The State of Data Rights

By IAPP Research Manager Margaret Honda and IAPP Market Research Specialist Christelle Kamaliza, CIPP/E, CIPM
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 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 exercising 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.
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.
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
- United States: 42%
- United Kingdom: 18%
- Netherlands: 5%
- Ireland: 5%
- Canada: 4%
- Germany: 2%
- Belgium: 2%
- Other: 22%

### Distribution of organization HQ
- United States: 46%
- European Union: 34%
- Non-EU Europe: 9%
- Canada: 4%
- Asia: 3%
- Australia or New Zealand: 1%
- Latin America (including Mexico): 1%
- Africa: 1%
- Middle East: <1%
- Indian subcontinent: <1%
Most respondents are in-house privacy professionals in the private sector, from a balanced mix of industries and organizations of all sizes.

### Industry

<table>
<thead>
<tr>
<th>Industry</th>
<th>Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software and services</td>
<td>14%</td>
</tr>
<tr>
<td>Financials services</td>
<td>10%</td>
</tr>
<tr>
<td>Government</td>
<td>6%</td>
</tr>
<tr>
<td>Banking</td>
<td>4%</td>
</tr>
<tr>
<td>Health care</td>
<td>4%</td>
</tr>
<tr>
<td>Insurance</td>
<td>4%</td>
</tr>
<tr>
<td>Retail</td>
<td>4%</td>
</tr>
<tr>
<td>Telecommunication services</td>
<td>4%</td>
</tr>
<tr>
<td>Consulting services</td>
<td>4%</td>
</tr>
<tr>
<td>Drug and biotechnology</td>
<td>4%</td>
</tr>
<tr>
<td>Education and academia</td>
<td>4%</td>
</tr>
<tr>
<td>Technology hardware and equipment</td>
<td>4%</td>
</tr>
<tr>
<td>Media</td>
<td>3%</td>
</tr>
<tr>
<td>Aerospace and defense</td>
<td>3%</td>
</tr>
<tr>
<td>Nonprofit</td>
<td>3%</td>
</tr>
<tr>
<td>Transportation</td>
<td>3%</td>
</tr>
<tr>
<td>Other</td>
<td>24%</td>
</tr>
</tbody>
</table>

### Current position

- Private-sector, in-house privacy professional: 79%
- Government sector, in-house privacy professional: 9%
- Nonprofit or education sector, in-house privacy professional: 8%
- Any sector, in-house IT professional: 3%

### Size of organization

- 1–250: 13%
- 251–1,000: 20%
- 1,001–5,000: 24%
- 5,001–25,000: 22%
- 25,001 or more: 21%
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

- Data discovery/inventory/mapping: 51%
- Consent and preferences management: 34%
- Enhancement or creation of consumer privacy portal: 30%
- Advisory services: 8%
- None: 30%
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

- **Data discovery/inventory/mapping**
  - United States: 41%
  - European Union: 33%
  - Non-EU Europe: 20%
  - Other: 29%
  - United States (62%): Indicates a statistically significant difference.
  - European Union: 40%
  - Non-EU Europe: 26%
  - Other: 19%

- **Consent and preferences management**
  - United States: 40%
  - European Union: 26%
  - Non-EU Europe: 19%
  - Other: 15%
  - United States (40%): Indicates a statistically significant difference.
  - European Union: 20%
  - Non-EU Europe: 19%
  - Other: 7%

- **Enhancement or creation of consumer privacy portal**
  - United States: 38%
  - European Union: 29%
  - Non-EU Europe: 29%
  - Other: 20%
  - United States (38%): Indicates a statistically significant difference.
  - European Union: 33%
  - Non-EU Europe: 31%
  - Other: 9%

- **Advisory services**
  - United States: 7%
  - European Union: 9%
  - Non-EU Europe: 15%
  - Other: 20%

- **None**
  - United States: 41%
  - European Union: 41%
  - Non-EU Europe: 29%
  - Other: 45%
  - United States (45%): Indicates a statistically significant 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

- Data discovery/inventory/mapping: 57%
- Consent and preferences management: 40%
- Enhancement or creation of consumer privacy portal: 38%
- Advisory services: 13%
- None: 17%
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:

