half of the organizations plan to measure the maturity of their data rights management program by benchmarking against industry peers, followed closely by measuring the degree to which their program is automated.

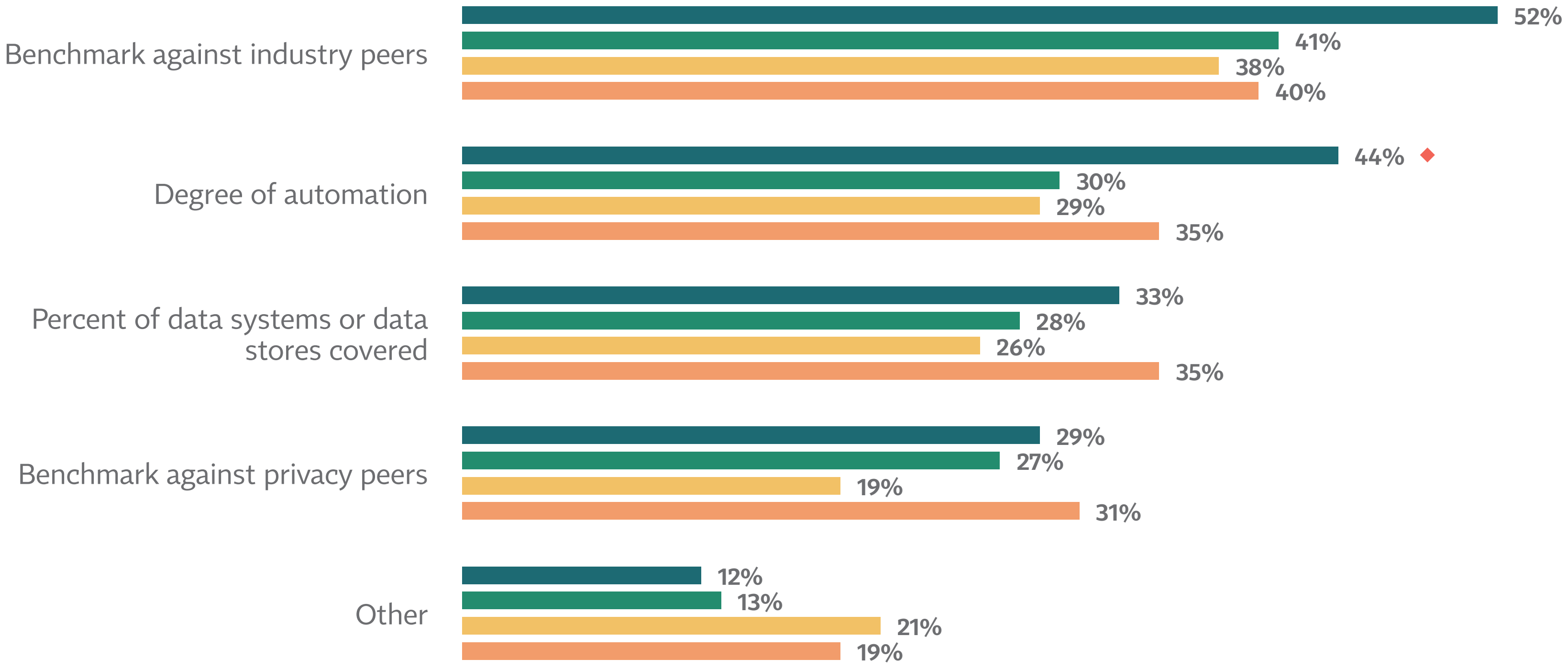
Metrics companies plan to use to measure the maturity of data rights management program



Organizations headquartered in the U.S. plan to use the metric “degree of automation” significantly more than those in the EU.

Metrics companies plan to use to measure the maturity of data rights management program

By organization HQ location



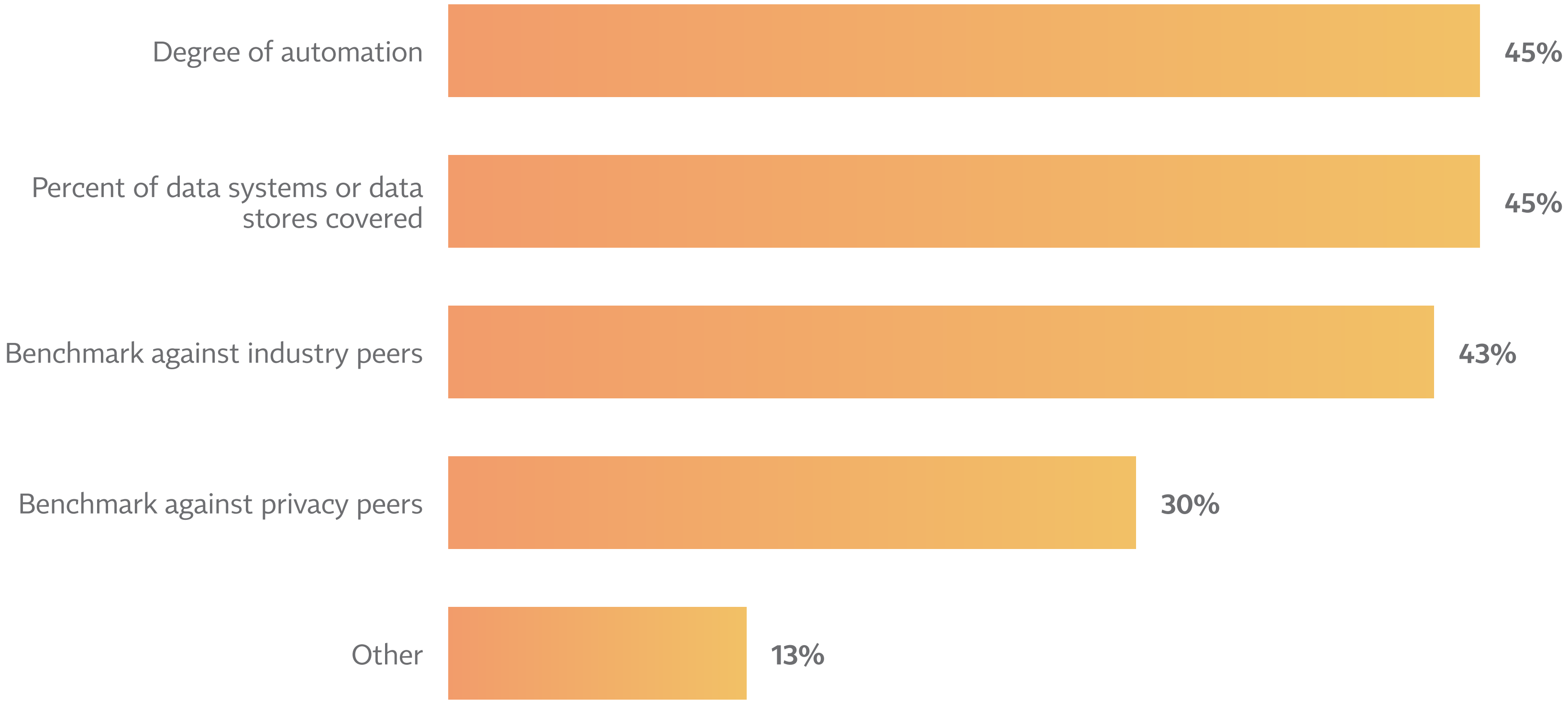
■ United States ■ European Union ■ Non-EU Europe ■ Other

◆ *Indicates a statistically signigicant difference.*

In the financial services industry, nearly half of the organizations mention that the degree of automation and percent of data systems/stores covered will be the top metrics to measure the maturity of their data rights management program.

Metrics companies plan to use to measure the maturity of data rights management program

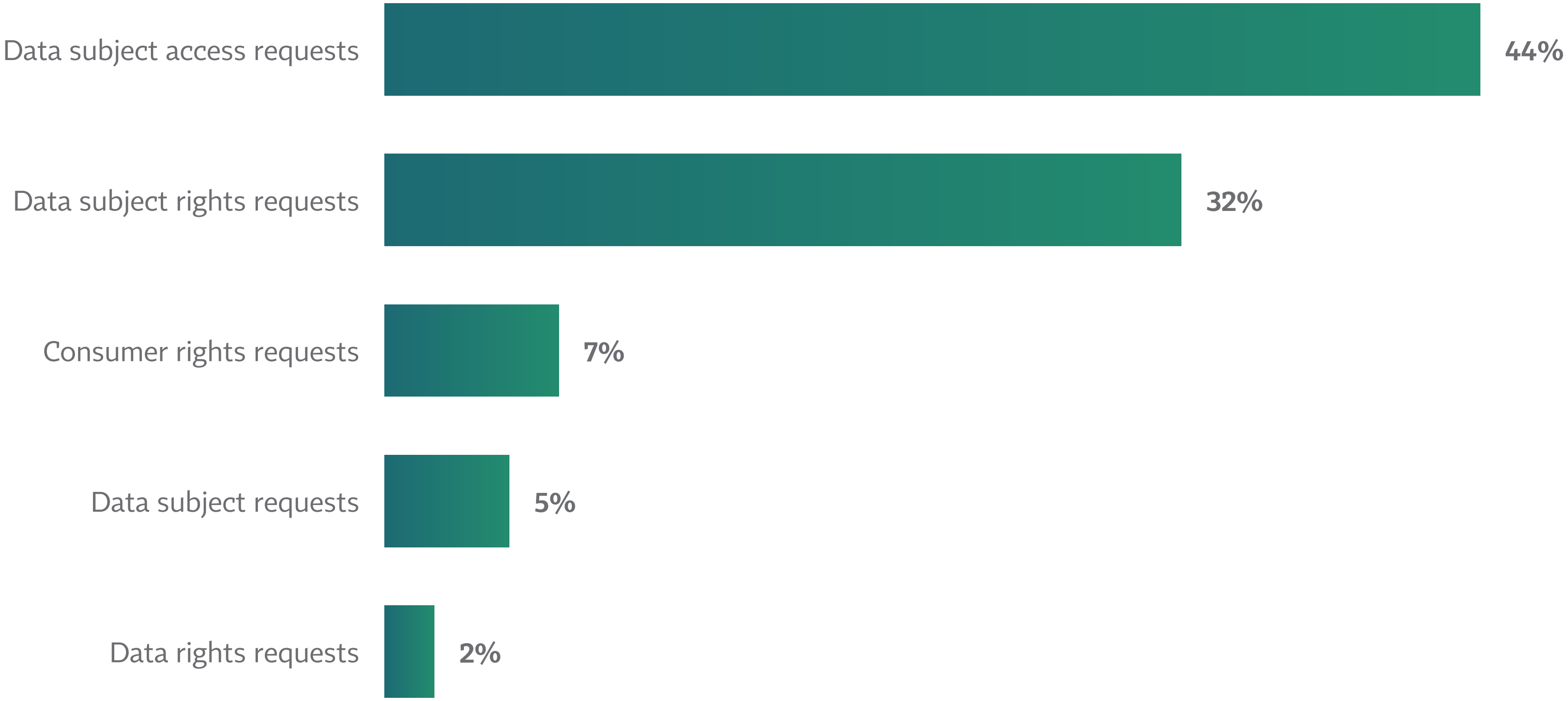
In the financial services industry



Survey Findings:
Data rights defined, why they matter and who addresses them

Four out of 10 organizations use the term "data subject access requests," while a third use "data subject rights requests."

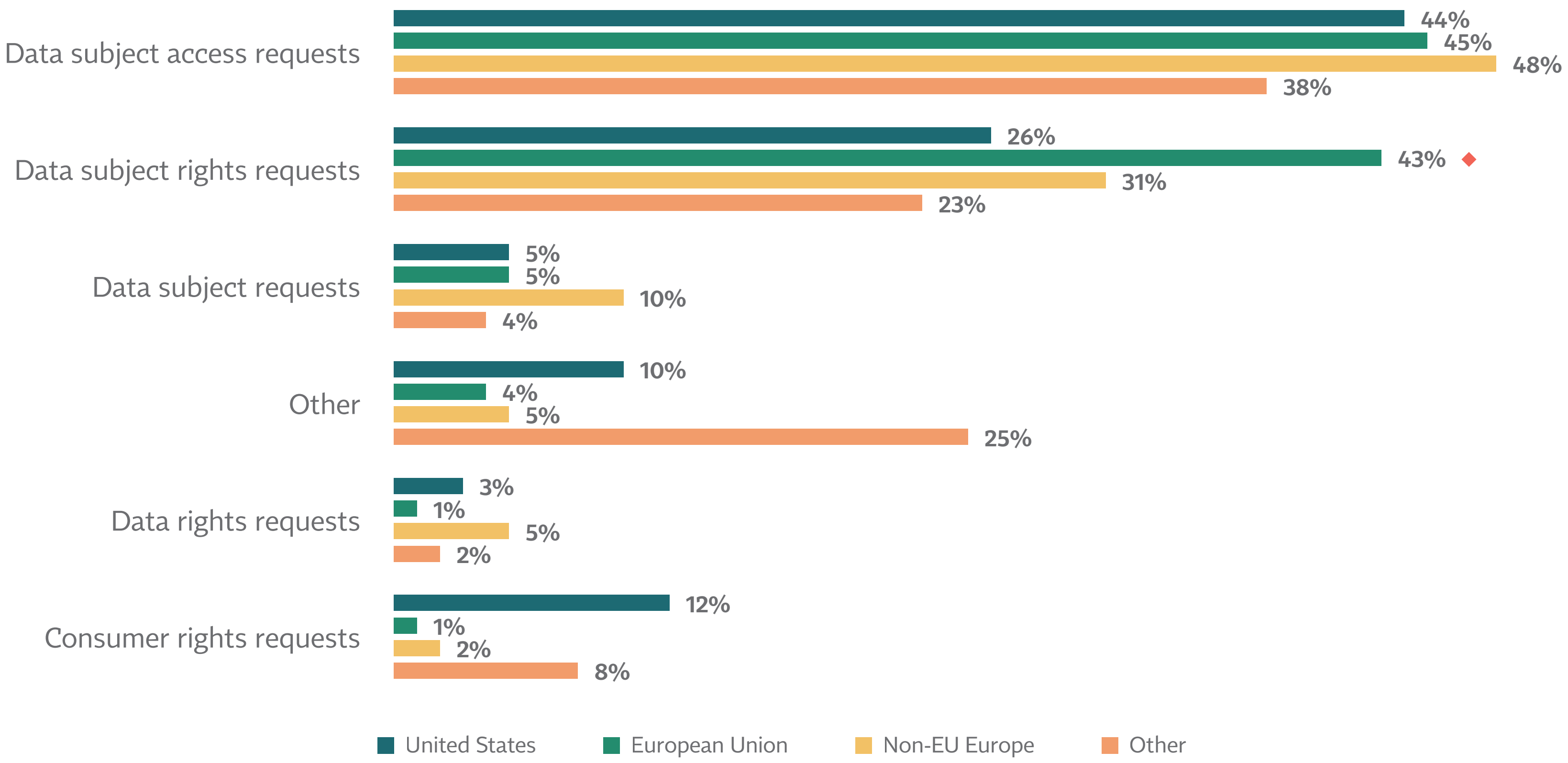
Terminology most often used to define consumers/data subjects exercising their rights for data/information



Most of the organizations using “data subject rights requests” are headquartered in the EU.

