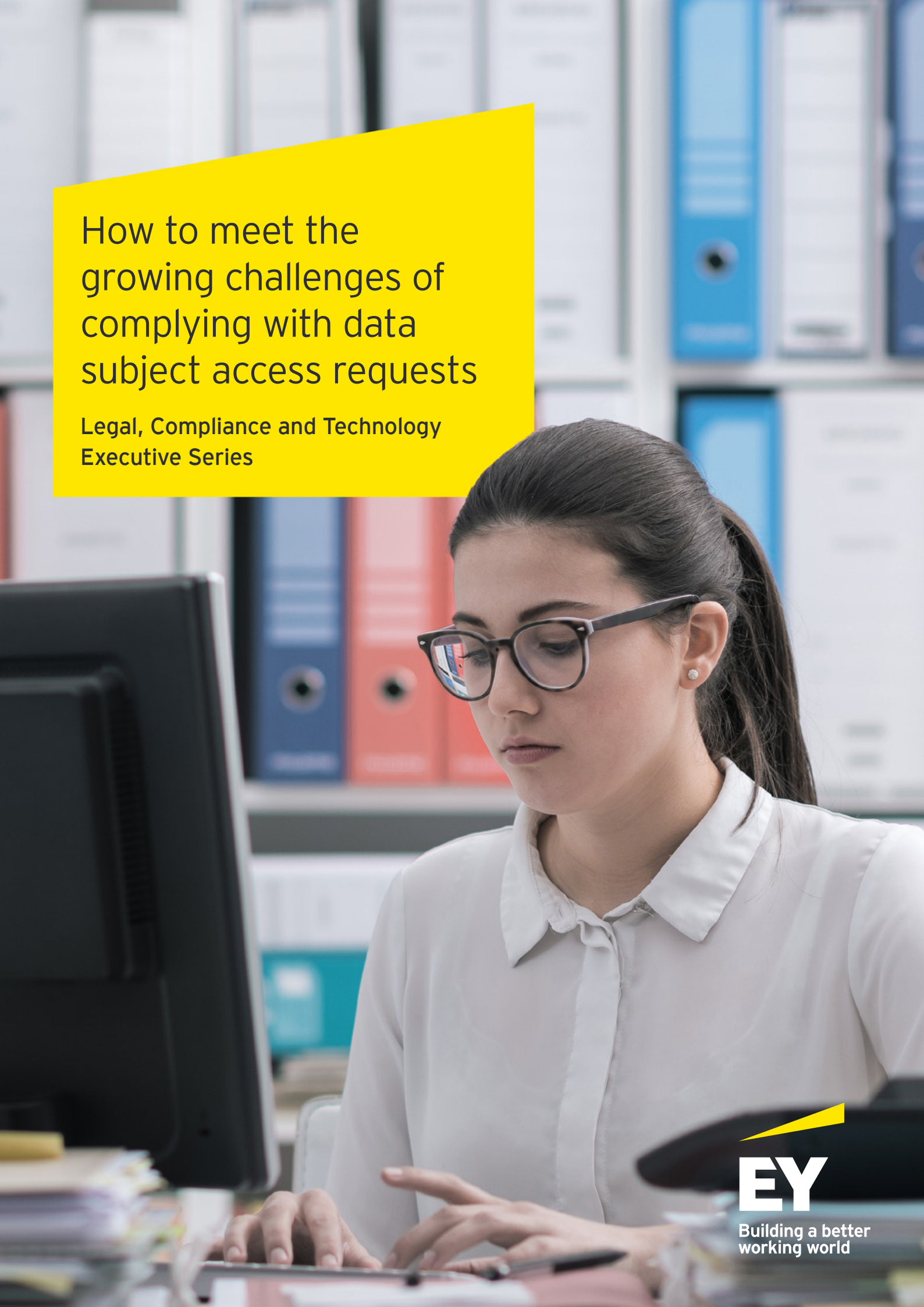
How to meet the growing challenges of complying with data subject access requests

Legal, Compliance and Technology Executive Series



EY
Building a better working world

Of special interest to:

- Legal counsel
- Corporate security officers
- Information security executives
- Compliance executives
- Risk management executives
- Internal audit

Introduction

Major DSAR noncompliance fines

- **€20 million:** Croatian bank failed to give 2,500 customers access to their data
- **€9.55 million:** German telecom provider gave callers personal information without properly verifying their identities
- **€0.8 million:** Dutch credit registration bureau made it overly difficult and expensive for people to access their data and have it deleted

Source: *Major GDPR Fine Tracker*, Coreview, accessed 21 September 2020.