- Integrate into governance, risk and compliance efforts: 20%
- Integrate into legal compliance initiatives: 13%
- Integrate into data governance: 9%
- Integrate into data security: 4%
- All of the above: 27%
- None: 26%
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

- Number of DSARs received: 62%
- Average DSAR response time: 56%
- Customer satisfaction: 44%
- Lack of fines: 36%
- Cost per DSAR response: 13%
- Other: 8%
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

<table>
<thead>
<tr>
<th>METRICS TO MEASURE SUCCESS OF DSAR STRATEGY INVESTMENTS</th>
<th>NUMBER OF DSARS RECEIVED OVER THE PAST YEAR</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
</tr>
<tr>
<td>Number of DSARs received</td>
<td>58%</td>
</tr>
<tr>
<td>Average DSAR response time</td>
<td>26%</td>
</tr>
<tr>
<td>Customer satisfaction</td>
<td>58%</td>
</tr>
<tr>
<td>Lack of fines</td>
<td>26%</td>
</tr>
<tr>
<td>Cost per DSAR response</td>
<td>11%</td>
</tr>
<tr>
<td>Other</td>
<td>0%</td>
</tr>
</tbody>
</table>

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.

### Metrics used to measure the success of data rights strategy investments

In the financial services industry

<table>
<thead>
<tr>
<th>Metric</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average DSAR response time</td>
<td>70%</td>
</tr>
<tr>
<td>Number of DSARs received</td>
<td>60%</td>
</tr>
<tr>
<td>Customer satisfaction</td>
<td>49%</td>
</tr>
<tr>
<td>Lack of fines</td>
<td>30%</td>
</tr>
<tr>
<td>Cost per DSAR response</td>
<td>17%</td>
</tr>
<tr>
<td>Other</td>
<td>11%</td>
</tr>
</tbody>
</table>
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:

- Benchmark against industry peers: 46%
- Degree of automation: 37%
- Percent of data systems or data stores covered: 31%
- Benchmark against privacy peers: 27%
- Other: 14%
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

<table>
<thead>
<tr>
<th>Metric</th>
<th>United States</th>
<th>European Union</th>
<th>Non-EU Europe</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Benchmark against industry peers</td>
<td>52%</td>
<td>38%</td>
<td>40%</td>
<td>41%</td>
</tr>
<tr>
<td>Degree of automation</td>
<td>44%</td>
<td>35%</td>
<td>35%</td>
<td>30%</td>
</tr>
<tr>
<td>Percent of data systems or data stores covered</td>
<td>33%</td>
<td>28%</td>
<td>26%</td>
<td>29%</td>
</tr>
<tr>
<td>Benchmark against privacy peers</td>
<td>29%</td>
<td>27%</td>
<td>19%</td>
<td>19%</td>
</tr>
<tr>
<td>Other</td>
<td>13%</td>
<td>21%</td>
<td>19%</td>
<td>12%</td>
</tr>
</tbody>
</table>

*Indicates a statistically significant 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

- Degree of automation: 45%
- Percent of data systems or data stores covered: 45%
- Benchmark against industry peers: 43%
- Benchmark against privacy peers: 30%
- Other: 13%
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

- Data subject access requests: 44%
- Data subject rights requests: 32%
- Consumer rights requests: 7%
- Data subject requests: 5%
- Data rights requests: 2%
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

- **Data subject access requests**
  - United States: 45%
  - European Union: 48%
  - Non-EU Europe: 38%
  - Other: 44%

- **Data subject rights requests**
  - United States: 43%
  - European Union: 31%
  - Non-EU Europe: 31%
  - Other: 38%

- **Data subject requests**
  - United States: 10%
  - European Union: 23%
  - Non-EU Europe: 23%
  - Other: 25%

- **Other**
  - United States: 5%
  - European Union: 4%
  - Non-EU Europe: 4%

- **Data rights requests**
  - United States: 5%
  - European Union: 12%
  - Non-EU Europe: 12%
  - Other: 2%

- **Consumer rights requests**
  - United States: 2%
  - European Union: 8%
  - Non-EU Europe: 8%

*Indicates a statistically significant difference.*
A quarter of the respondents work in industries with legal exemptions related to fulfilling DSARs under privacy/data protection laws.
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 process.