Terminology most often used to define consumers/data subjects exercising their rights for data/information

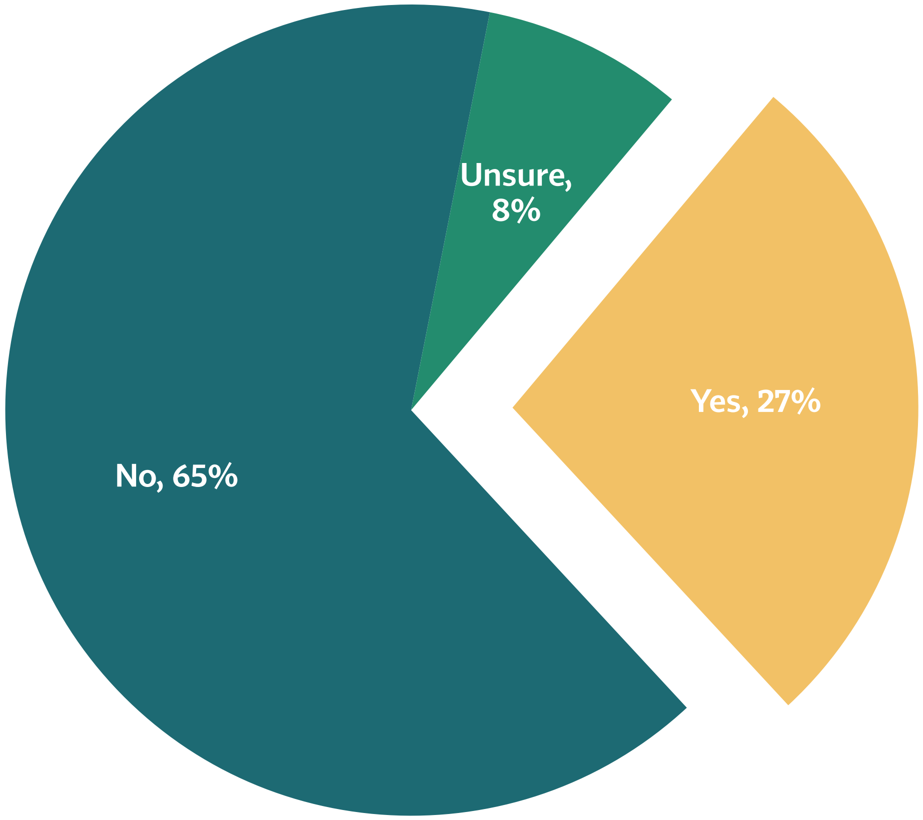
By organization HQ location



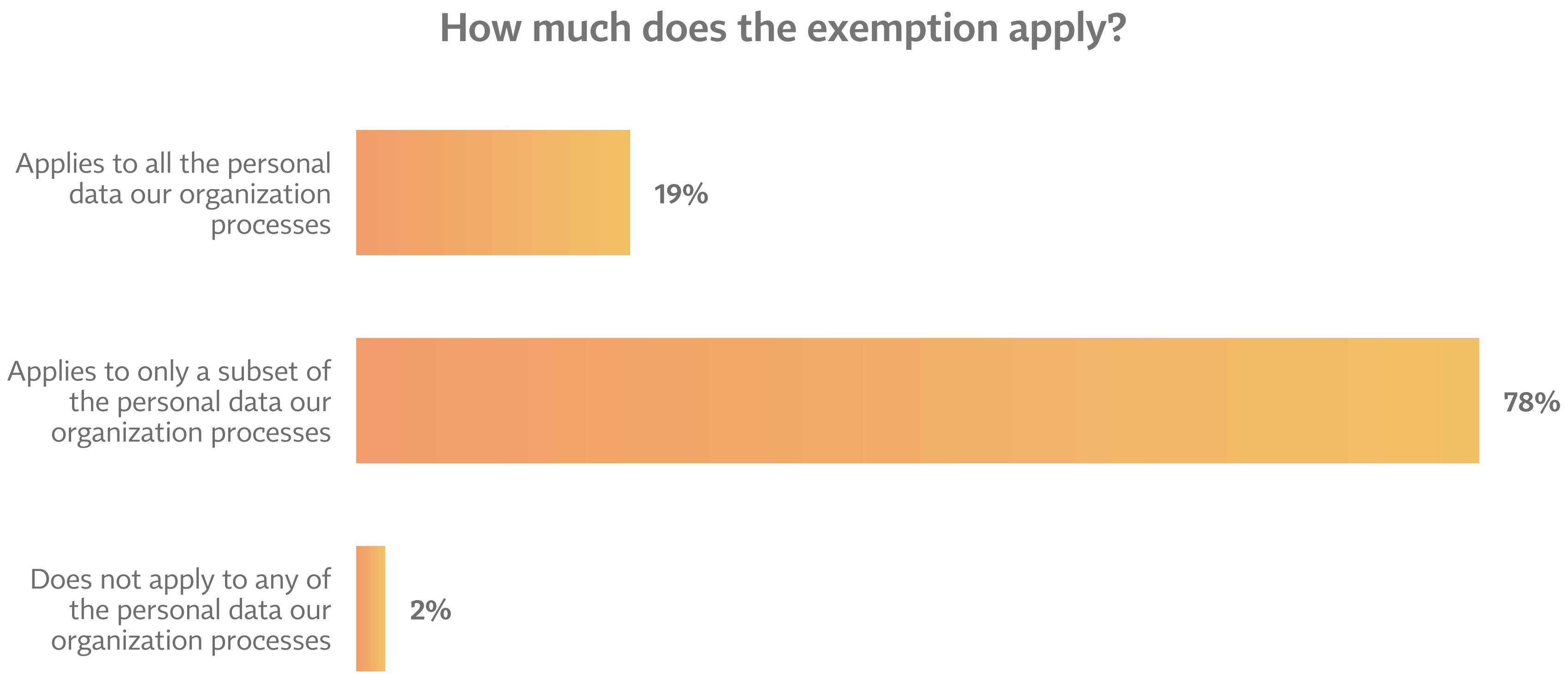
◆ *Indicates a statistically signigicant difference.*

A quarter of the respondents work in industries with legal exemptions related to fulfilling DSARs under privacy/data protection laws.

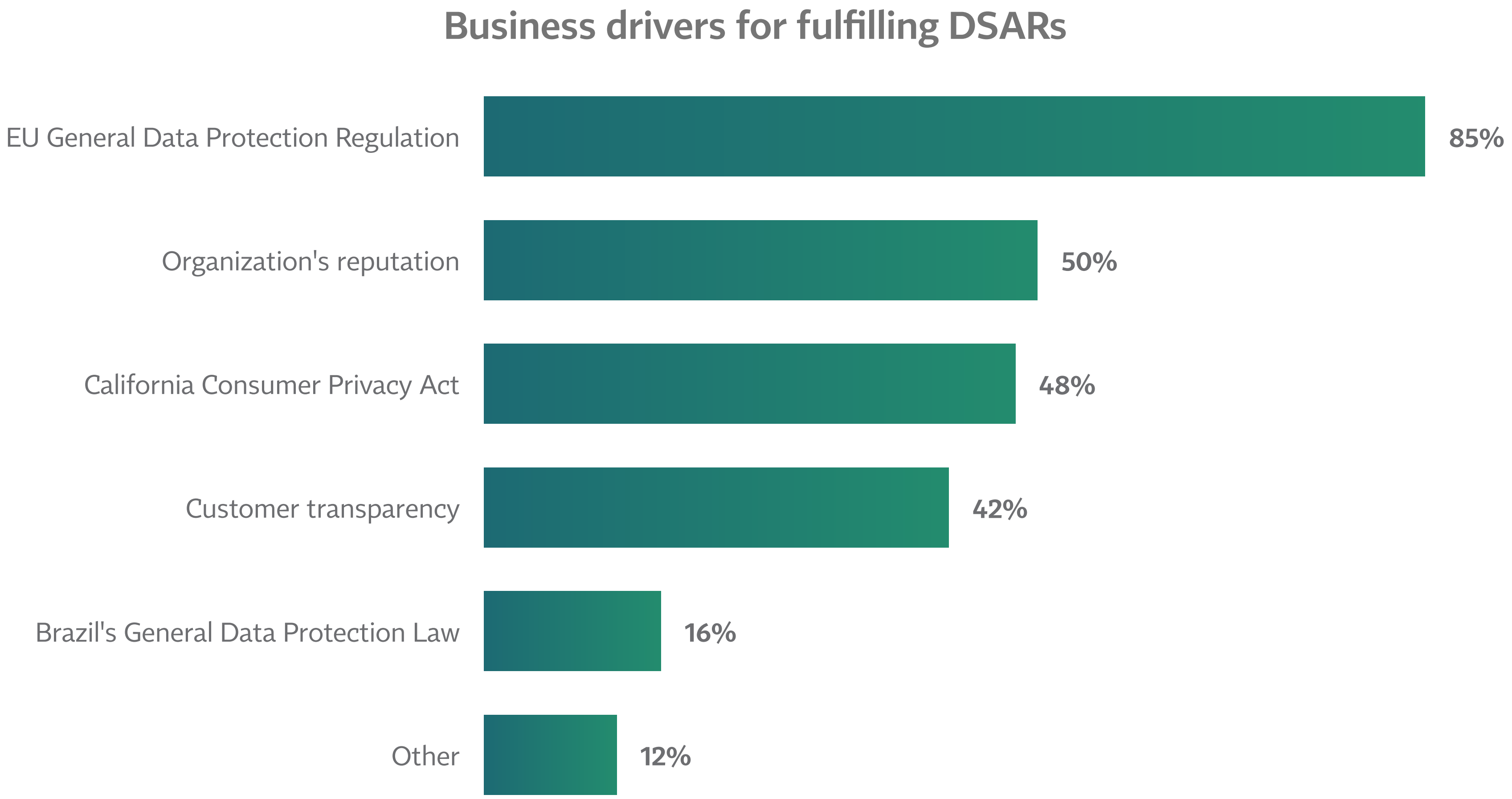
Work in industry where there are legal exemptions for fulfilling DSARs



Of the 27% of companies who replied they work in an industry with legal exemptions, most of the respondents said these exemptions apply only to a subset of the personal data they processes.



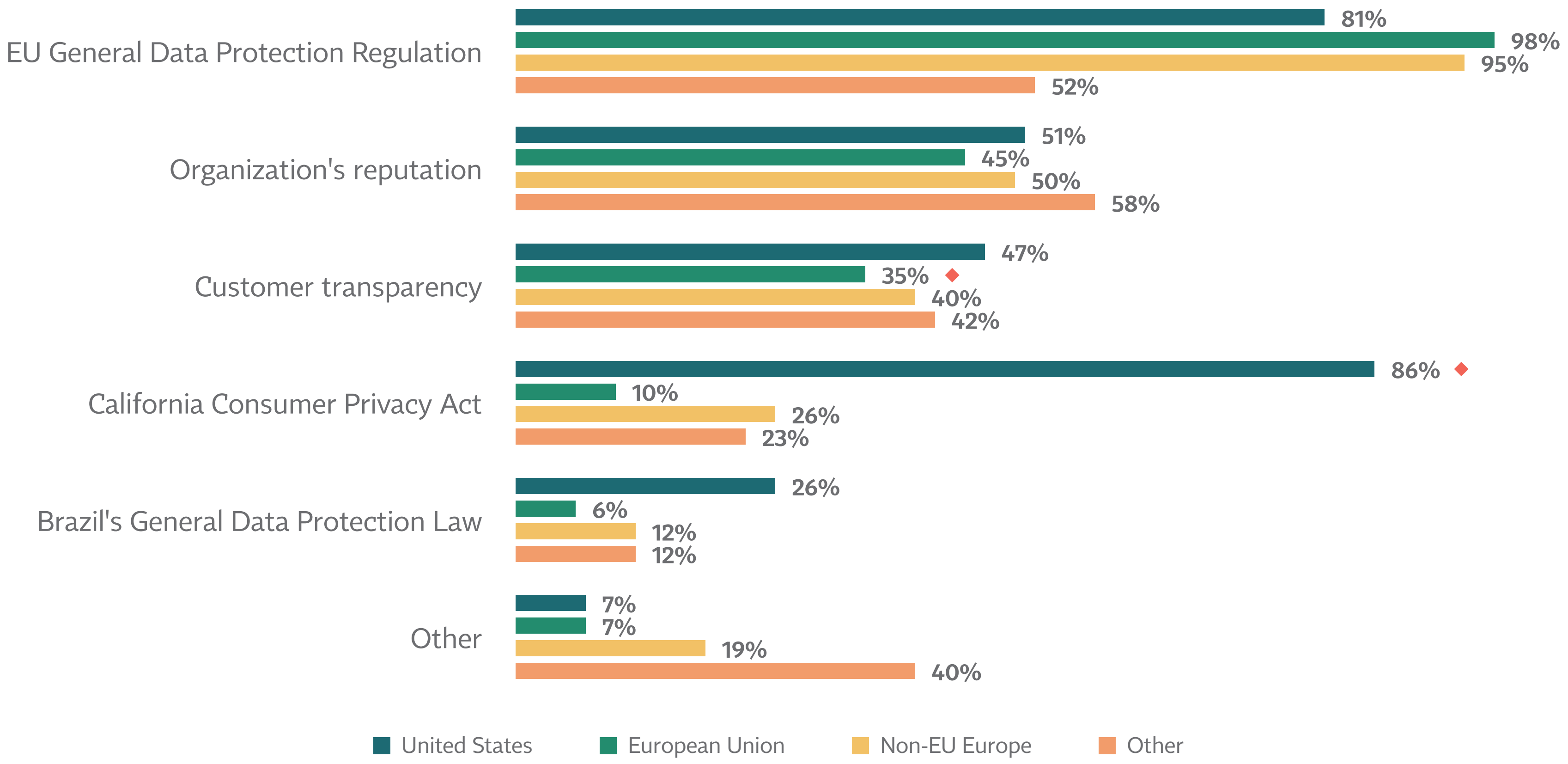
Overall, the GDPR is the major business driver for fulfilling DSARs, followed by maintaining an organization's reputation and CCPA compliance.



Business drivers for fulfilling DSARs are relatively uniform across regions, with the CCPA as the major exception, which is far more relevant for U.S. organizations.

