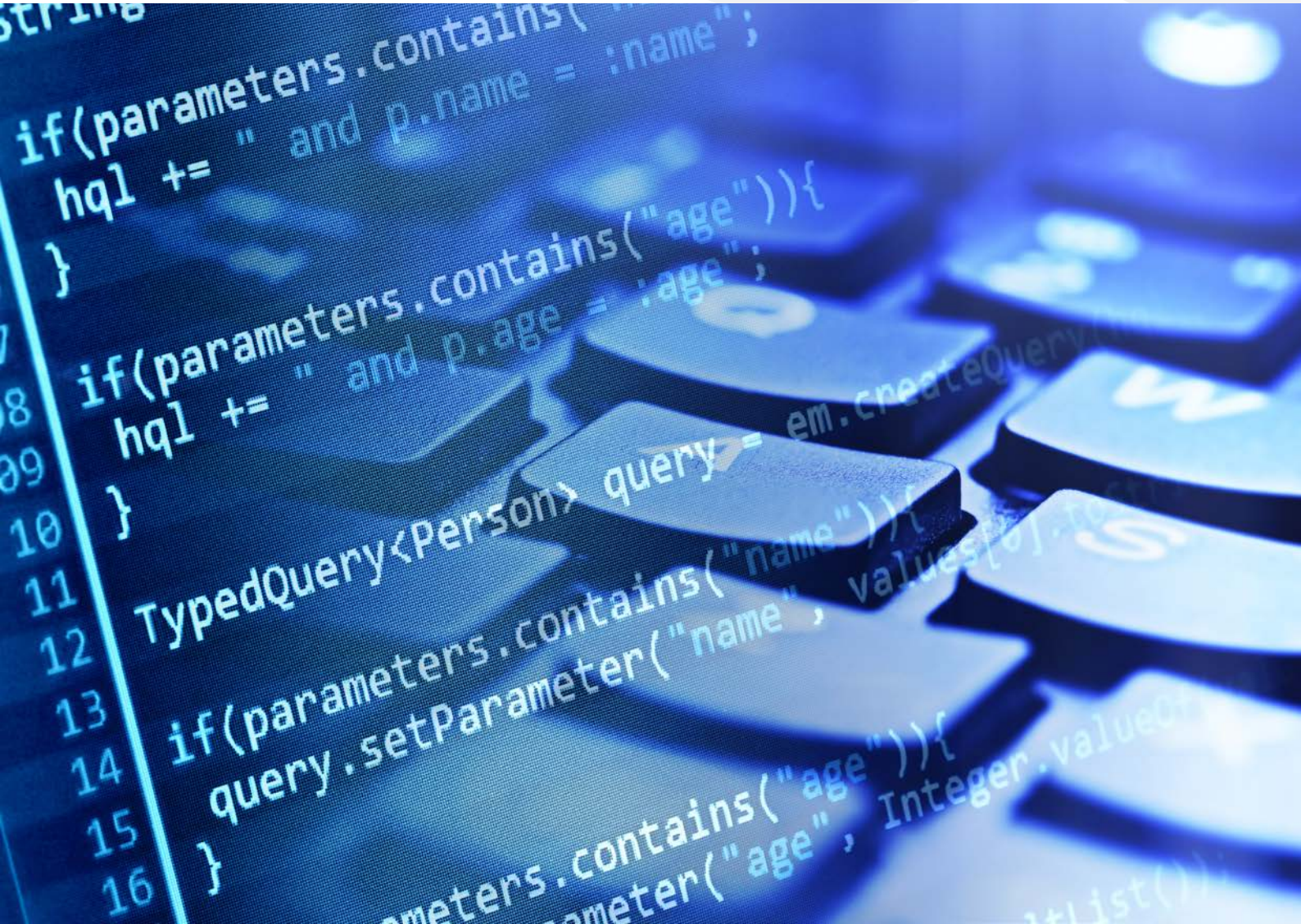
opentext™

WHITE PAPER

Efficient data privacy compliance using e-discovery workflows



Contents

According to IDC, "data subject access requests… follow identical workflows to that of litigation response. The right eDiscovery provider will be able to quickly and effectively respond to data subject access requests and protect the organization from related compliance violations."[1]

1 IDC Worldwide eDiscovery Software Forecast, 2019–2023, Doc # US45344219, July 2019

Executive summary

In civil litigation or regulatory inquiries and investigations, parties engage in electronic discovery, also known as e-discovery, which is the process of identifying, preserving, collecting, reviewing, and producing electronically stored information that is potentially relevant in the matter to the requesting party. The goal is to discover (i.e., find) potentially relevant documents to produce, while identifying privileged and other sensitive data, such as personally identifiable information (PII) pursuant to data privacy requirements, to withhold from the requesting party for production (e.g., the opposing party, government agency or regulatory authority).