> "Many businesses also promote respect for personal data as a competitive differentiator and a selling point on the global marketplace, by offering innovative products and services with novel privacy or data security solutions.
>
> **European Commission report**
> **24 June 2020**

Since 2018, organizations covered by the EU's General Data Protection Regulation (GDPR) have had to disclose personal data upon request of the data subject or face stiff penalties. Besides the GDPR, more and more data protection and privacy laws, such as the California Consumer Privacy Act (CCPA) and Brazil's General Data Protection Law (LGPD), are requiring organizations to identify personal data; disclose, correct or delete data upon request; and demonstrate regulatory compliance. Organizations that fail to comply with relevant legislation face not only litigation and fines that can run into the millions but also reputational damage that can cost customers.

This paper explores data subject access request (DSAR) compliance challenges that are common to many data protection and privacy regulations. For the ease of discussion, we use the GDPR definitions of "data subject" and "data subject access requests" (DSARs) as general references.

Since the COVID-19 pandemic began, many organizations have experienced an increasing number of DSARs, mostly from displaced employees.[1] The shift to a remote workforce is also making processing DSARs more challenging. These factors make it more important than ever for organizations to create a clear compliance strategy and workflows for fulfilling DSARs.

According to a 2020 BigID-IAPP survey of privacy professionals globally,[2] many organizations are planning investments in data rights management to improve their governance, risk, compliance and security efforts. Demonstrating strong data protection and privacy controls can also help companies protect their brands and gain competitive advantage. Nearly one-third of global consumers surveyed by Cisco said they are willing to spend time and money to protect their data and have switched companies or providers over their data policies.[3]

1 *DSARs and the impact of COVID-19*, May 2020, www.guardum.com.

2 The State of Data Rights, BigID-IAPP, October 2020.

3 *Consumer Privacy Series: The growing imperative of getting data privacy right*, Cisco, www.cisco.com, November 2019.

DSARs are becoming one of the most difficult aspects of data privacy compliance

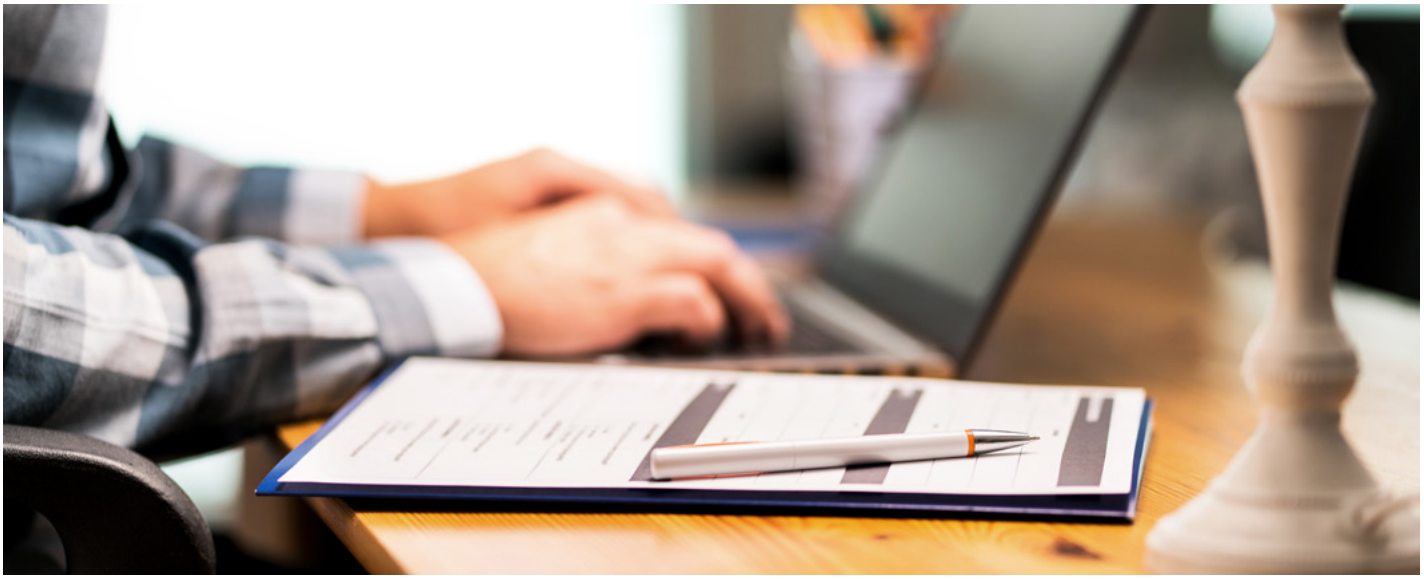
Two years after the enforcement of the GDPR, companies are still struggling with DSAR compliance. A Gartner survey found that it costs an average of US$1,400 for organizations to manually process a DSAR, with most taking more than two weeks to respond.[4] The most difficult aspects of processing DSARs involve locating personal data that is in an unstructured format, monitoring data protection practices of third parties and data minimization.[5]