How much does the exemption apply?

- Applies to all the personal data our organization processes: 19%
- Applies to only a subset of the personal data our organization processes: 78%
- Does not apply to any of the personal data our organization processes: 2%
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

- **EU General Data Protection Regulation**: 85%
- **Organization's reputation**: 50%
- **California Consumer Privacy Act**: 48%
- **Customer transparency**: 42%
- **Brazil's General Data Protection Law**: 16%
- **Other**: 12%
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**

**EU General Data Protection Regulation**
- United States: 81%
- European Union: 98%
- Non-EU Europe: 95%
- Other: 52%

**Organization's reputation**
- United States: 51%
- European Union: 45%
- Non-EU Europe: 50%
- Other: 58%

**Customer transparency**
- United States: 47%
- European Union: 35%
- Non-EU Europe: 40%
- Other: 42%

**California Consumer Privacy Act**
- United States: 10%
- European Union: 26%
- Non-EU Europe: 23%
- Other: 26%

**Brazil's General Data Protection Law**
- United States: 6%
- European Union: 12%
- Non-EU Europe: 12%
- Other: 26%

**Other**
- United States: 7%
- European Union: 7%
- Non-EU Europe: 19%
- Other: 40%

*Indicates a statistically significant difference.*
Nearly half of companies across the globe report DSAR management budgets are held by privacy departments.

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

- **Privacy/data protection**
  - United States: 41%
  - European Union: 50%
  - Non-EU Europe: 45%
  - Other: 52%

- **Legal**
  - United States: 25%
  - European Union: 29%
  - Non-EU Europe: 29%
  - Other: 45% (Indicates a statistically significant difference)

- **Regulatory compliance**
  - United States: 16%
  - European Union: 24%
  - Non-EU Europe: 29%
  - Other: 29%

- **Information technology**
  - United States: 7%
  - European Union: 17%

- **Information security**
  - United States: 10%
  - European Union: 15%

- **Customer service**
  - United States: 10%
  - European Union: 20% (Indicates a statistically significant difference)

*Indicates a statistically significant 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.

**DSAR management budget responsibility**
*In the financial services industry*

- Privacy/data protection: 47%
- Legal: 30%
- Regulatory compliance: 28%
- Customer service: 21%
- Information technology: 17%
- Human resources: 15%
- Risk management: 11%
- Information security: 9%
- Finance and accounting: 2%
- Records management: 2%
- Other: 13%
Seven in 10 organizations have fewer than six employees responsible for DSAR management.
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

- 2–5, 60%
- 6–15, 19%
- 16–30, 9%
- More than 30, 9%
- 1 person, 4%
56% of companies report receiving less than 75 DSARs in 2020.

The number of DSARs respondents report receiving in 2020

- 0: 4%
- 1-25: 39%
- 26-75: 13%
- 76-300: 17%
- 301-600: 8%
- 601-1000: 6%
- More than 1,000: 13%
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

- United States: 33%
- European Union: 53%
- Non-EU Europe: 9%
- Other: 5%

- Software and services: 50%
- Retail: 16%
- Financial services: 13%
- Banking: 9%
- Marketing: 6%
- Other: 6%
The vast majority of DSARs originate from consumers.

Main profile of DSARs requestors

- Consumers: 70%
- Current employees: 8%
- Former employees: 7%
- Other: 15%
**Survey Findings: Data rights defined, why they matter and who addresses them**

**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

<table>
<thead>
<tr>
<th>Requestor</th>
<th>United States</th>
<th>European Union</th>
<th>Non-EU Europe</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consumers</td>
<td>64%</td>
<td>75%</td>
<td>60%</td>
<td></td>
</tr>
<tr>
<td>Current employees</td>
<td>4%</td>
<td>12%</td>
<td>10%</td>
<td></td>
</tr>
<tr>
<td>Former employees</td>
<td>7%</td>
<td>9%</td>
<td>5%</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>14%</td>
<td>15%</td>
<td>26%</td>
<td></td>
</tr>
</tbody>
</table>

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

*Indicates a statistically significant difference.*
Half of the respondents report honoring DSARs from anyone globally.