E-discovery platforms designed to find potentially relevant information in investigations and litigation contain significant data privacy capabilities for the primary purpose of protecting against contravening data privacy regulations and disclosing personal data to requesting parties. These same e-discovery tools and workflows can also be used to fulfill two other prevalent use cases: itemizing the specific data exposed through data breaches, and enabling efficient subject rights request response programs, particularly when those requests involve large volumes of diverse documents and data.

Data privacy regulations have created a new mandate for organizations regarding how they manage the personal information of their customers and employees, one which requires holistic changes in how they collect, manage, protect, and process data that contributes to defining the identity of these individuals. The incentives to comply are material, including non-compliance fines of up to four percent of revenue under the General Data Privacy Regulation (GDPR), payments of $100 to $750 per person whose data is breached under the California Consumer Privacy Act (CCPA), and loss of reputation and business for vendors that fail to act as responsible stewards of data privacy.

Executable rights are among the most challenging aspects of data privacy laws and have an impact on the appropriate technology-assisted workflows organizations take in response to data subject requests. These rights vary between the various regulations but include the right of individuals to instruct organizations that process their personal information to provide a report on what data is held on them, opt out from further use of their data, request that the data be deleted, or have the data provided to them or a third-party in an accessible format.

E-discovery technology is an effective approach for responding to the daunting volume of legitimate requests within the prescribed timelines of 30 days for GDPR and 45 days for CCPA.

The methods and tools used to collect, review, analyze, and act on privacy rights requests are the same as those that organizations apply in their litigation, investigation, and regulatory response programs. Many legal departments find that the integrated data processing, automation, analytics, machine learning, PII detection and redaction and production tools in e-discovery platforms, such as OpenText™ eDiscovery are easily repurposed for handling DSAR/SRR volumes at scale—efficiently and within tight timelines.

Disclaimer

Organizations are responsible for ensuring their own compliance with the laws and regulations to which they are subject, including the GDPR and CCPA.

Organizations are solely responsible for obtaining advice of legal counsel as to the interpretation of and what they may need to do to comply with any such relevant laws and regulations. This document is not legal advice. The products, services, and approaches described herein are not suitable for all client situations. OpenText does not represent that its services or products will ensure that clients are in compliance with any law or regulation.

The world of data privacy

Traditionally, organizations collected digital personal information from their customers and treated it as their own to use or sell as they please. Regulations were slow to keep up with the information age, as identity theft and cyberthreats took center stage. Numerous data breaches started occurring, such as the breach of data from all three billion Yahoo! users in the 2013, making the issue hit home for many organizations and consumers.

Regulators are executing on demands for a fundamental shift in data privacy. The core objective of data privacy regulation is to legally assign the ownership of personal information to the people described by that data so that individuals are the undisputed owners of their identities and of all of the data that contributes to defining it.

The implications for organizations are far-reaching and complex. In addition to transforming their methods for collecting, storing, managing, and protecting personal information, organizations also need to determine how to comply with the extensive executable rights conferred to employees and customers.

Essential rights? The anchors of data privacy

GDPR and CCPA are the global models for how customer privacy rights are defined and executed. These rights are conferred as overarching natural rights to know how their data will be used and managed before providing it, and executable rights that customers can exercise as they please.

Executable rights

Despite variance in the details, GDPR and CCPA proclaim a similar set of executable rights that individuals can exercise with regard to their personal information. These include:

- the right to request a report on what information is held on them for what purposes.
- the right to opt-out from future use of their data.
- the right to have their data delivered to themselves (GDPR and CCPA) or others (GDPR).
- the right to have their data deleted.

2 Alpin – GDPR fines list
3 DLA Piper, GDPR data breach survey: January 2020

GDPR adds the right to request that personal information be amended.