Many data privacy regulations provide similar rights for individuals to access, correct or delete personal data held by an organization. Data subjects can also request information on how their data is processed, stored and shared.

It is important for legal counsel to carefully consider the differences between privacy regulations. For example, the differences in the definition of individual rights under the GDPR and the CCPA will have impact on the design of DSAR workflows. Variances mean that any workflows created for one regulation may require modifications to ensure compliance with another. Organizations can benefit from assessing whether existing processes can be revised to improve compliance, efficiency and cost-effectiveness.

Important differences between GDPR and CCPA data subject rights

- The GDPR gives rights to "data subjects" – any identified or identifiable EU resident, while the CCPA protects "consumers" who are California residents. Employees are expected to obtain rights in 2021.
- Under the GDPR, organizations have one month to respond to a verifiable request, with a two-month extension allowed for complex requests. The CCPA mandates an initial 45-day response deadline with one 45-day extension allowed when reasonably necessary.
- While both laws provide the right to delete personal information that is no longer needed for the purpose it was collected, each law includes a number of different exemptions.



[4] *Market Guide for Subject Rights Request Automation*, Gartner, 21 February 2020, www.gartner.com.

[5] *IAPP-EY Annual Privacy Governance Report 2019*, IAPP-EY, 2019, www.iapp.org.

Sharing data with third-party vendors poses additional challenges

Organizations that share personal data need to ensure their third parties are contractually bound to offer adequate data protection and privacy compliance. When an organization receives a request to delete personal data, the GDPR requires notification to all downstream parties that received or processed the subject's personal information. Under the GDPR, data processors share responsibility for fulfilling requests with data controllers.

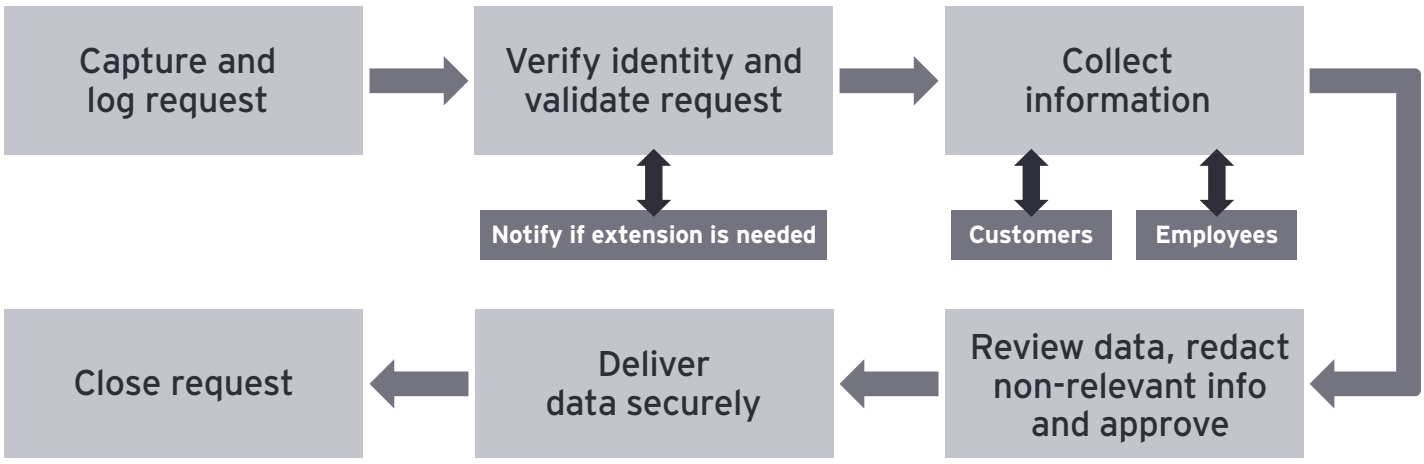
Processor due diligence is specifically outlined under Article 28 of the GDPR. To meet the accountability and responsibility requirements, controllers should regularly assess how vendors protect the personal data they process. Both the GDPR and the CCPA require detailed written contracts between businesses and vendors that process data.