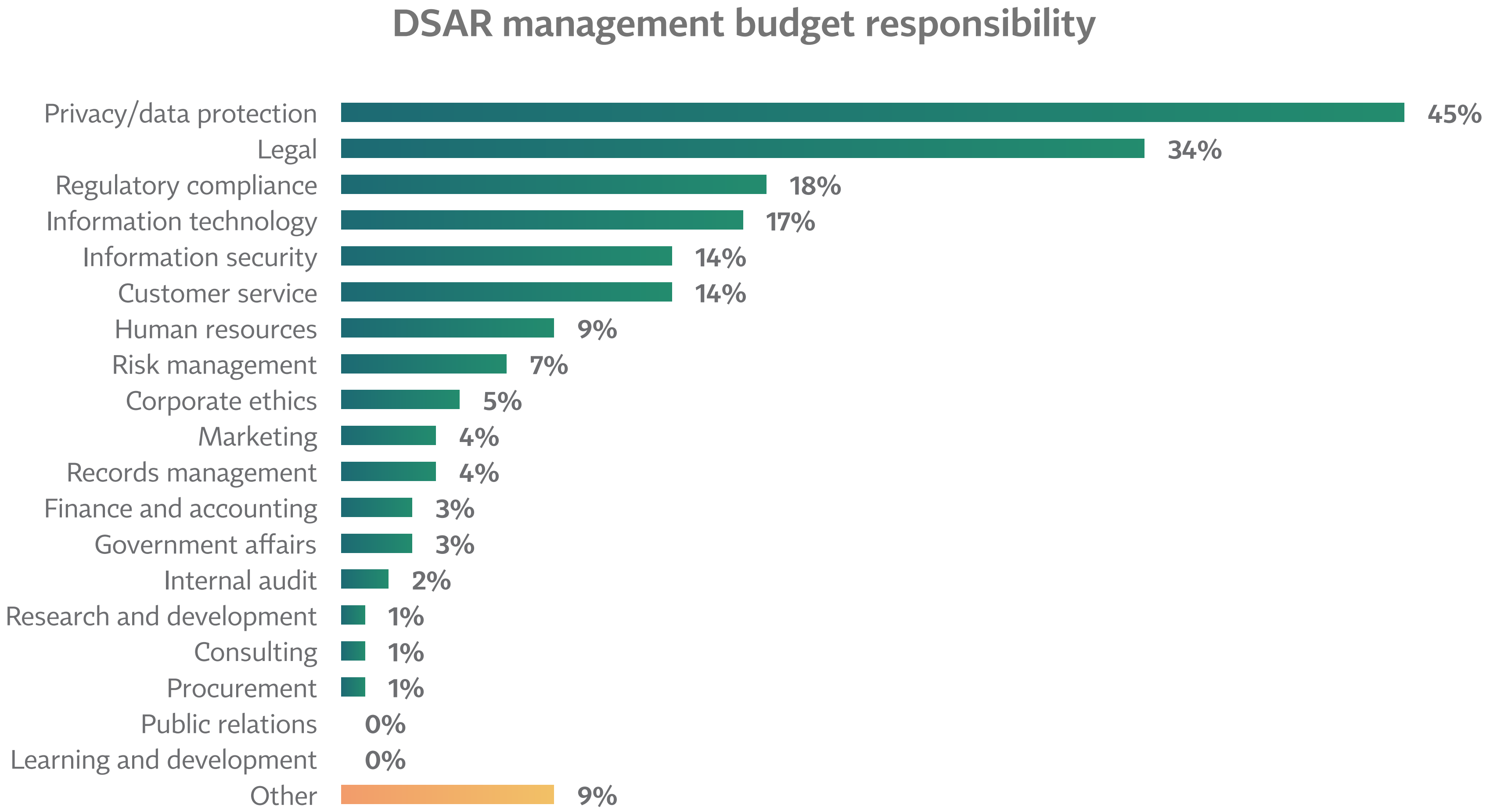
Business drivers for fulfilling DSARs

By organization HQ location



◆ *Indicates a statistically signigicant difference.*

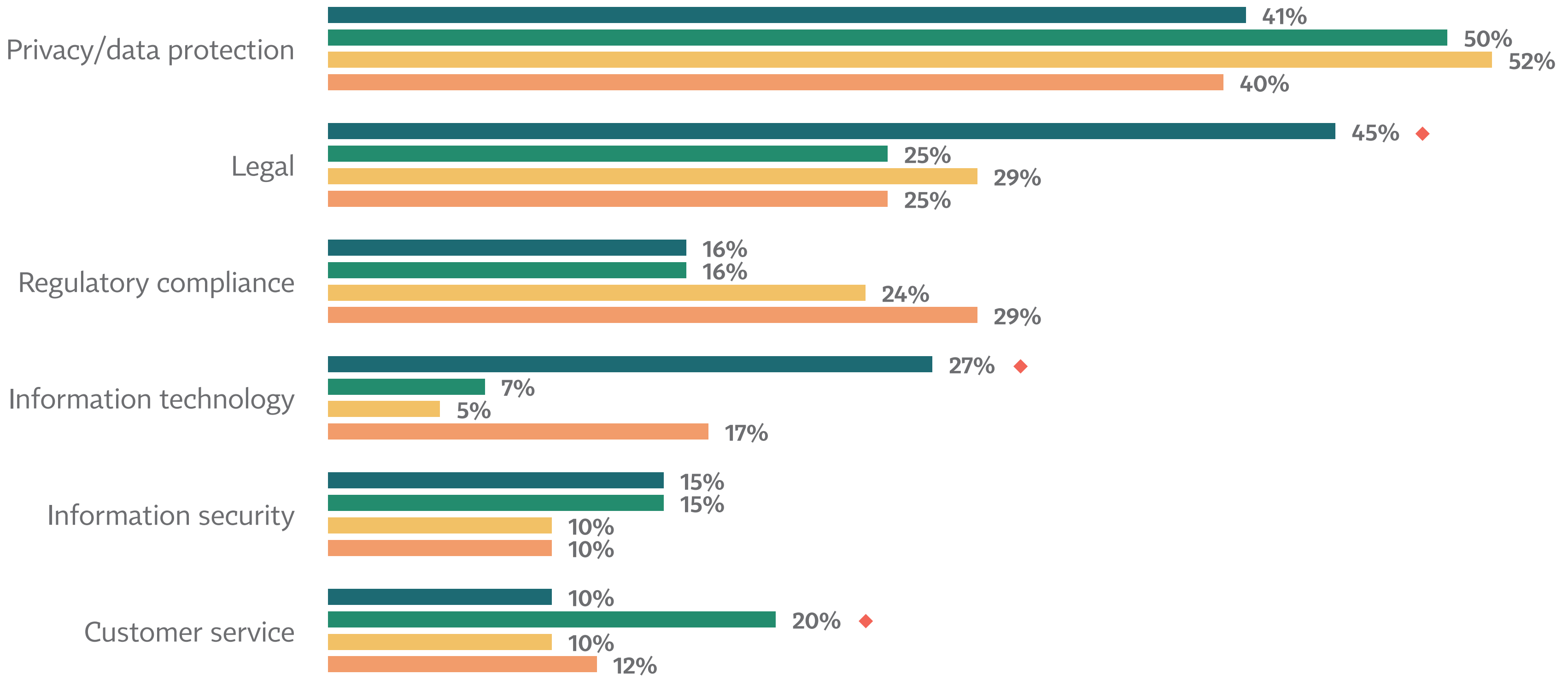
Nearly half of companies across the globe report DSAR management budgets are held by privacy departments.



Companies headquartered in the U.S. report budgets in legal and IT departments at a significantly higher rate than those headquartered in other regions.

DSAR management budget responsibility

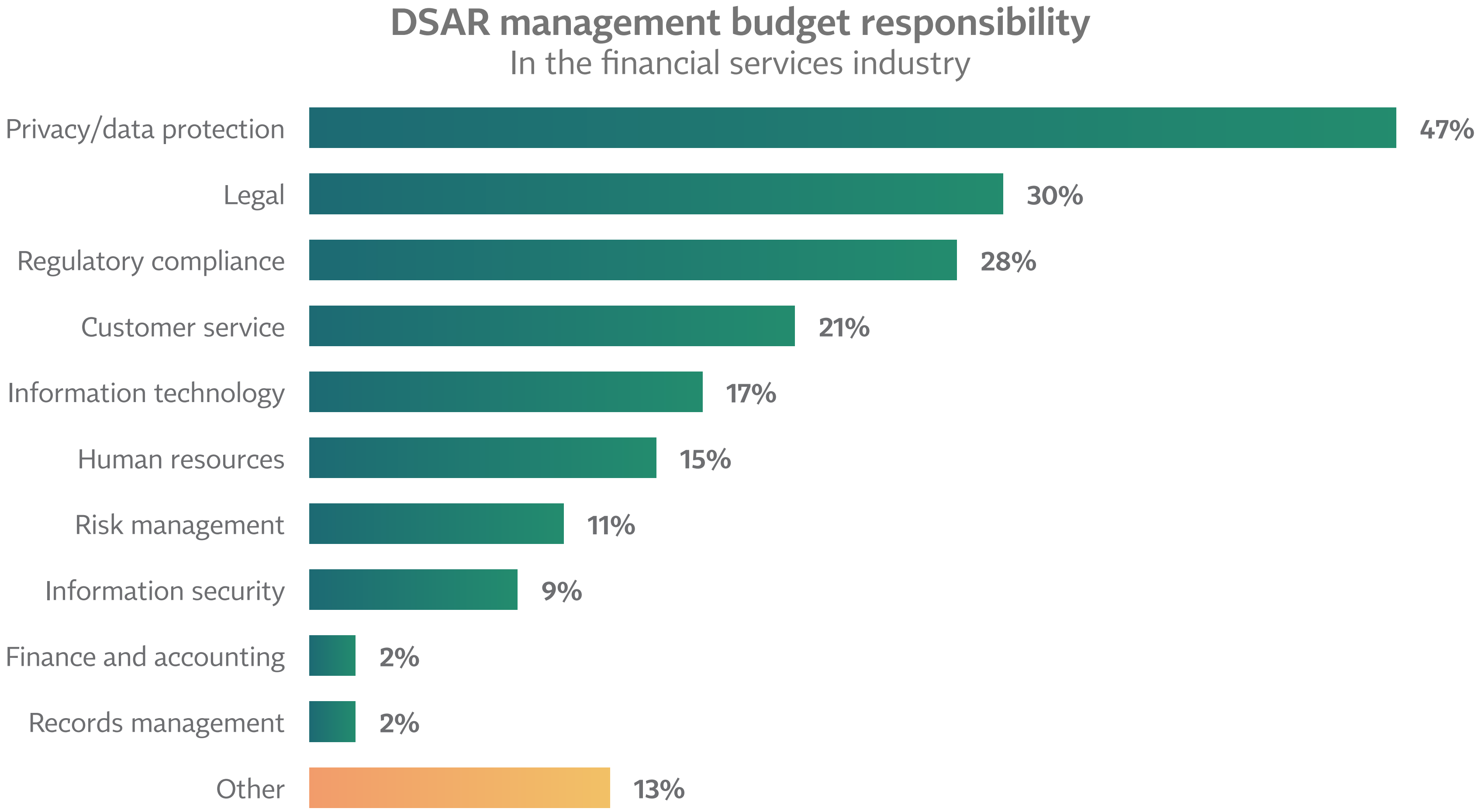
By organization HQ location



■ United States ■ European Union ■ Non-EU Europe ■ Other

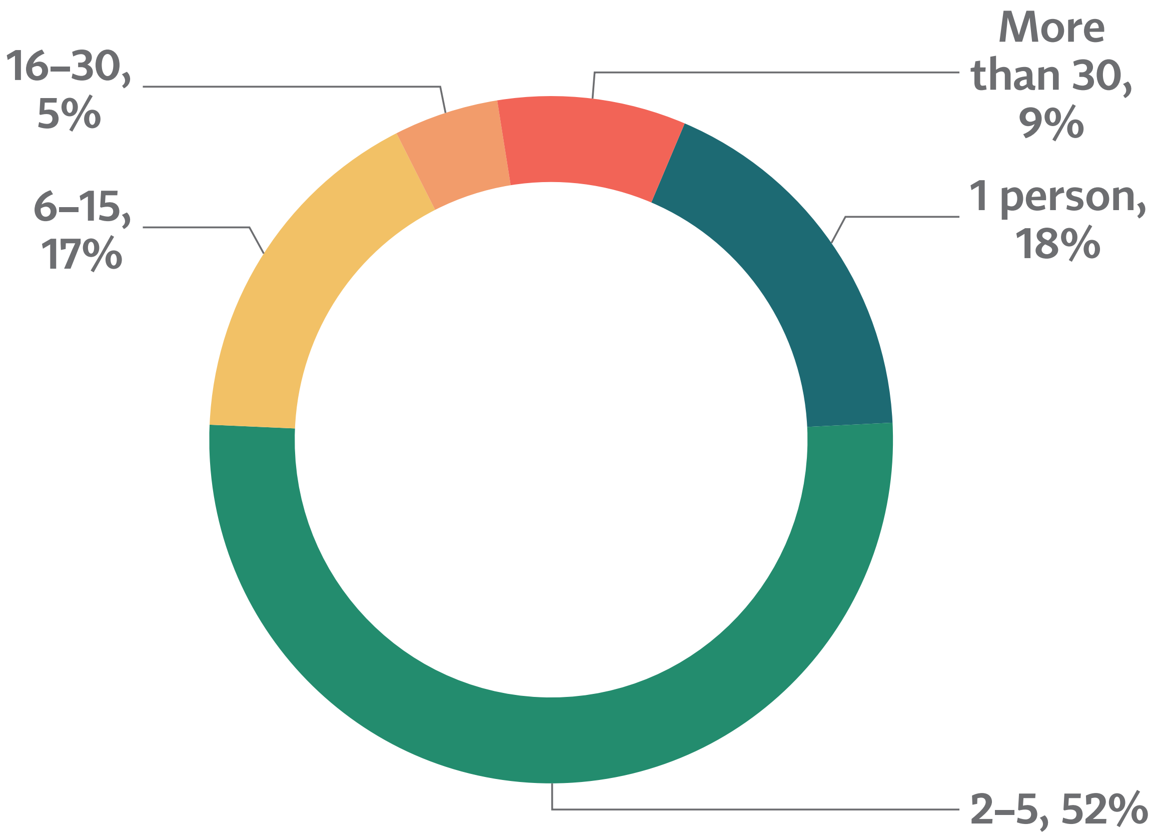
◆ *Indicates a statistically signigicant difference.*

DSAR management budgets for respondents in the financial services industry are most often held by the privacy or data protection function, followed by legal, regulatory compliance and customer service.