GDPR (Data Subject Access Rights – DSARs) and CCPA (Subject Rights Requests – SRRs) dictate that organizations must provide clear and accessible instructions for customers to submit requests, including both electronic and phone access.

Notably, organizations are prohibited from charging fees for processing Subject Rights Requests except in circumstances where the requests are repetitive. This puts a burden on organizations for absorbing the cost of legitimate DSARs/SRRs but protects them from unintended use of the laws.

Developing a defensible and cost-effective subject rights request workflow

This white paper focuses on the programmatic aspects and the application of e-discovery technology to the core of DSAR/SRR workflows to collect, cull, review, de-risk, and produce reports in response to legitimate requests.

As part of the programmatic aspects of requests, organizations should also familiarize themselves with DSAR/SRR exemption rules, such as the ability to deny requests to delete data required to support ongoing legitimate business processes. For example, organizations do not have to delete someone's credit card information if the card is being used to process monthly bills on an open annual contract. A detailed list of exemptions is provided as bonus content in the appendix.

Another complexity is that executable rights can be transferred to agents, informal or formal, who can act on an individual's behalf. To avoid providing sensitive information to an imposter, organizations must verify the identity of the customer, the identity of the agent and the validity of the appointment to act on the customer's behalf before processing the request.

Organizations do not typically use e-discovery platforms for DSARs/SRRs from customers because the requests often involve narrow quantities of data housed in a single or small set of information systems. However, in reality, many requests from employees are often much more complex; they involve data over longer time periods and that data is typically dispersed across numerous systems in diverse formats.

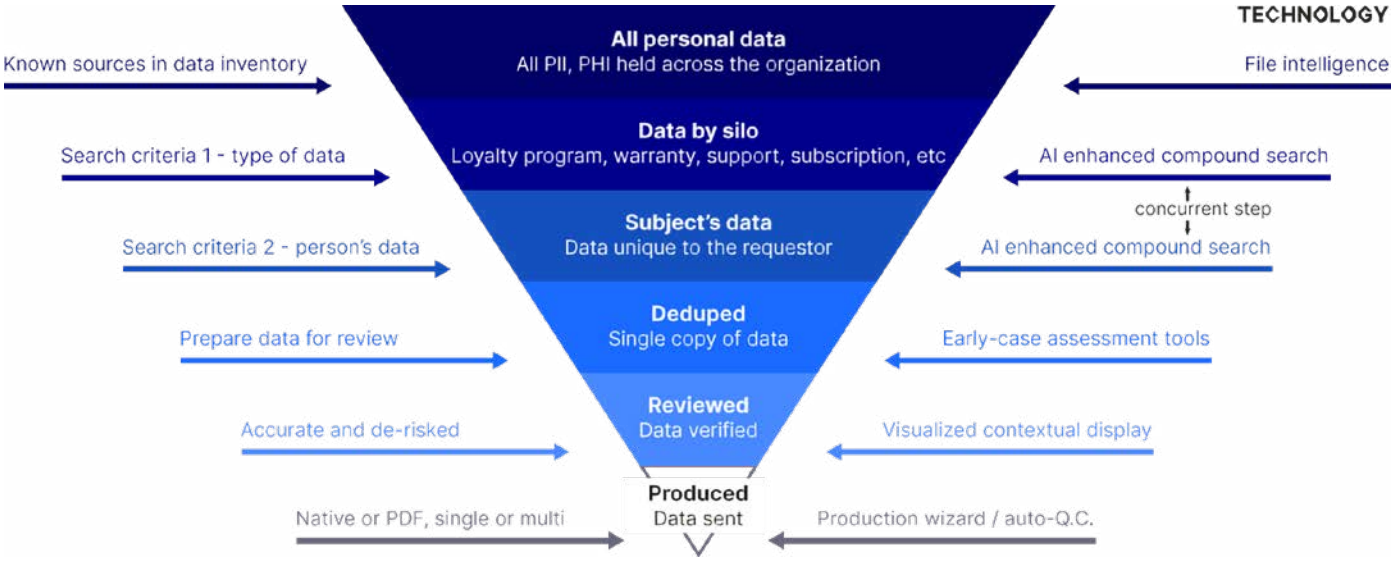
In scenarios in which requests may be more complex, e-discovery platforms are the ideal solution because DSARs/SRRs from employees closely resemble review processes in litigation and investigations in which the objective is to distill relevant data from within huge volumes of background data, often from disparate systems within the organization, while identifying sensitive data, such as PII.