To whom do companies provide individual data rights?

- EU residents: 39%
- California residents: 25%
- Brazilian residents: 5%
- Residents in other location(s) where the law requires it: 22%
- Anyone in the U.S.: 9%
- Anyone globally: 50%
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

- EU residents
  - United States: 45%
  - European Union: 45%
  - Non-EU Europe: 26%
  - Other: 8%

- California residents
  - United States: 2%
  - European Union: 52%
  - Non-EU Europe: 0%
  - Other: 2%

- Brazilian residents
  - United States: 1%
  - European Union: 10%
  - Non-EU Europe: 2%
  - Other: 4%

- Residents in other location(s) where the law requires it
  - United States: 12%
  - European Union: 31%
  - Non-EU Europe: 17%
  - Other: 26%

- Anyone in the U.S.
  - United States: 1%
  - European Union: 18%
  - Non-EU Europe: 0%
  - Other: 0%

- Anyone globally
  - United States: 37%
  - European Union: 55%
  - Non-EU Europe: 67%
  - Other: 75%

*Indicates a statistically significant 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.

<table>
<thead>
<tr>
<th>Types of DSARs handled by organizations</th>
<th>Requests received by organizations</th>
<th>Supported by organizations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access requests</td>
<td>83%</td>
<td>97%</td>
</tr>
<tr>
<td>Deletion requests</td>
<td>77%</td>
<td>92%</td>
</tr>
<tr>
<td>Rectification requests</td>
<td>23%</td>
<td>83%</td>
</tr>
<tr>
<td>Portability requests</td>
<td>7%</td>
<td>59%</td>
</tr>
<tr>
<td>Opt out/do not sell</td>
<td>46%</td>
<td>73%</td>
</tr>
<tr>
<td>Opt in</td>
<td>9%</td>
<td>51%</td>
</tr>
</tbody>
</table>

- Access requests: 83% received, 97% supported
- Deletion requests: 77% received, 92% supported
- Rectification requests: 23% received, 83% supported
- Portability requests: 7% received, 59% supported
- Opt out/do not sell: 46% received, 73% supported
- Opt in: 9% received, 51% supported
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

- **Access requests**
  - United States: 78%
  - European Union: 88%  
  - Non-EU Europe: 88%
  - Other: 81%

- **Deletion requests**
  - United States: 85%
  - European Union: 81%
  - Non-EU Europe: 50%
  - Other: 81%

- **Rectification requests**
  - United States: 13%
  - European Union: 30%
  - Non-EU Europe: 29%
  - Other: 35%

- **Portability requests**
  - United States: 7%
  - European Union: 8%
  - Non-EU Europe: 5%
  - Other: 10%

- **Opt out/do not sell**
  - United States: 55%
  - European Union: 39%
  - Non-EU Europe: 38%
  - Other: 37%

- **Opt in**
  - United States: 7%
  - European Union: 10%
  - Non-EU Europe: 14%
  - Other: 10%

*Indicates a statistically significant 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

- Manually with a front-end portal or similar submission form: 82%
- Backend data fulfillment automation software or tool(s): 24%
- Data discovery software or tool(s): 13%
- Consent and preference management software or tool(s): 15%
- We don't currently manage DSARs: 6%
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.

Here are the current management strategies:

- Manually with a front-end portal or similar submission form: 91%
- Backend data fulfillment automation software or tool(s): 26%
- Data discovery software or tool(s): 17%
- Consent and preference management software or tool(s): 13%
- We don't currently manage DSARs: 2%
Nearly half of the respondents process DSARs via email or by phone.