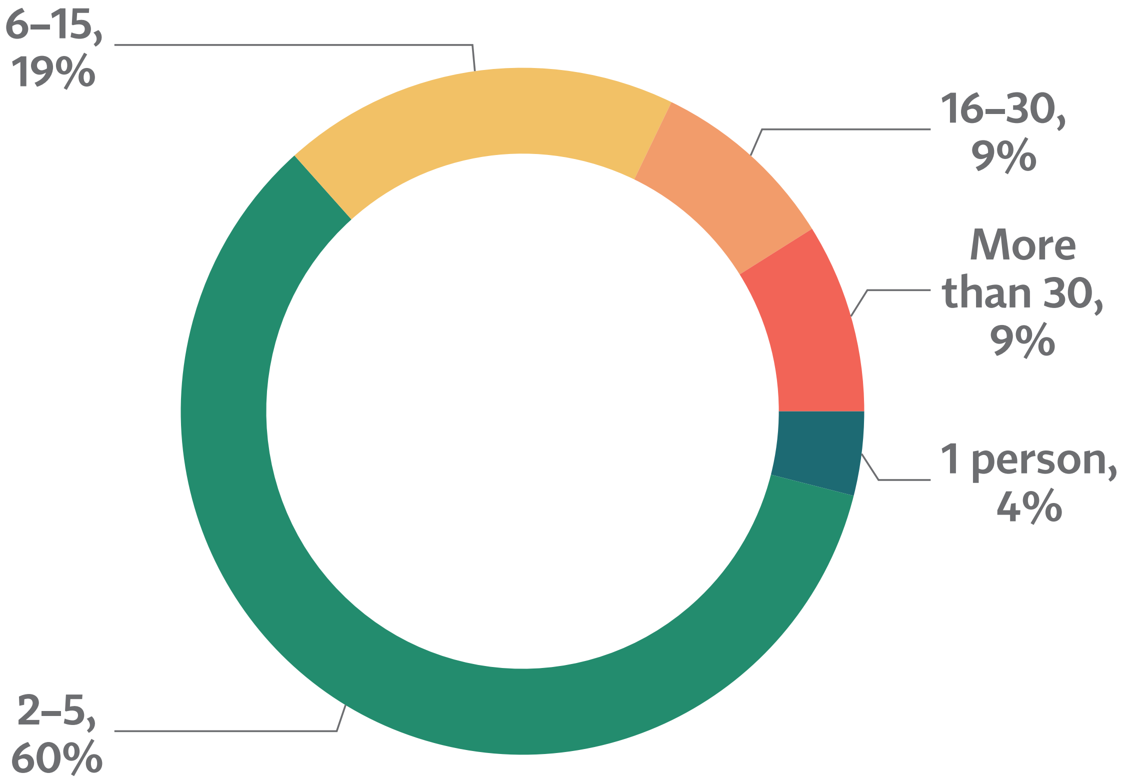
Seven in 10 organizations have fewer than six employees responsible for DSAR management.

Number of personnel responsible for DSARs management within the organization



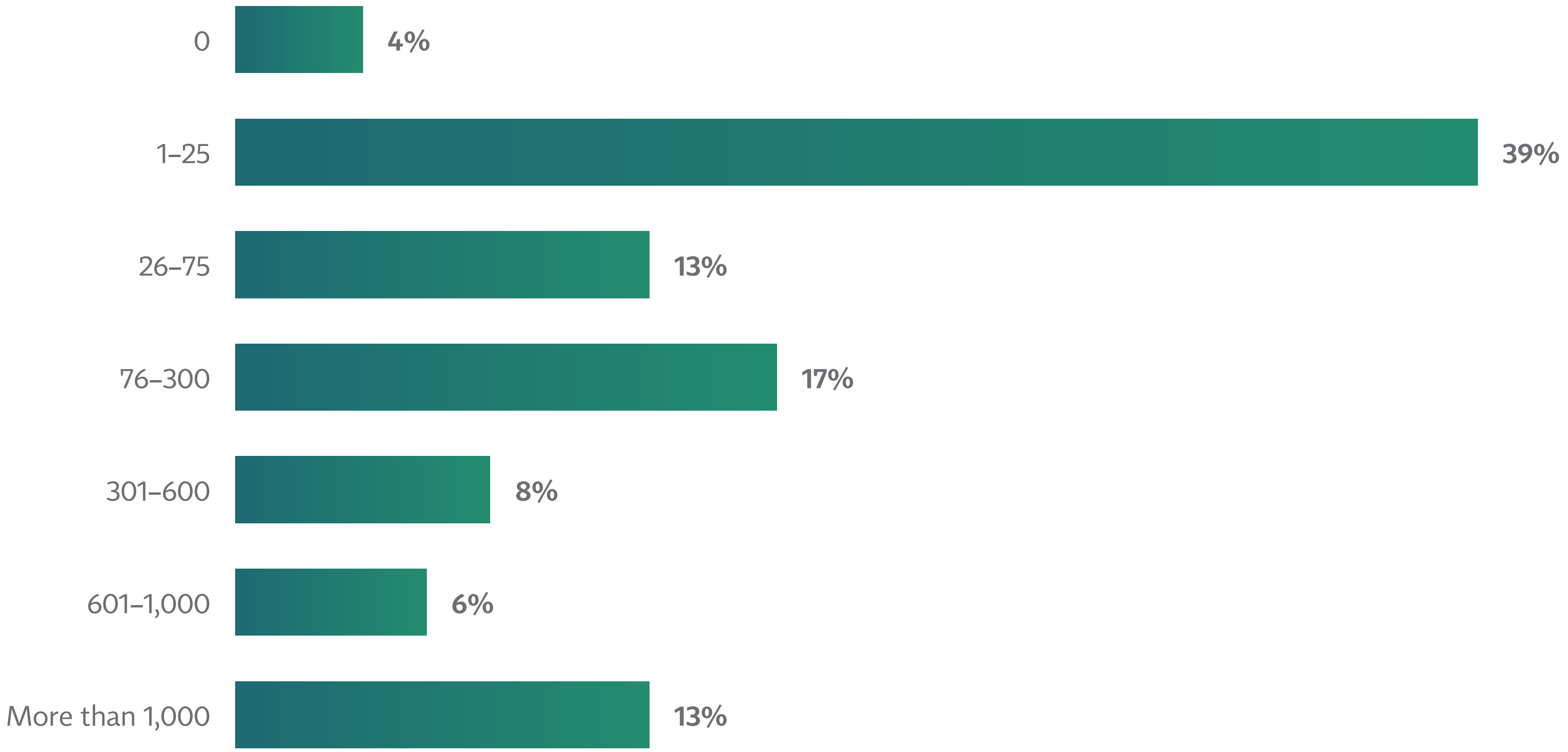
Organizations in the financial services industry reported higher numbers of staff working on data rights management.

Number of personnel responsible for data rights management within the organization
In the financial services industry



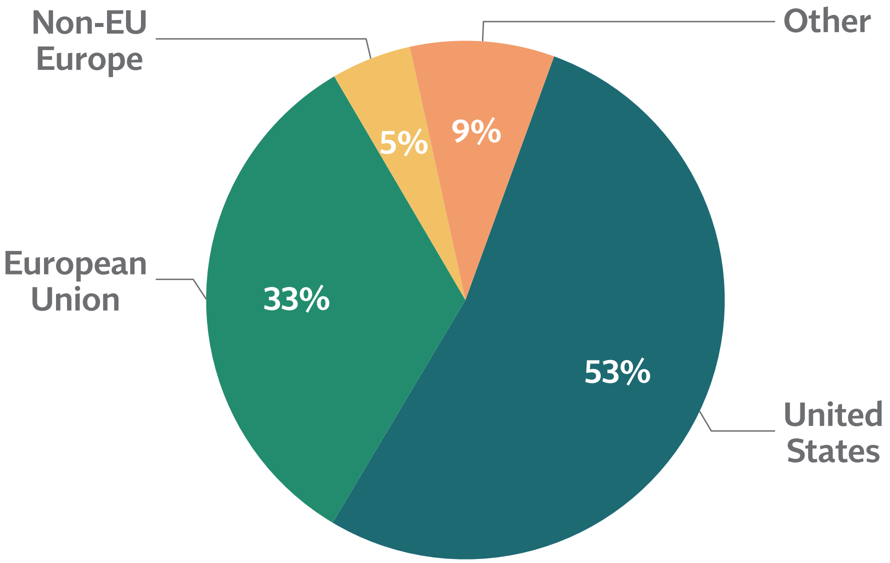
56% of companies report receiving less than 75 DSARs in 2020.

The number of DSARs respondents report receiving in 2020

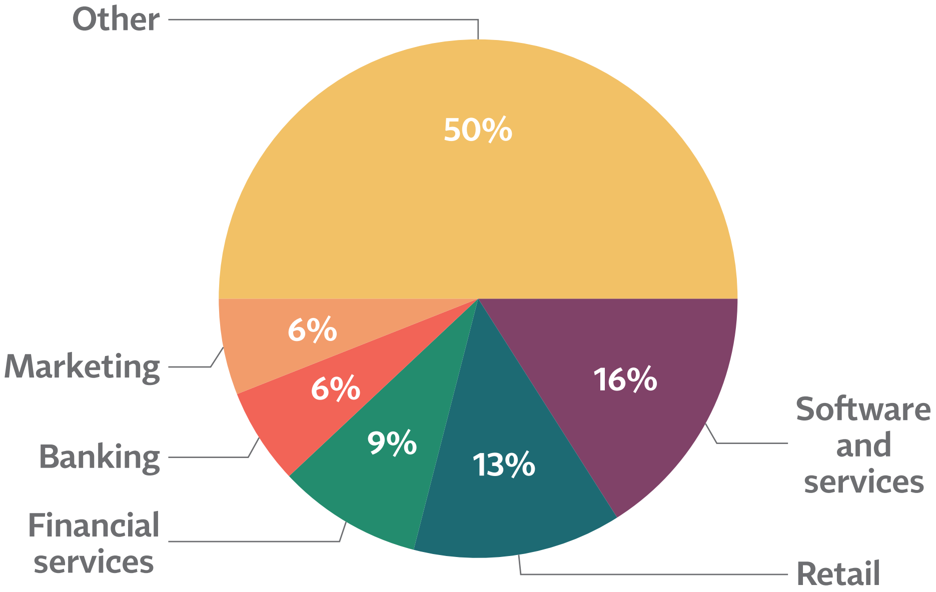


13% of organizations that have received more than 1,000 DSARs in 2020, half are in the U.S. and mostly in the software, retail and financial services sectors.

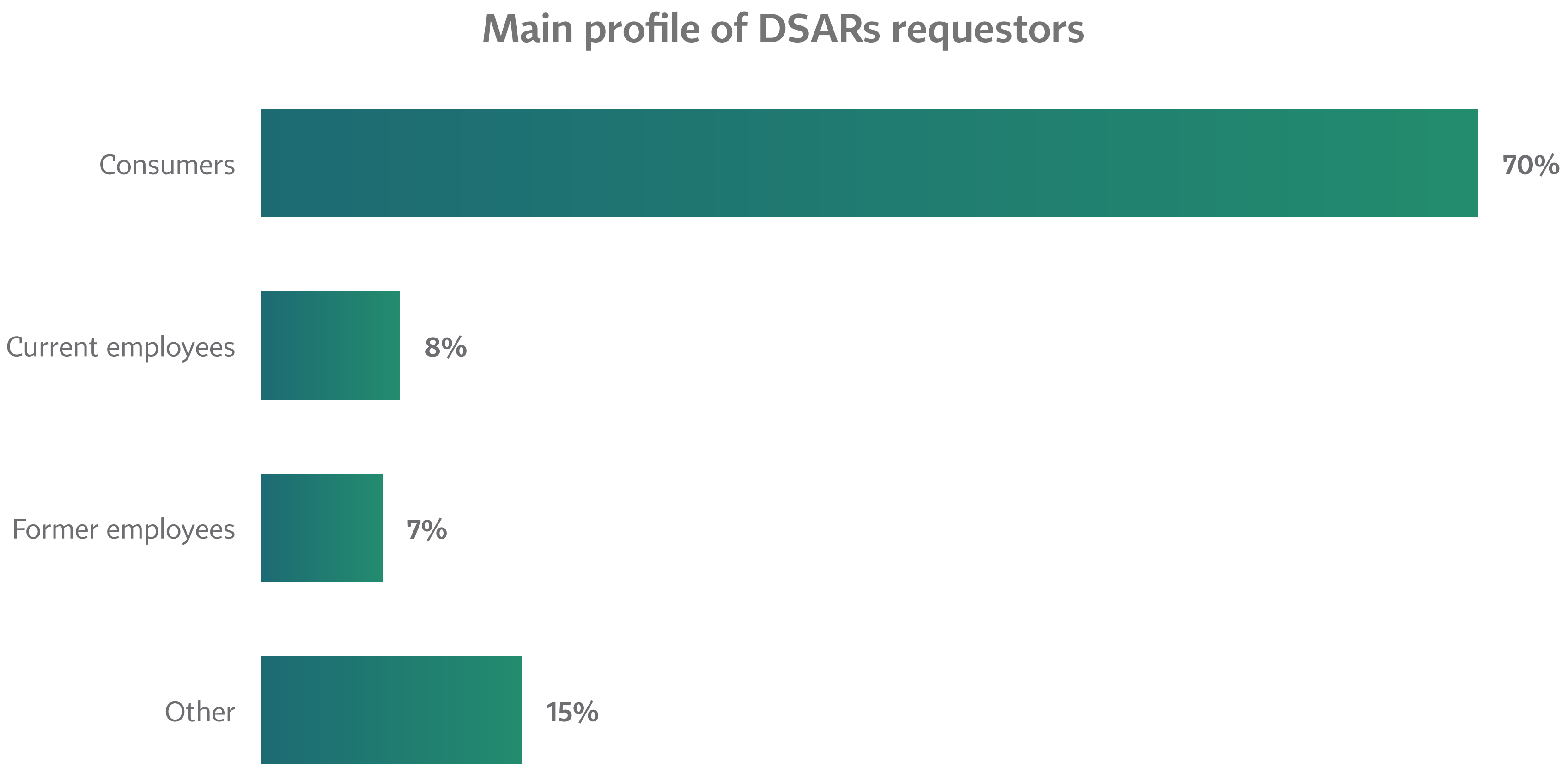
Organizations receiving more than 1,000 DSARs
By organization HQ location



Organizations receiving more than 1,000 DSARs
By industry



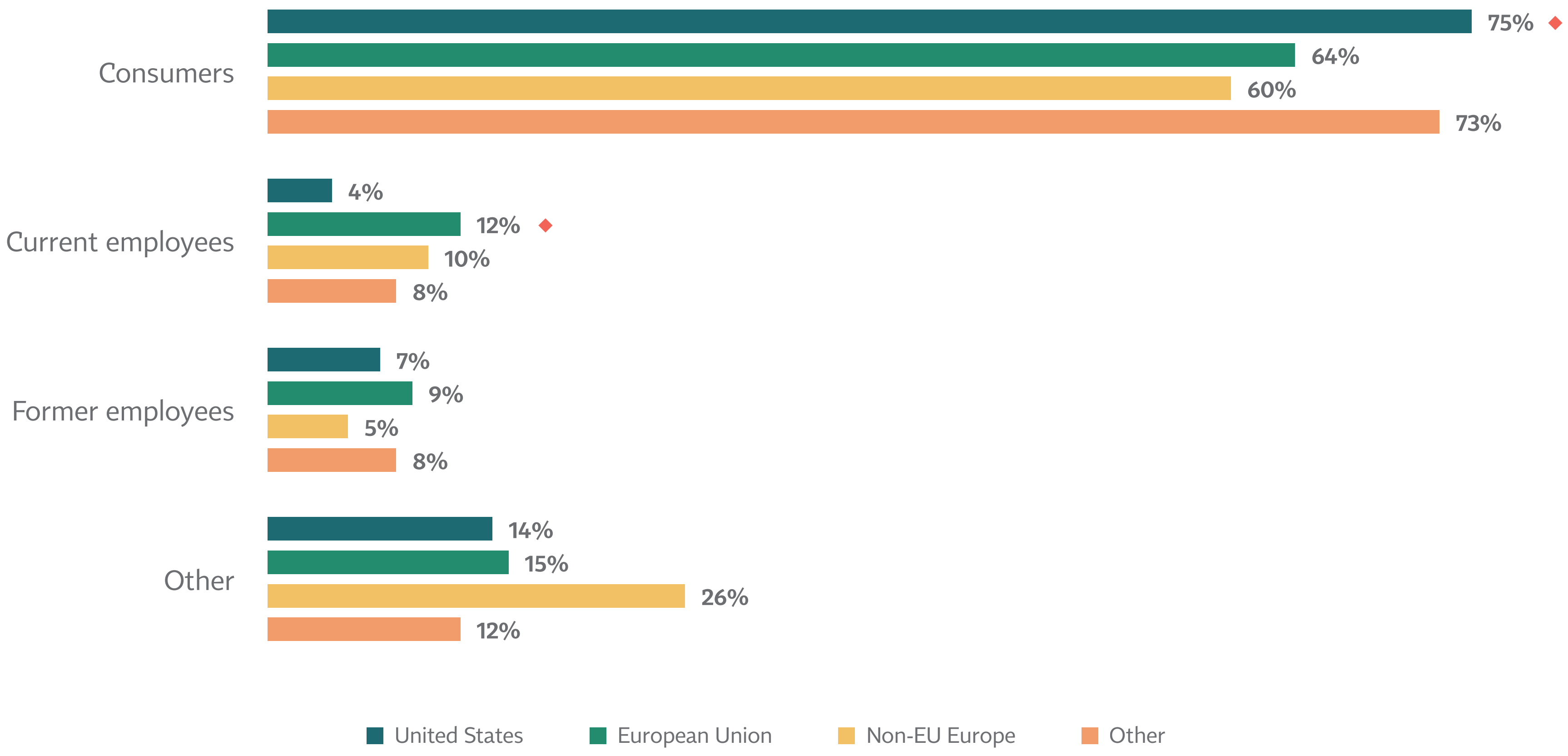
The vast majority of DSARs originate from consumers.