DSAR/SRR Workflow Framework

As mentioned previously, data subject access requests follow identical workflows to that of litigation document review. In both cases, the goal is to find the relevant data among large volumes of extraneous content as efficiently as possible. To achieve this, tools must be applied to search, deduplicate, and de-NIST the data to surface the most accurate and inclusive set of initial content for review as possible, while minimizing non-relevant data. Analytics and machine learning, such as technology- assisted review (also known as predictive coding) can then be applied to identify the most relevant content, while pre-configured PII detection libraries, customizable RegEx pattern search and automated redaction tools protect sensitive and confidential information. Finally, the relevant documents are produced to the requesting party.

The value of automated workflows is apparent across all aspects of the review process. Just connecting to the relevant content stores across email, CRM, ECM, file shares, cloud, hybrid cloud, and other systems can take two weeks or more. Not only is this costly and inefficient, the time-crunch for completing subject rights requests becomes even tighter. Turnkey connectors such as those in OpenText eDiscovery effectively address collections challenges and allow more time to apply predictive coding and related technologies for better, less stressful review.

The illustration below shows how e-discovery technology can surface relevant data from large document sets quickly and efficiently.



Efficient use of e-discovery technology to winnow down large document collections to the relevant personal data

Below is an example of specific e-discovery technology tools that can help organizations efficiently fulfill DSARs/SRRs. E-discovery technology delivers across the entire workflow from data identification to data delivery in a single platform that can be flexibly deployed to support specific client needs and processes. Integrated culling, review, machine learning, redaction, and production automation improves efficiency in order to minimize DSAR/SRR costs while lowering the risk of disclosing incorrect information or other people's PII.

E-discovery tools	Definition	Application to DSAR/SRR workflows
Connectors	Turn-key connectors to common content stores for access to content wherever it resides.	Connecting to content stores that house personal data is laborious and costly without turn-key connectors.
Multi-faceted concurrent search	AI-enhanced search that allows for multiple concurrent queries to be fielded in tandem. For example, in OpenText eDiscovery it is possible to run several Boolean and natural language searches in a single query for optimal and efficient results.	Reduces the steps to find relevant personal information by avoiding sequential individual searches. Narrow in from all personal data to the data relevant to the requestor.
Processing and culling	Process the documents and apply OCR, as needed, to make the data searchable, deduplicate and de-NIST.	Minimizes the volume of documents that need to be reviewed by eliminating erroneous files and duplicate instances of personal data.
Smart filters	Rapidly isolate key data with dozens of stackable filters based on metadata, content and customizable work-product.	Quickly click from lists of types of personal data to find the requestor's data.
Predictive filters	Find relevant data faster with predictive filters by using known relevant data as examples to uncover similar data that is also likely to be relevant.	Use the results from previous rights request searches to expedite finding the right data for the current search.
Technology-assisted review (also known as predictive coding)	Continuous machine learning that automates the prioritization of documents for review, substantially reducing "eyes on" review of every document for efficiency and improved accuracy.	Prioritize the most relevant documents containing personal information for review.
Entity identification	Integrated detection tools that automatically surface the names of people, organizations and places.	Isolate the requestor easily and quickly find the names of people entwined with the requestor's data to remove third-party data.
Visualization	Visualized display of potentially relevant content with key indicators and criteria clearly presented to facilitate fast and accurate review.	The contextual display of personal data helps reviewers assess the search results and move quickly through fulfilling each request.
Automated data detection and redaction	Auto-identify sensitive content in any identifiable pattern, such as PII, PCI, PHI, and NPI, and automatically redact it in bulk before review or production.	Redaction is essential to de-risk sending reports on personal data and for de-risking at scale.
Production Wizard	Select from pre-configured options for how the discovery set is produced.	Streamlines the delivery of data subject reports.

Subject rights requests workflows in detail

Now, let's look at each stage of the DSAR/SRR process and how e-discovery tools are essential to efficiently fulfilling the requests.