Organizations who invest in workflow automation and data analytics can reduce the time and costs involved in third-party due diligence while gaining risk and business insights.

Key considerations in DSAR workflow design

A DSAR requires a sophisticated chain of events, from intake of the request, identity authentication and processing, to reporting and delivery. Building a standard methodology is critical for streamlining the process, meeting relevant regulatory and legal requirements, and engaging all stakeholders in an effective and efficient manner. Considering that the data privacy regulatory landscape is still fast evolving, a clearly-defined workflow can help an organization stay agile and effectively respond to changing compliance requirements.

Chart 1. Basic DSAR workflow



When designing a DSAR workflow, there are some important performance indicators to consider:

- **Turnaround —** time needed to fulfill a request. Organizations should track the time needed for each part of their workflow to identify bottlenecks and areas for improvement.
- **Cost —** financial and human resources required to fulfill a request. Businesses that calculate this only by the person-hour rate of the team processing requests may miss the opportunity losses incurred when diverting resources. Third-party billing must also be included.
- **Capacity —** the volume of requests a business can fulfill in the required time frame. Businesses that cannot address all requests within the mandated deadlines face penalties and reputational damage.
- **Scalability —** the ability to address the global expansion of data privacy regulations, resulting in DSAR growth. Multinational organizations need to understand how a workflow that satisfies the regulatory requirements of one jurisdiction might also fulfill the requirements of another country.

One of the biggest challenges of creating an efficient DSAR workflow is coordination among various stakeholders, not just the legal and compliance function. The IT team will become increasingly critical as DSAR workflows require the support of various technologies and systems. Cybersecurity professionals need to provide expertise on data protection issues as personal data moves from secured storage to delivery. The client-facing functions can be an excellent resource for creating workflows that align with customer experience.

Companies often struggle with verifying the identity of the requestor, gathering data (especially in unstructured formats) that may be stored across multiple departments and in siloed systems, and addressing the legal issues related to disclosure. This means various functions must work together to create a workflow, with each department taking ownership for its part of the process. For example, responding to employee data requests requires the compliance and legal functions to work closely with HR and business leaders to consider the rights of impacted coworkers and managers.

Building a robust DSAR workflow begins with data mapping

Businesses can't execute DSARs without knowing what personal data they hold and where to access it. Data mapping is essential to gaining a clear understanding of personal data governed by relevant privacy legislation. Data maps align personal data to an organization's information systems and provide a clear view of data sources that may be requested, including data kept by third parties. Organizations that know precisely where personal data is stored can better protect that information, and apply appropriate retention and minimization policies.

Data mapping helps track data through its life cycle, from collection and processing to retention or removal. As personal data moves from one jurisdiction to another, it may be subject to different privacy regulations. Data mapping also helps to determine whether personal information is used or stored beyond its original, lawful purpose. Storing identical personal data in various formats spread among different systems violates GDPR data minimization regulations and makes responding to DSARs much more time consuming and costly. For businesses handling rectification or data deletion requests, good data governance is essential to confirm that data corrected or deleted in one system is automatically updated everywhere.

More than half of privacy professionals surveyed by BigID-IAPP say their companies plan to invest in data discovery, inventory and mapping to manage data rights.