Consumer DSARs are most common in the U.S. Employees are more likely to submit a DSAR in the EU than the U.S.

Profile of DSARs requestors

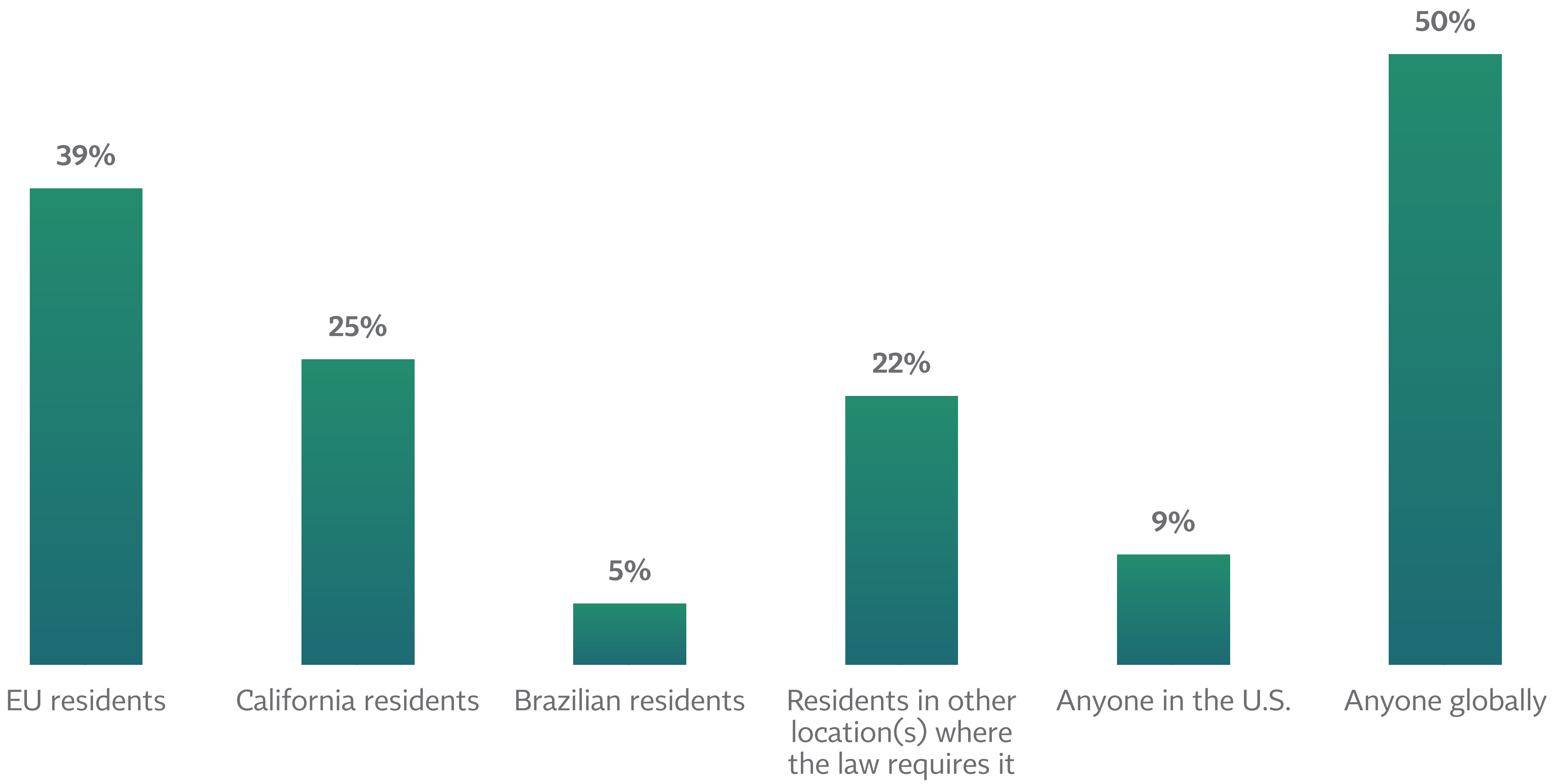
By organization HQ location



◆ *Indicates a statistically signigicant difference.*

Half of the respondents report honoring DSARs from anyone globally.

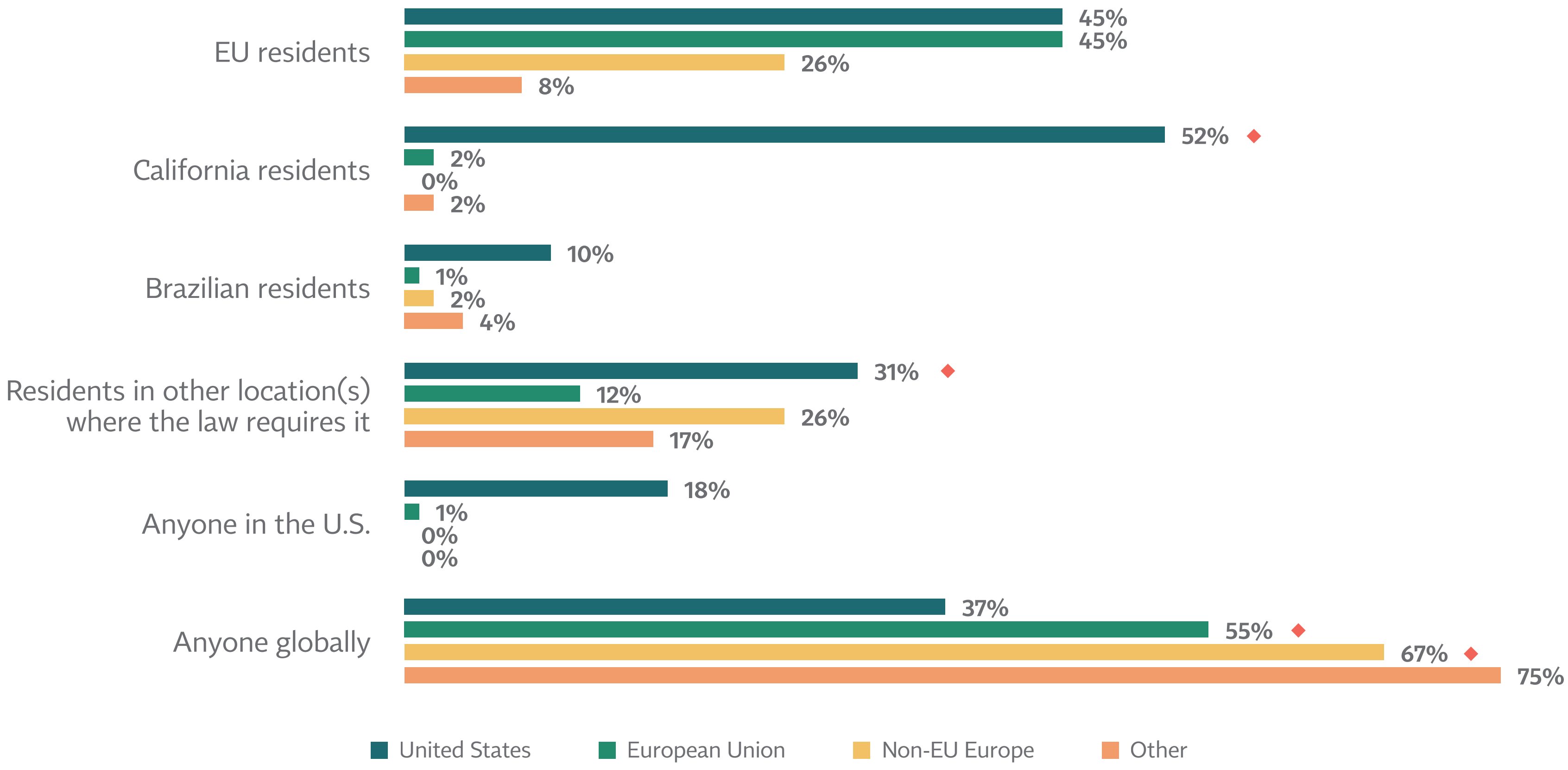
To whom do companies provide individual data rights?



European companies are more likely to provide access rights to data subjects globally. U.S. companies are more likely to honor requests from California residents and other locations, as required by law.

To whom do companies provide data subject access rights?