Collect, cull, and review responsive data

Collect data and constrain results: Use turn-key connectors to the relevant data sources to expose all of the potentially relevant content to the review tools. Constrain data to the specific individual and collect the initial data set using smart filters and multi-faceted search.

Relevant e-discovery tools: Connectors to common content stores; smart filters; multifaceted concurrent search.

Cull and process: Use automated content conversion tools to make data searchable, deduplicate and de-NIST to further refine the initial data set./

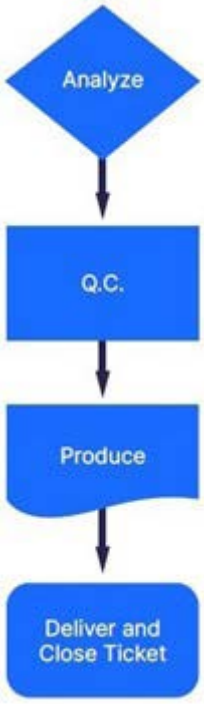
Relevant e-discovery tools: Data processing and early case assessment tools.

Analysis and review: Assess initial data set as accurate and complete per the specific request. Use machine learning, such as predictive coding, to automate the prioritization of documents for review that are likely to be most relevant to the search.

Relevant e-discovery tools: Predictive coding/ technology-assisted review.

Review for risk: Use automated PII detection and redaction tools to de-risk the refined data set, and automated tools to identify third-party names and redact data related to those individuals whose data may be comingled with the requestor.

Relevant e-discovery tools: Automated PII detection, redaction, and entity identification tools.



Analyze, conduct quality control (QC), produce, and deliver

Analyze: Monitor the progress of rights requests with interactive dashboards that detail the status of each request. Projects can be tracked down to the individual coding decisions within them to build a knowledge base of the most efficient path to relevant results for future requests.

Relevant e-discovery tools: Business intelligence dashboard.

QC: Conduct final approval of the refined data set. Use automated redaction QC tool to check that all data flagged for redaction has been properly redacted.

Relevant e-discovery tools: Automated redaction QC tools.

Produce: Produce the data report as appropriate in the desired format in alignment with the requirements of the request.

Relevant e-discovery tools: Production wizard.

Deliver and close ticket: Send the final data set to the requestor and/or third parties if they insist on data transfer (GDPR).

From onboarding data subject requests to collecting and reviewing the relevant data and preparing a final de-risked report for the data subject, e-discovery technology is critical for achieving the most efficient compliance within stringent timelines.

Essential takeaways

With growing data privacy regulations, many organizations are struggling with how to efficiently comply with data subject requests. The new rights afforded to individuals—customers and employees alike—pose significant challenges to organizations when identifying, verifying, and supplying the data back to the individual.

Fortunately, however, organizations need not reinvent the wheel with new technology, processes, and people. The very same technology and processes used for litigation and investigations can be applied to DSAR/SRR programs, allowing efficient compliance.

OpenText provides comprehensive, automated, and flexible technology that enables organizations to respond to DSARs/SRRs rapidly, leveraging OpenText eDiscovery to streamline the time involved in responding to requests and the overall resource overhead associated with compliance.

It facilitates the expedient retrieval of personal data from multiple data sources, culling to the potentially relevant documents, automating the redaction of personal information, machine learning to prioritize documents for review, and visualized data to speed assessment. This eliminates up to 80 percent or more of the irrelevant information, saving time and cost to derive the final deliverable for the requestor and expedite its delivery via standardized production tools.

When organizations need to scale without investing in additional resources, OpenText can provide supporting services to meet demands, including DSAR/SRR process consulting and collection services. Managed document review services leveraging OpenText eDiscovery are also available on a project basis to help clear subject rights request backlogs or on a program basis to offload the effort of a go-forward subject rights request routine.

Appendix – Bonus content to help determine which DSARs/SRRs require fast fulfillment

Executable rights exemptions

The following describes each of the executable rights and the exemptions that relate to each.