Use technology to enhance DSAR workflow

Building a consistent and efficient DSAR workflow requires technology. Many companies are retooling traditional electronic discovery tools and workflows used in document reviews for DSAR compliance because of their ability to handle unstructured data and address complex data processing requirements. Machine-learning algorithms can continually improve the ability to locate relevant data across multiple systems, reducing costs and increasing capacity. Investing in automation technologies can make the DSAR workflow more accurate and shift compliance professionals into higher-value tasks.

Self-service portal for DSAR intake and identity verification

A basic online DSAR intake tool doesn't necessarily require complex technologies or skills to build. Done right, it can save resources, bring consistency and improve customer relationships. Strong identity verification is critical to help prevent data from falling into the wrong hands. There are also many ways to augment an intake tool using AI and automation technologies. Ultimately, an advanced, self-service portal can not only capture requests but also verify identities, leading to an automated search for the relevant personal data. A third of the BigID-IAPP respondents plan to invest in consent and preferences management and a consumer privacy portal.

Data redaction in review and processing

Data redaction tools are indispensable during DSAR review and processing. They help to reliably obfuscate or remove sensitive information unrelated to the data subject and prevent it from being shared.

Data encryption for secure delivery

The final step of the DSAR fulfillment process needs to be handled with appropriate security measures that reduce the risk of a data breach. Data encryption technologies are often used to safely transfer information to the data subject.

Case management with audit trail

A DSAR workflow requires the coordinated efforts among businesses and diverse support functions such as customer service, IT, records management, compliance and legal. A robust case management tool is essential to help all DSAR stakeholders work together. It should take into consideration all of the steps resulting from a DSAR, including how requests are collected, processed, reported and delivered. The case management tool should allow legal professionals to conduct reviews for relevancy, privilege and confidentiality; offer global accessibility; provide clearly defined key performance indicators; and include an audit trail that can stand up to regulatory scrutiny.

Key takeaways

Building an effective DSAR compliance program requires cross-functional collaboration, good data mapping and innovative use of technology to create efficient, standardized workflows. Businesses that use unwieldy manual processes to process DSARs may fail to meet regulatory deadlines and other requirements, running the risk of significant fines and damage to their brand.

Organizations cannot lose sight of scalability. Whether a company has cross-border dealings or not, the fast-evolving privacy compliance landscape will likely require it to constantly tweak its DSAR program to take into account changing requirements, as well as new regulations.

Advanced tools, such as self-service privacy portals, AI-assisted automation and sophisticated case management, will increasingly become the norm for responding to requests. This will help companies to lower costs, maintain regulatory compliance and satisfy a public that is increasingly placing a premium on privacy.

EY | Assurance | Tax | Strategy and Transactions | Consulting

About EY
EY is a global leader in assurance, tax, strategy, transaction and consulting services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. For more information about our organization, please visit ey.com.

About EY Forensic & Integrity Services
Embedding integrity into an organization's strategic vision and day-to-day operations is critical when managing complex issues of fraud, regulatory compliance, investigations and business disputes. Our international team of more than 4,000 forensic and technology professionals helps leaders balance business objectives and risks, build data-centric ethics and compliance programs, and ultimately develop a culture of integrity. We consider your distinct circumstances and needs to assemble the right multidisciplinary and culturally aligned team for you and your legal advisors. We strive to bring you the benefits of our leading technology, deep subject-matter knowledge and broad global sector experience.

EYG no. 007529-20Gbl
WR #2010-3598477
ED None

ey.com

Authors:

Meribeth Banaschik
Partner, Forensic & Integrity Services
Ernst & Young GmbH
Wirtschaftsprüfungsgesellschaft
Germany
meribeth.banaschik@de.ey.com

Gesa Pari Schatz
Senior Manager, Forensic & Integrity Services
Ernst & Young GmbH
Wirtschaftsprüfungsgesellschaft
Germany
gesa.pari.schatz@de.ey.com

Jenny Le
Manager, Forensic & Integrity Services
Ernst & Young GmbH
Wirtschaftsprüfungsgesellschaft
Germany
jenny.w.le@de.ey.com

For more information:

Visit ey.com/Forensics