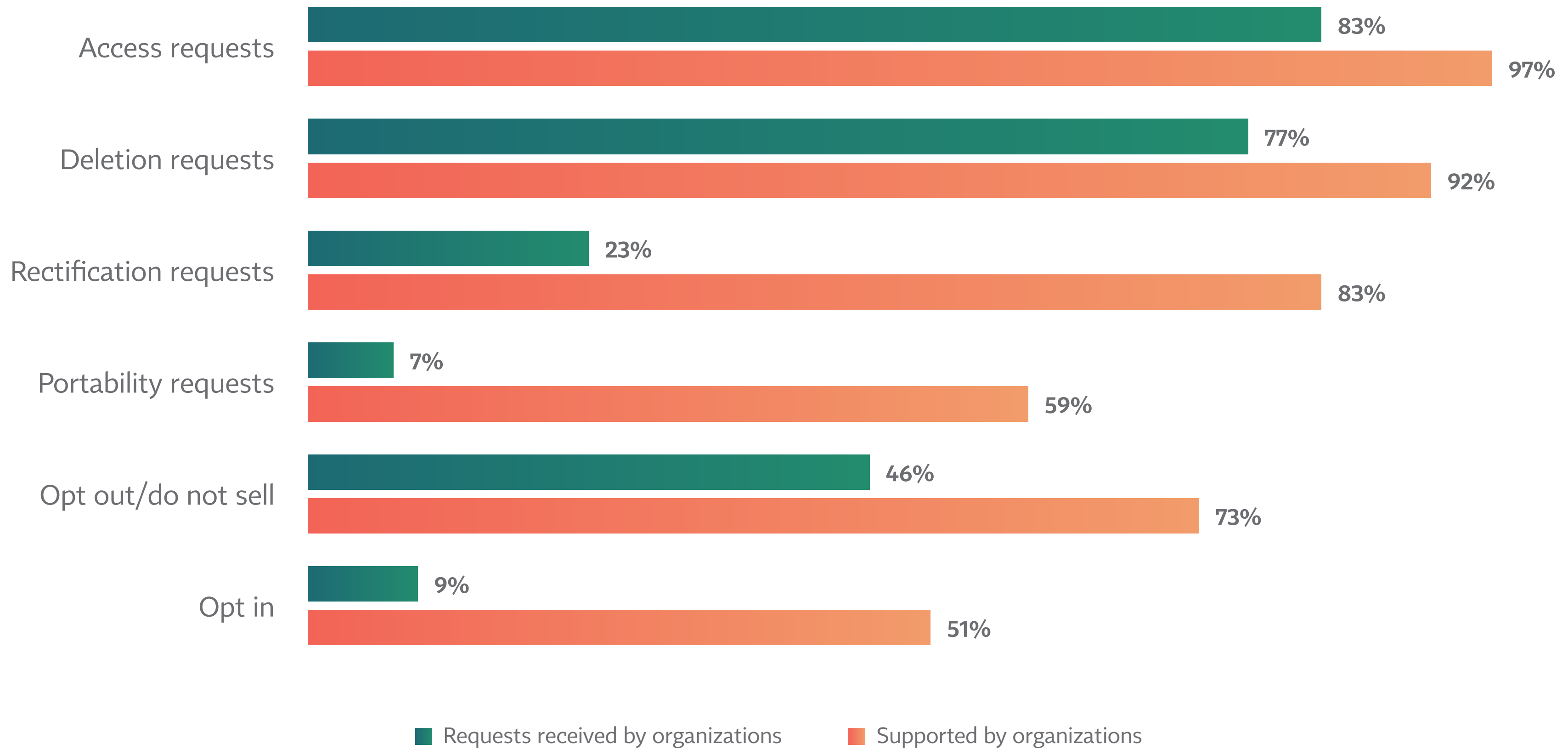
By organization HQ location



◆ *Indicates a statistically signigicant difference.*

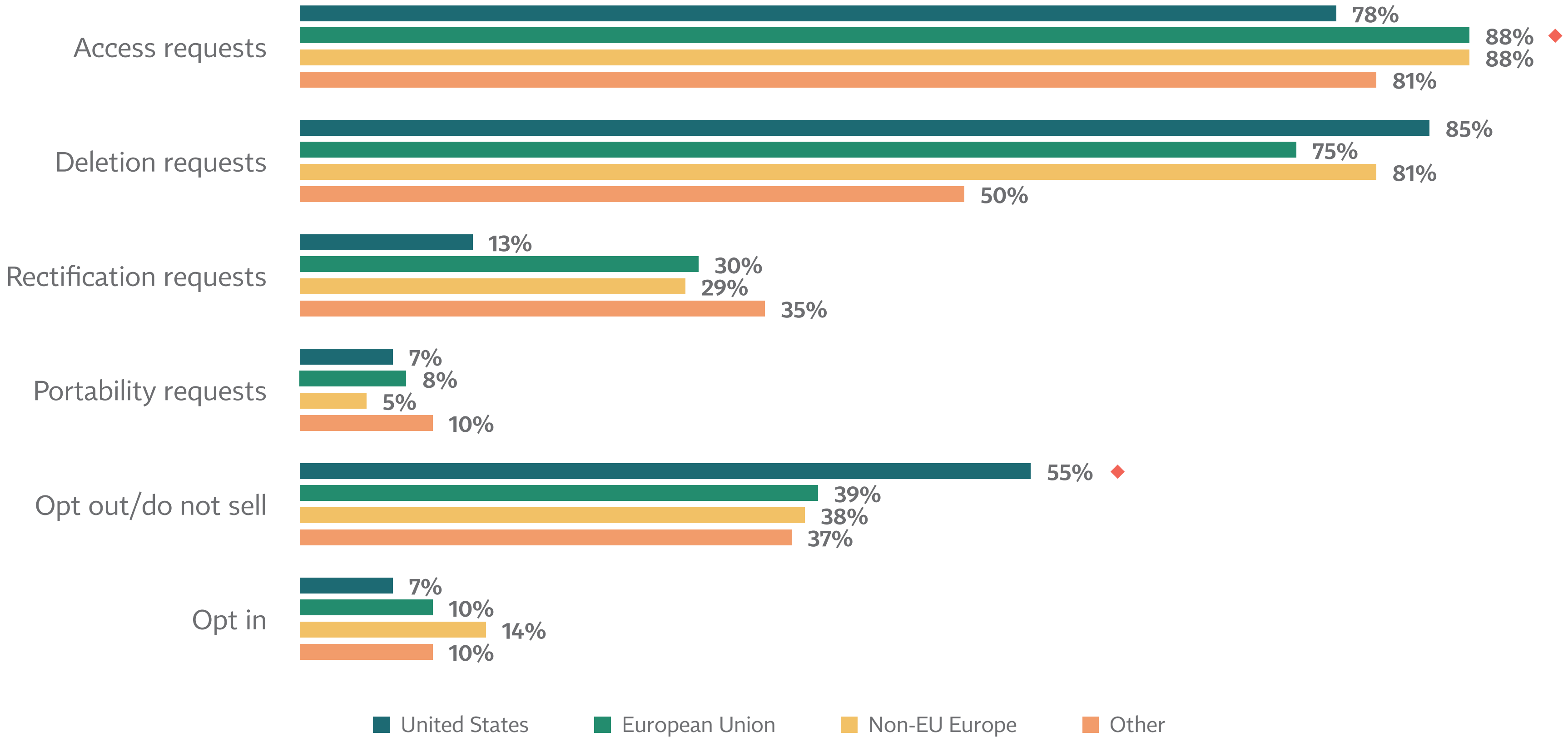
Access and deletion requests are the most common type of DSARs received. Portability and opt-in requests are the least common. Organizations support all types of DSARs received.

Types of DSARs handled by organizations



Organizations in the EU receive significantly more access requests than those in the U.S. Companies in the U.S. report getting significantly more opt-out/do-not-sell requests than all other regions.

Types of DSARs requested
By organization HQ location

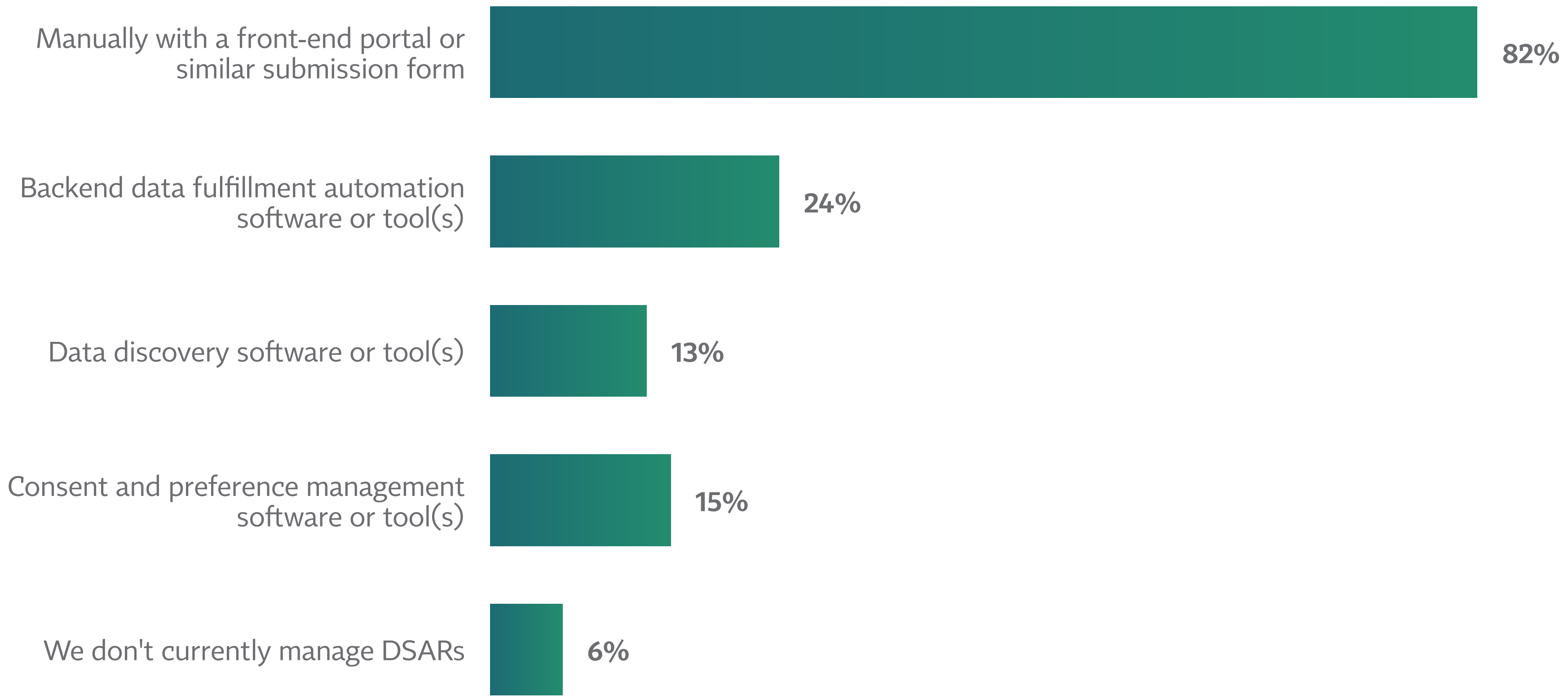


◆ *Indicates a statistically signigicant difference.*

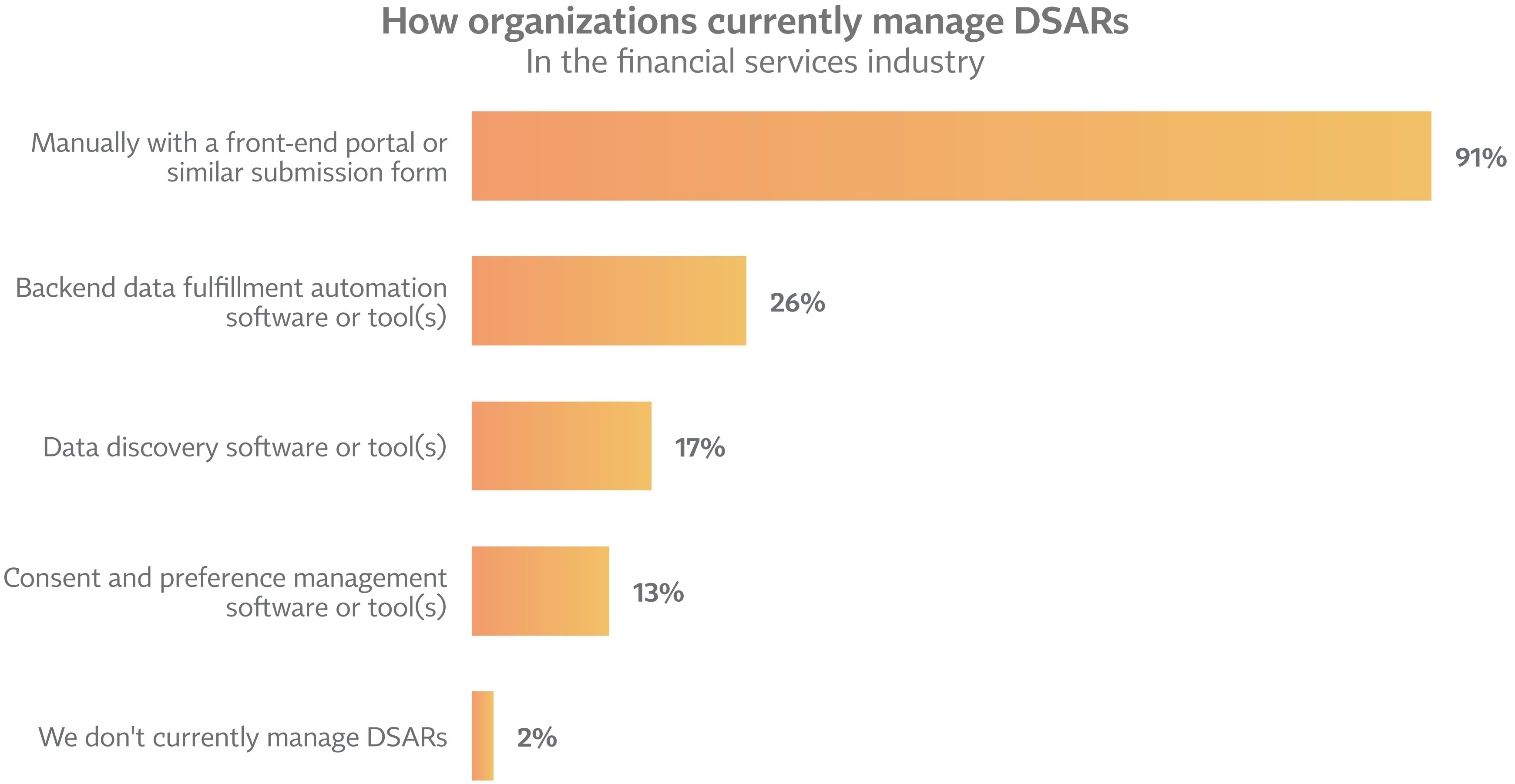
Survey Findings: DSAR intake, discovery and output

Most organizations are manually managing DSARs with a front-end portal or something similar. Less than 20% are using an automated DSAR management tool.

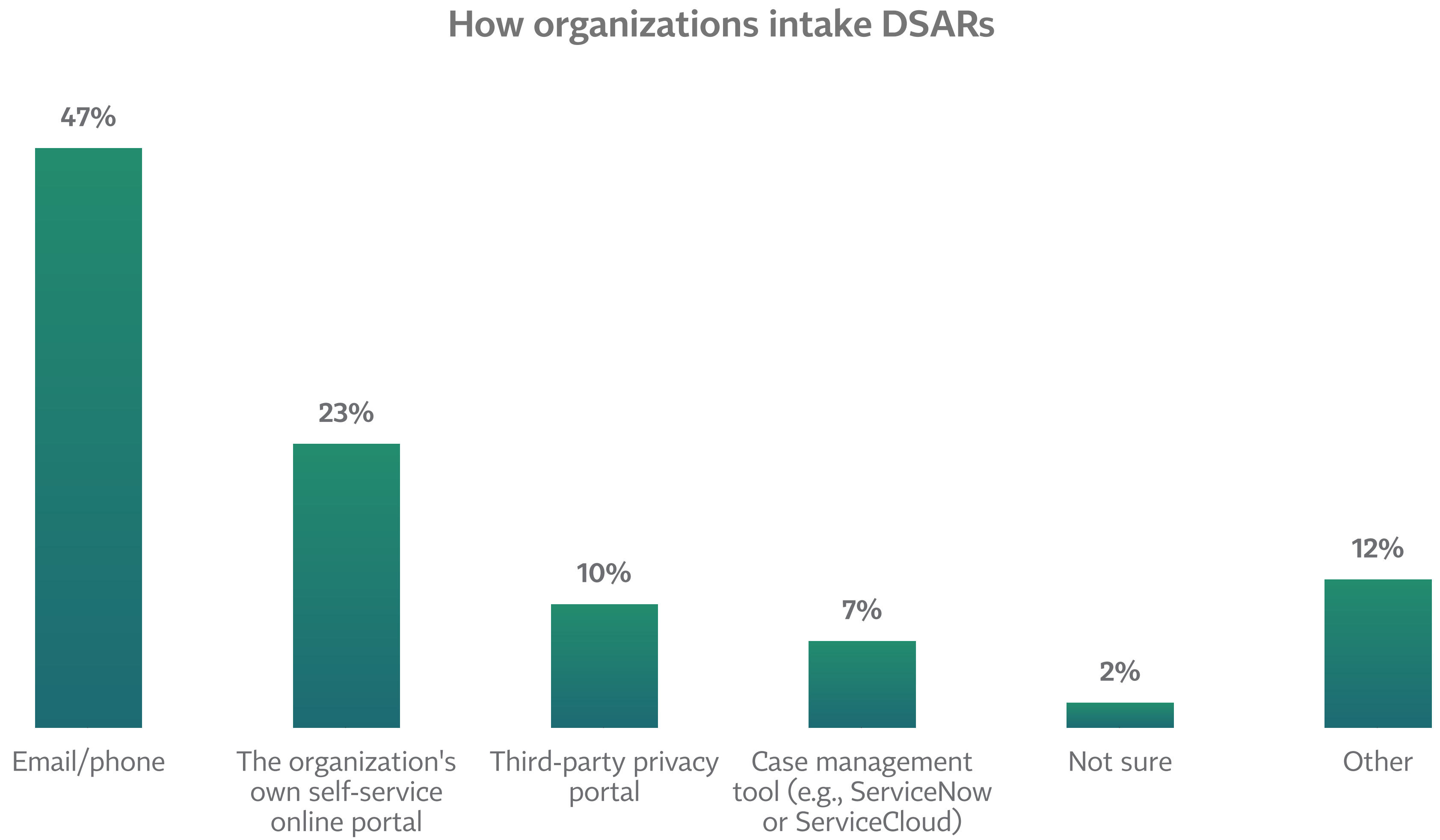
How organizations currently manage DSARs



In the financial services industry, 9 in 10 organizations use a manual front-end portal or submission form to manage DSARs, though sometimes in combination with automated tools.