**How organizations intake DSARs**

- **Email/phone**: 47%
- **The organization's own self-service online portal**: 23%
- **Third-party privacy portal**: 10%
- **Case management tool (e.g., ServiceNow or ServiceCloud)**: 7%
- Not sure: 2%
- **Other**: 12%
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

- **Email/phone**
  - United States: 31%
  - European Union: 58%
  - Non-EU Europe: 67%
  - Other: 67%

- **The organization's own self-service online portal**
  - United States: 31%
  - European Union: 20%
  - Non-EU Europe: 12%

- **Third-party privacy portal**
  - United States: 16%
  - European Union: 10%
  - Non-EU Europe: 4%

- **Case management tool (e.g., ServiceNow or ServiceCloud)**
  - United States: 7%
  - European Union: 7%

- **Not sure**
  - United States: 3%
  - European Union: 1%
  - Non-EU Europe: 5%

- **Other**
  - United States: 11%
  - European Union: 12%

- Indicates a statistically significant 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

- Email only: 47%
- Photo identification (e.g., driver’s license or passport): 47%
- Login with email and password: 30%
- Challenge question: 29%
- Identity proofing platform: 15%
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**

<table>
<thead>
<tr>
<th>Method</th>
<th>United States</th>
<th>European Union</th>
<th>Non-EU Europe</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email only</td>
<td>55%</td>
<td>30%</td>
<td>37%</td>
<td>22%</td>
</tr>
<tr>
<td>Photo identification (e.g., driver's license or passport)</td>
<td>43%</td>
<td>59%</td>
<td>63%</td>
<td>69%</td>
</tr>
<tr>
<td>Login with email and password</td>
<td></td>
<td></td>
<td>35%</td>
<td></td>
</tr>
<tr>
<td>Challenge question</td>
<td></td>
<td></td>
<td>31%</td>
<td></td>
</tr>
<tr>
<td>Identity proofing platform</td>
<td></td>
<td></td>
<td>33%</td>
<td></td>
</tr>
</tbody>
</table>

*Indicates a statistically significant 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.

**How organizations verify a data subject’s identity**

In the financial services industry

- Photo identification (e.g., driver's license or passport) - 64%
- Email only - 36%
- Challenge question - 36%
- Identity proofing platform - 26%
- Login with email and password - 23%
Most organizations search databases and applications to identify data for DSAR responses.

<table>
<thead>
<tr>
<th>Data stores used to search for personal and sensitive data for DSAR responses</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Databases</td>
<td>87%</td>
</tr>
<tr>
<td>Applications (e.g., SAP, Salesforce, Workday and ServiceNow)</td>
<td>68%</td>
</tr>
<tr>
<td>Files in file stores in Cloud (e.g., O365, Box, Gdrive)</td>
<td>49%</td>
</tr>
<tr>
<td>Files in file servers (e.g., NetApp and EMC)</td>
<td>35%</td>
</tr>
<tr>
<td>Big data and data lakes</td>
<td>28%</td>
</tr>
<tr>
<td>Mainframe</td>
<td>16%</td>
</tr>
<tr>
<td>noSQL</td>
<td>8%</td>
</tr>
<tr>
<td>Data in motion</td>
<td>5%</td>
</tr>
<tr>
<td>Other</td>
<td>6%</td>
</tr>
<tr>
<td>Unsure</td>
<td>7%</td>
</tr>
</tbody>
</table>
Half of the respondents use an organizational survey to build their data inventory, and only a third use privacy-specific data discovery.
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

- Manually search for a keyword, like email or name: 34%
- Targeted query on a table or application programming interface using a keyword: 10%
- Purpose-built privacy tool: 5%
- A combination of the above: 40%
- Not sure: 10%
- Other: 2%
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

- Manually search for a keyword, like email or name: United States - 26%, European Union - 31%, Non-EU Europe - 43%, Other - 40%
- Targeted query on a table or application programming interface using a keyword: United States - 9%, European Union - 19%, Non-EU Europe - 2%, Other - 6%
- Purpose-built privacy tool: United States - 4%, European Union - 5%, Non-EU Europe - 8%, Other - 13%
- A combination of the above: United States - 35%, European Union - 31%, Non-EU Europe - 45%, Other - 31%
- Not sure: United States - 9%, European Union - 5%, Non-EU Europe - 8%, Other - 1%
- Other: United States - 1%, European Union - 1%, Non-EU Europe - 2%, Other - 4%

*Indicates a statistically significant difference.*
Contact

Sarah Hospelhorn
BigID
VP, Product & Content Marketing
165 Mercer St., 4th Floor, New York, NY, 10012
sarah@bigid.com