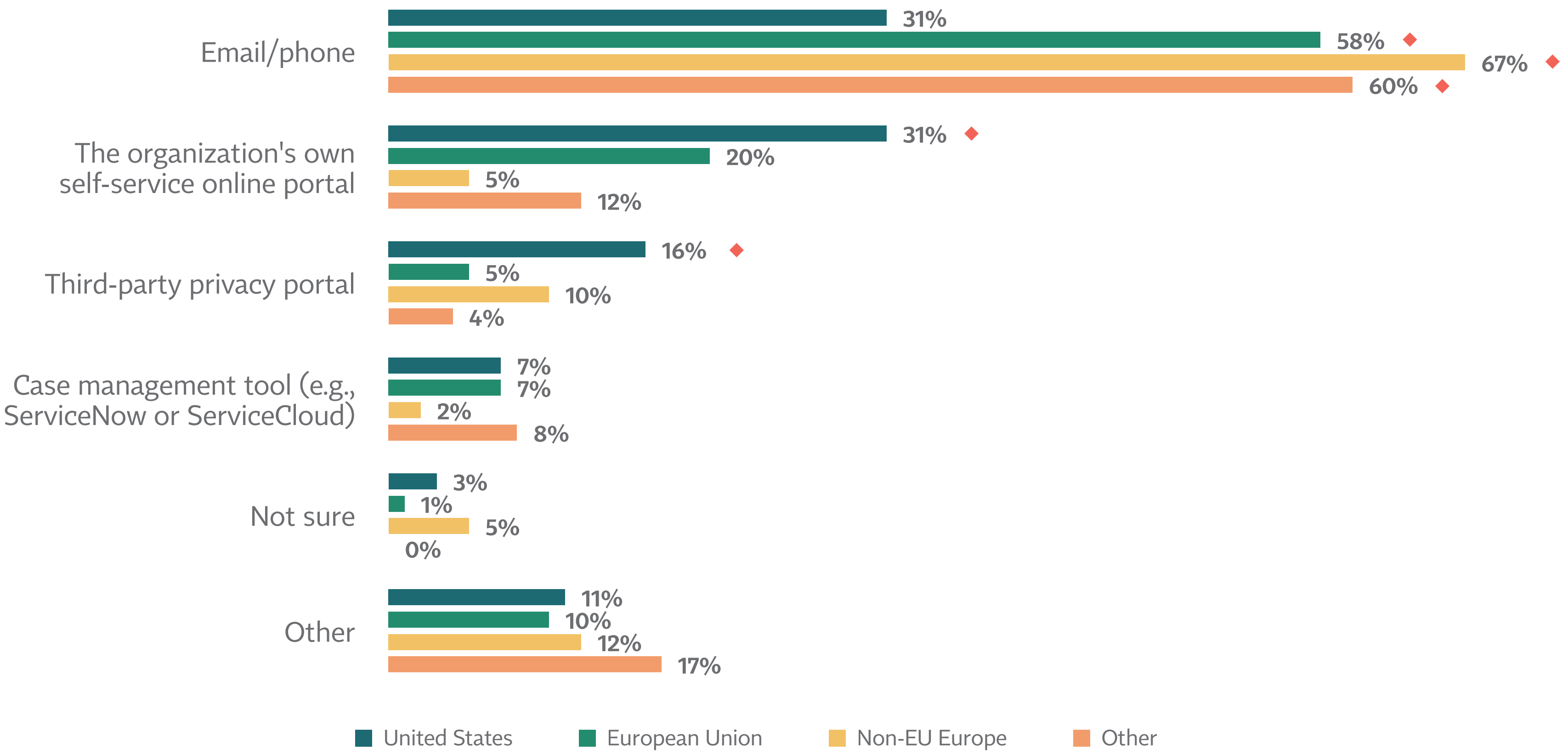
Nearly half of the respondents process DSARs via email or by phone.



Organizations in the U.S. are significantly less likely to use email for DSAR intake and instead use their own self-service online portal or a third-party privacy portal.

How organizations intake DSARs

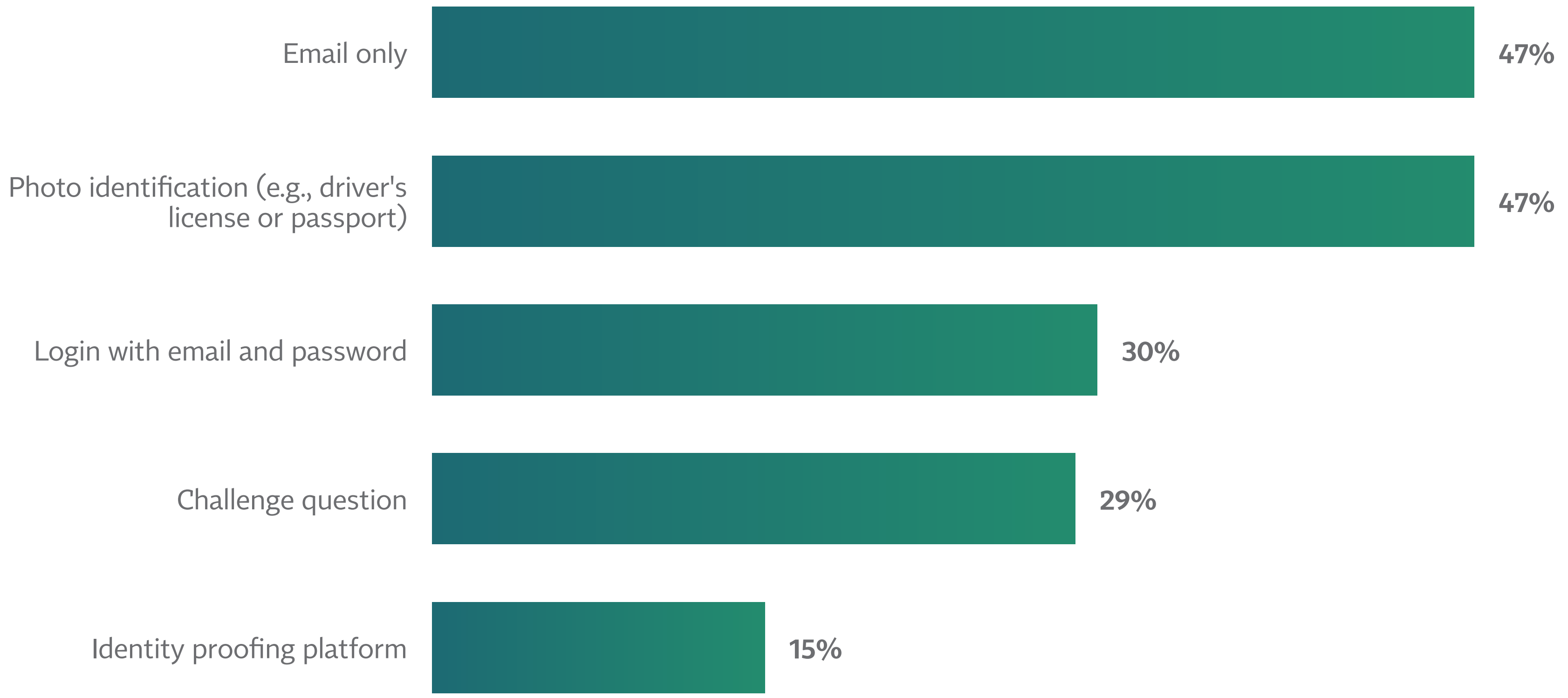
By organization HQ location



◆ *Indicates a statistically signigicant difference.*

47% of responding organizations use only email or ask for a photo identification to verify a data subject's identity.

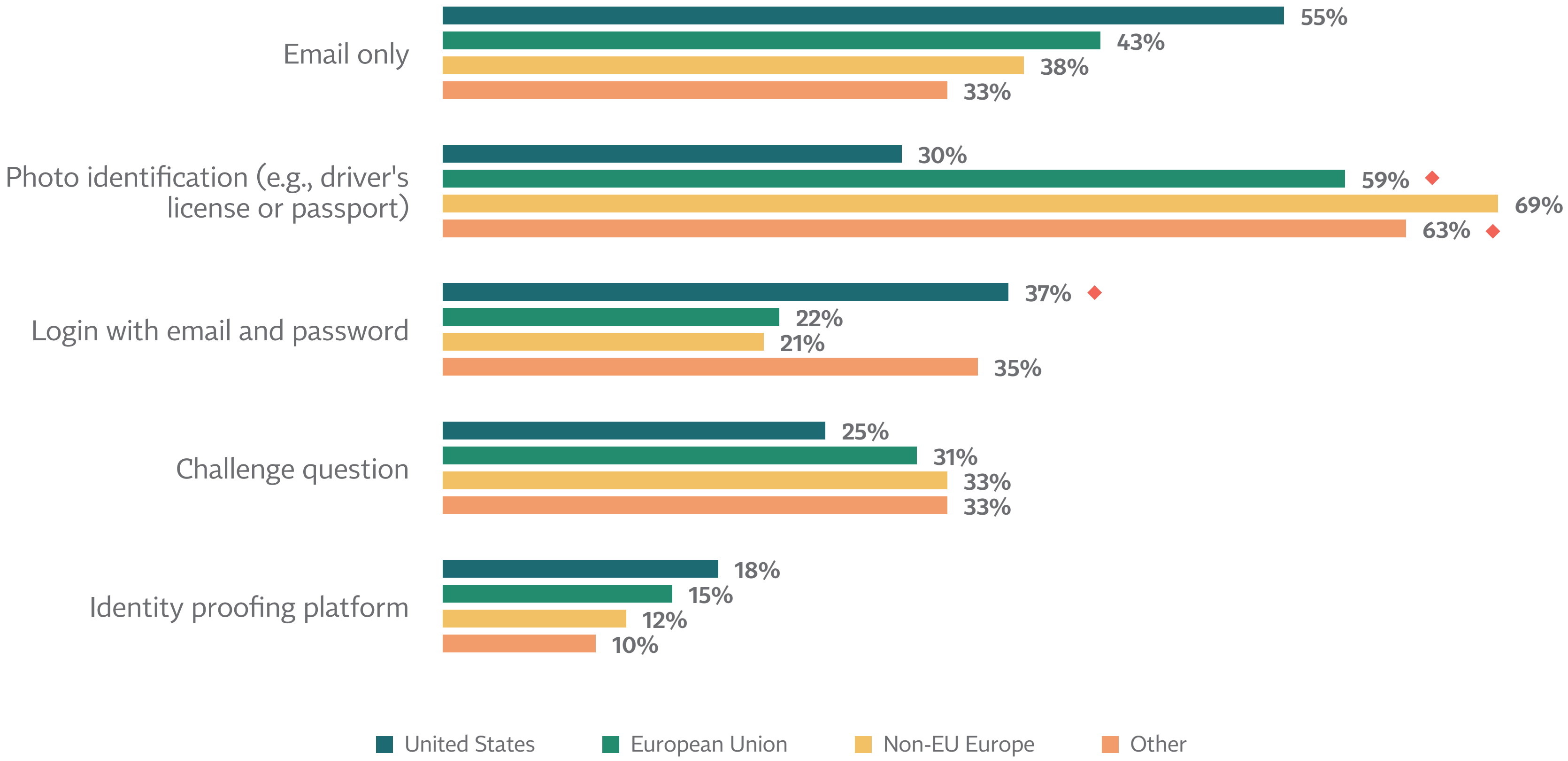
How organizations verify a data subject's identity



Companies in the U.S. are significantly less likely to require a photo identification than organizations in Europe. Instead, U.S. companies are more likely to use a login with email and password.

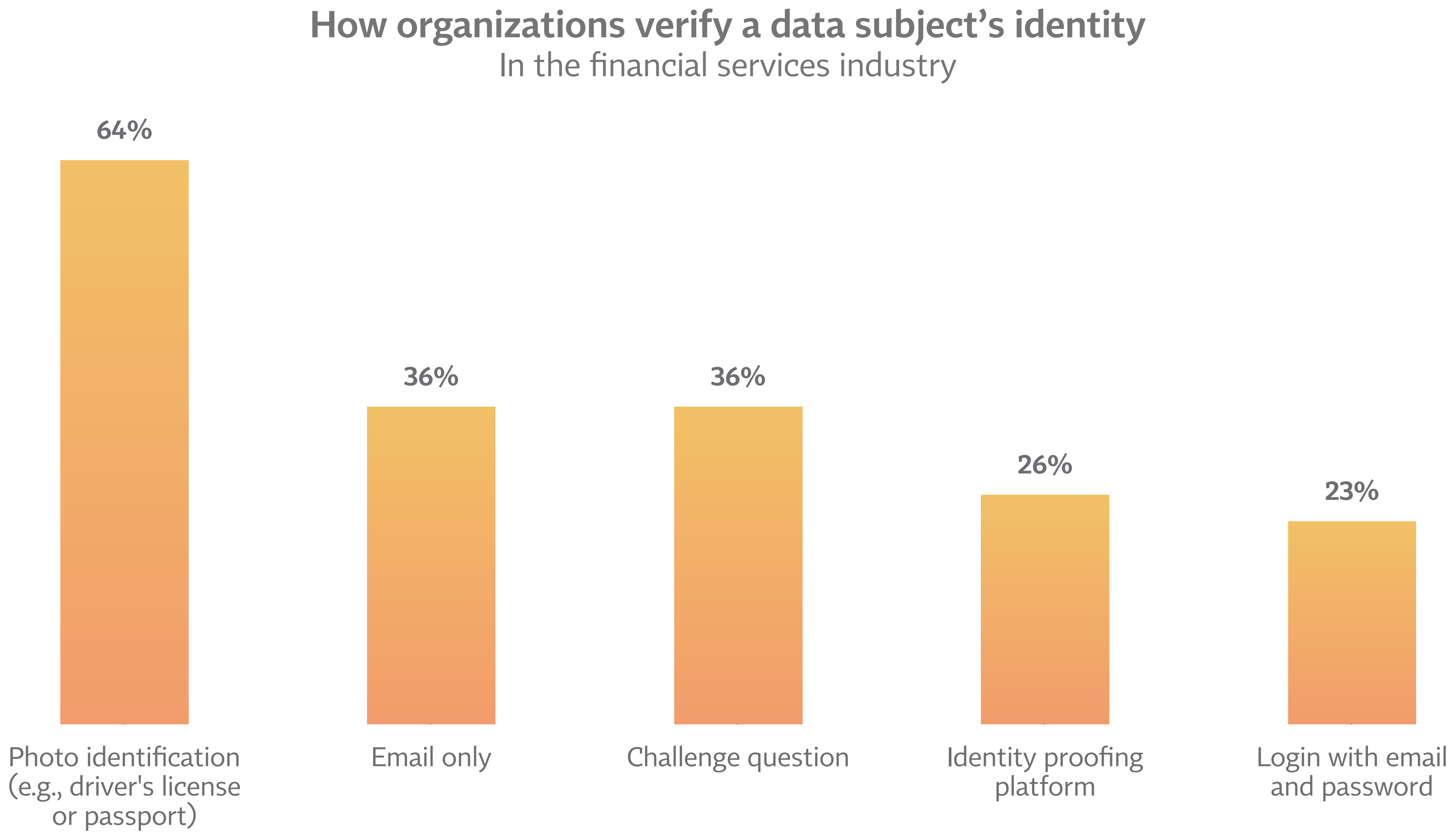
How organizations verify a data subject's identity

By organization HQ location

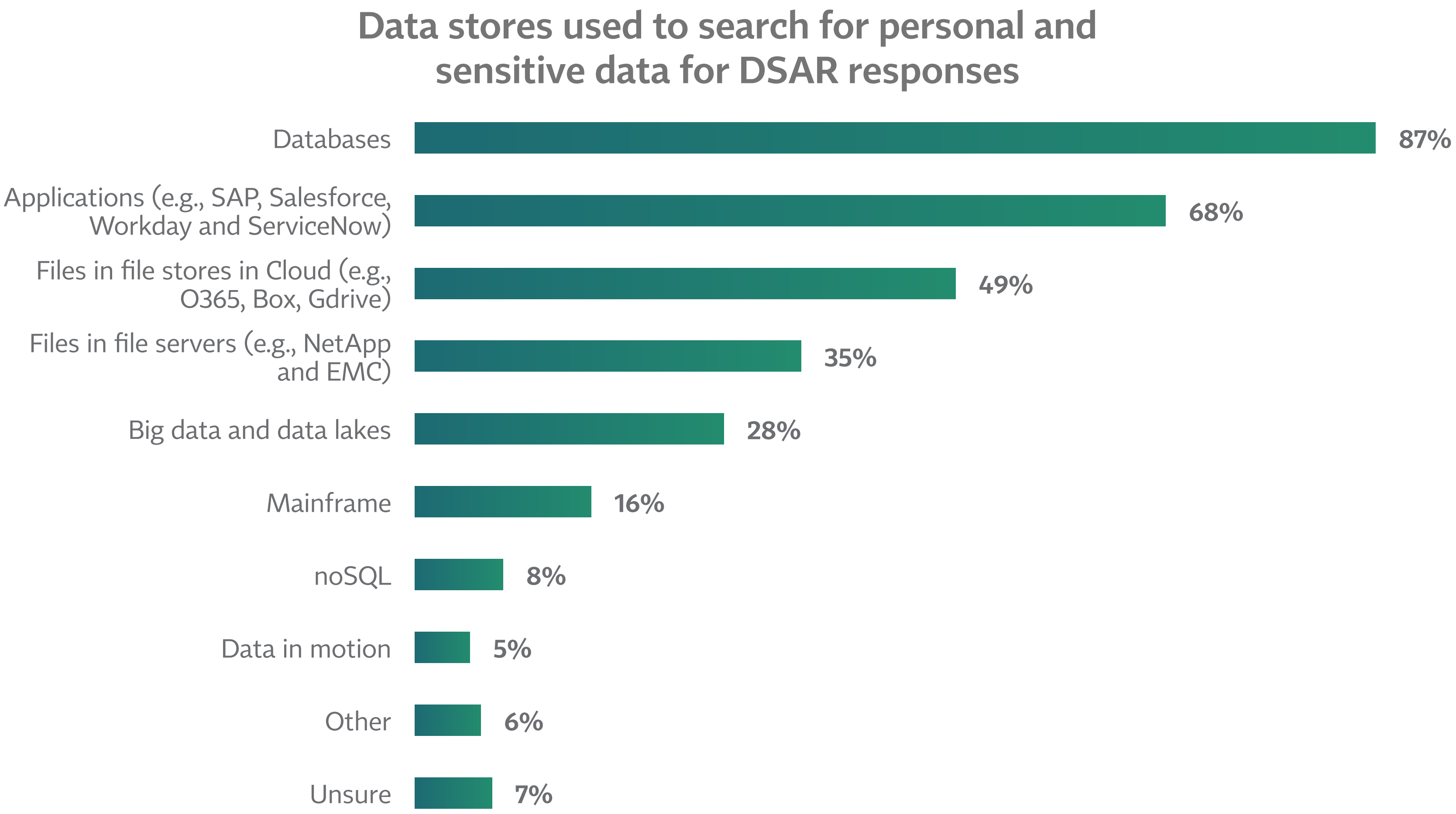


◆ *Indicates a statistically signigicant difference.*

Six in 10 organizations in the financial services industry use photo ID to verify a requestor's identity. Email and a challenge question are the next most frequently used methods.

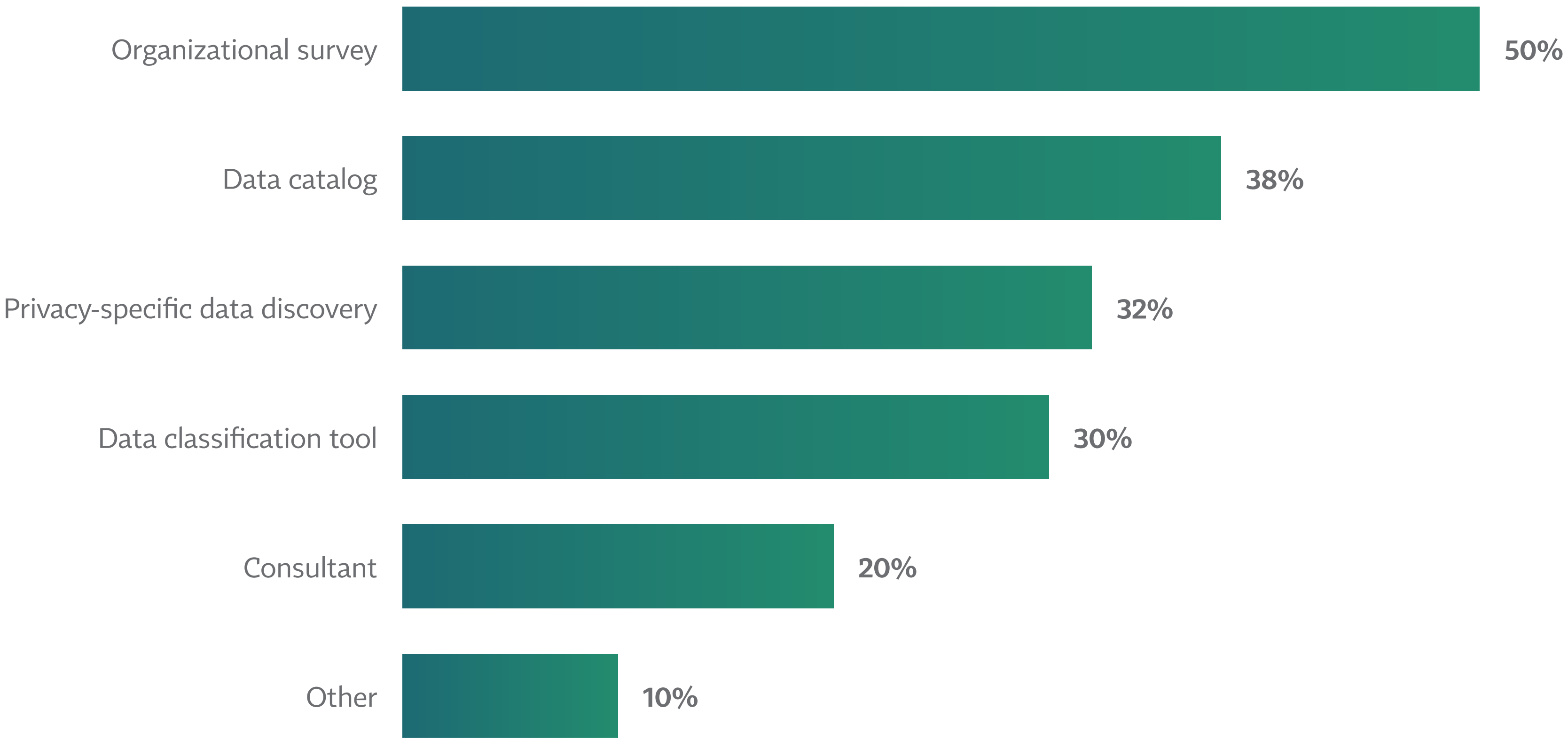


Most organizations search databases and applications to identify data for DSAR responses.



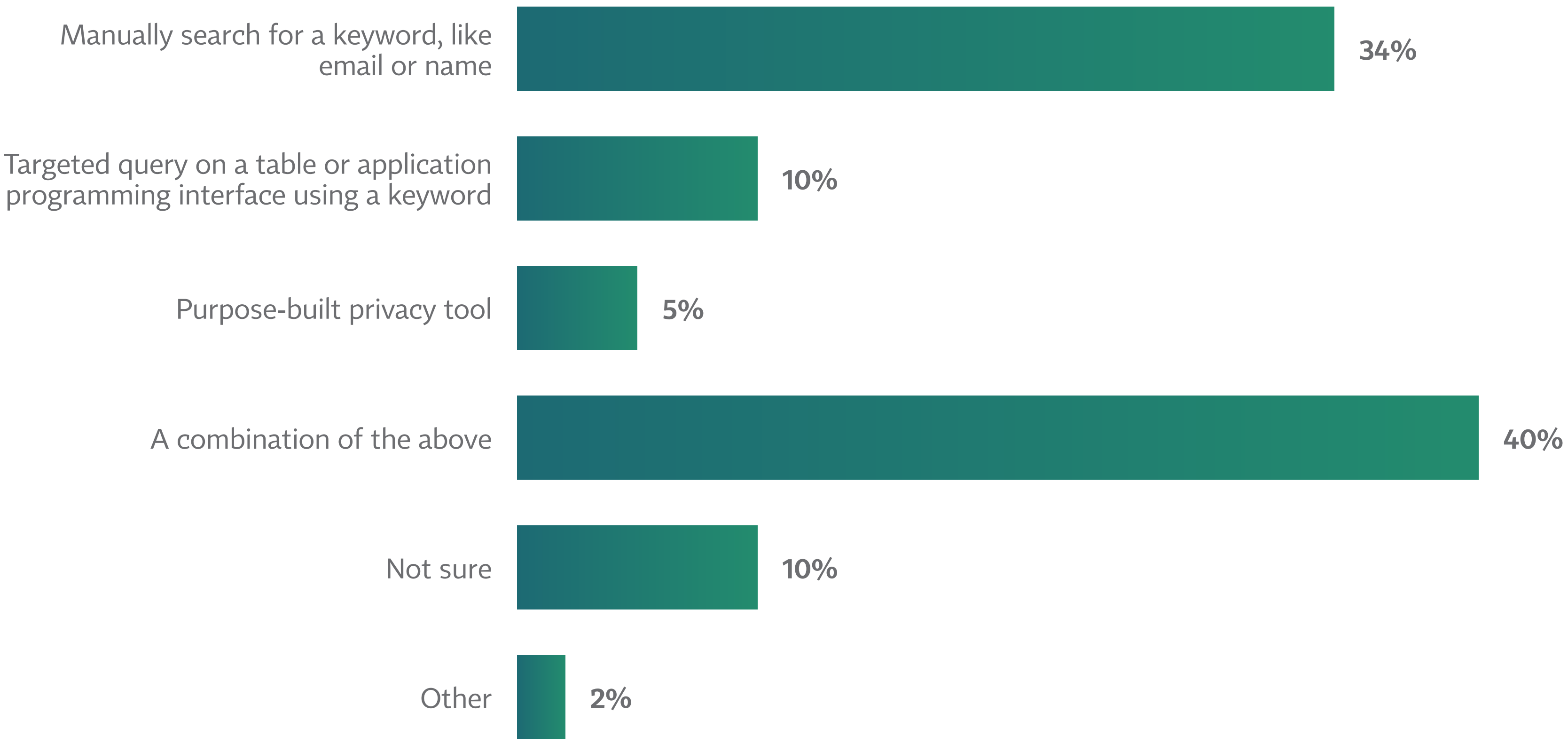
Half of the respondents use an organizational survey to build their data inventory, and only a third use privacy-specific data discovery.

Resources used to build data inventory



Four in 10 organizations use a combination of manual and automated tools to correlate data to an identity.

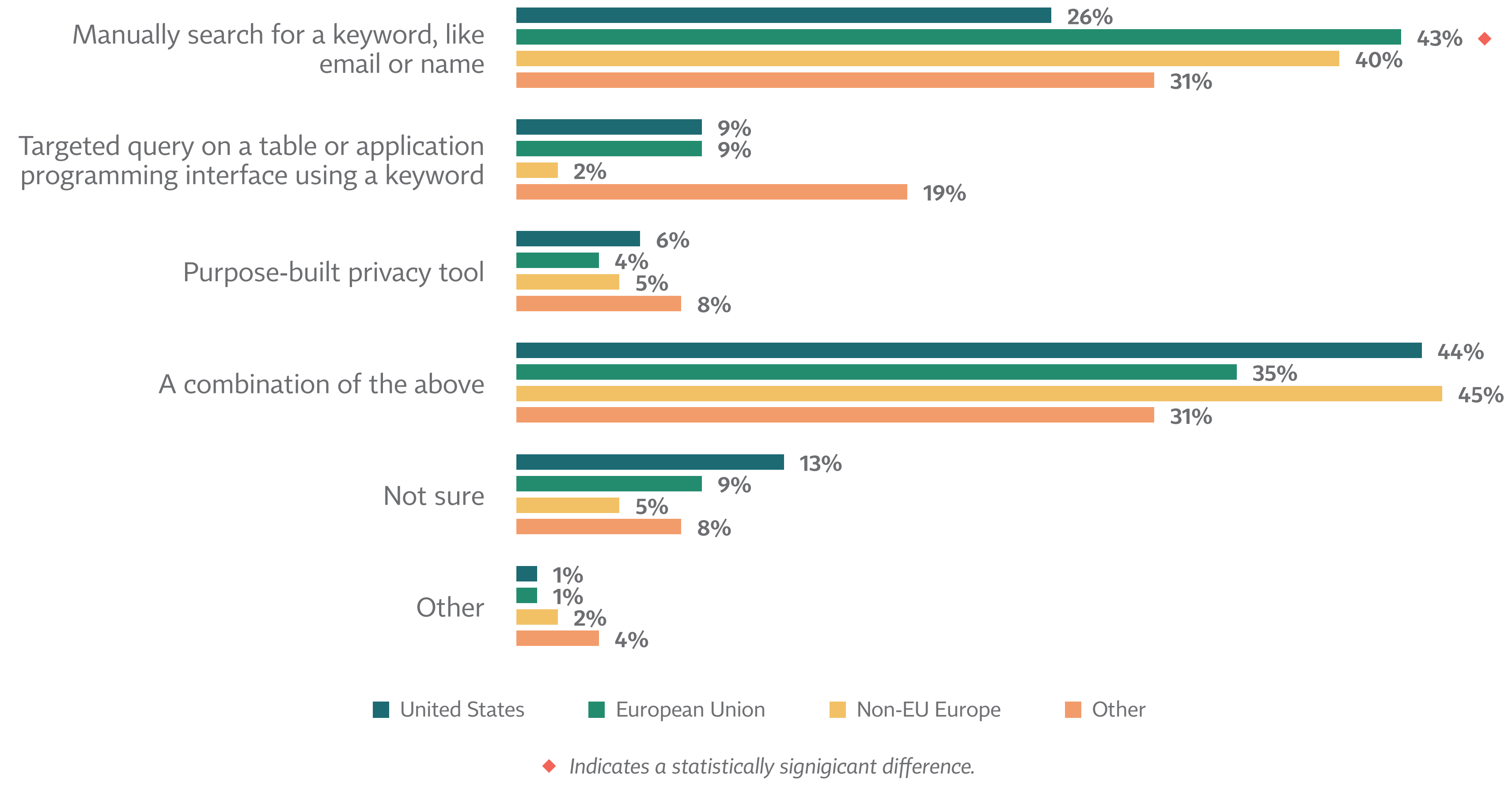
How organizations correlate data to an identity



A third of organizations, mostly in Europe, use manual keyword searches to correlate data to an identity.

How organizations correlate data to an identity

By organization HQ location



Contact

Sarah Hospelhorn

BigID

VP, Product & Content Marketing

165 Mercer St., 4th Floor, New York, NY, 10012

sarah@bigid.com