Executable rights	Exemptions
The right to know: • The types of data covered in right to know requests mirrors the breadth of data needed to fulfill the right to be informed. • The right to be informed pertains to the point of data collection, whereas right to know requests are exercised whenever an individual wants to know what data an organization holds on them, subject to specific exemptions. • As discussed above, GDPR and CCPA provide different levels of granularity regarding the amount of detail that needs to be provided.	**Right to know exemptions:** • The first exemption to right to know requests is easily overlooked and applies to all executable rights. Namely that, data privacy laws put the onus on the individual to reasonably verify their identity. If they are unable to do so, executable rights do not need to be fulfilled. • Companies may also push back on requestors if the request appears to be unfounded, excessive or repetitive. Requests can either be denied or fees can be charged. • CCPA further restricts right to know requests to data collected within the past 12 months and limits the frequency of requests to twice per year per individual.
Right to opt out: • GDPR is much broader than CCPA in terms of the right to opt out. • Under GDPR, individuals can opt-out of allowing their data to be used by an organization by withdrawing their consent at any time. • Data subjects can also specifically opt out of having their information used for direct marketing purposes but allow the organization to continue to use their data for other purposes related to their existing relationship. • Organizations must make the effort of opting out as easy as the consent to opt in. • The CCPA includes the right to opt out but only regarding the sale of personal information. In addition to being able to opt out of having their information sold at the time of data collection, individuals can go back to the organization at any time to prohibit them from ever selling it. If their data has already been sold, customers can submit a demand that their data not be re-sold any further by the initial organization and the third parties that have received it. • Under CCPA, a customer's general right to opt out is more directly housed within the right to have their information deleted.	**Right to opt out exemptions:** • Under GDPR, organizations can refuse opt out requests if they can demonstrate that the use of the individual's personal data involves a compelling legitimate interest that overrides the individual's privacy rights. • For example, trying to withdraw consent for using personal information when the person has a one-year subscription to a service would impede the organization's legitimate interest in processing the rest of the monthly bills. • Under CCPA, the right to prohibit the sale of personal information is absolute—there are no exemptions.

Executable rights	Exemptions
Right to have data transferred: • GDPR and CCPA contain similar rights for individuals to request that the personal information that an organization holds on them is packaged up and delivered in a structured, commonly used and machine-readable format. • CCPA only goes so far as obliging organizations to provide the data to the requestor. • GDPR places a further onus on organizations to send the data directly to third parties dictated by the customer.	**Right to data transfer exemptions:** • For both GDPR and CCPA, the right to data transfers only applies to data collected directly from the data subject. • This is further restricted under CCPA as the data provided by the customer within the past twelve months. • Except with complex multi-component applications, exercising the right of data transfer is not likely to achieve much for customers. Filling out a new form will typically be much easier than submitting a request and waiting for it to be processed as a Subject Right Request. • Organizations are welcome to push back on data transfer requests by letting the requestor know that fulfilling the request creates a privacy risk for them because it requires sending potentially sensitive data in exposed raw form.
Right to deletion: • The CCPA and GDPR are consistent in providing the right to individuals to request that their personal information be deleted. • Requests for data deletion should be fulfilled if there are no legal grounds for processing the data or the personal information is no longer required for the purpose for which it was collected. • Because of the irrevocable nature of deletion, this right comes with an extensive set of exemptions.	**Right to deletion exemptions:** Under the CCPA and GDPR, deletion requests can be denied if the data is: • reasonably aligned to the customer's ongoing relationship with the organization. • required to fulfill a legal obligation and / or is subject to legal hold. • necessary for ongoing research that supports the interests of public health. CCPA adds several other reasons to deny deletion requests if the data is: • material to an open or anticipated investigation into illegal activity. • required as part of a security investigation into malicious, deceptive, or fraudulent activity. • part of a contract between the business and customer. GDPR adds that deletion requests can be denied if deleting the data would compromise freedom of expression and free speech.

Connect with us

OpenText CEO Mark Barrenechea's blog ›

OpenText eDiscovery ›

Exemptions that can usually be determined up front	Exemptions that usually require review of the data

Purpose: Limiting the number of requests that have to go to full review.
• Right to know requests that are repetitive, spurious, or excessive in scope
• Right to opt-out requests that are aligned to the legitimate and ongoing interests of the organization
• Right to transfer requests that includes data beyond what was submitted by the customer
• Right to delete requests where the data is material to an ongoing relationship, included in a contract, or part of public health research
	Purpose: Protecting against legal risks and limiting the number of requests that need a report to be produced.
	• Right to know requests to determine when the data was collected – within the previous twelve months the data is subject to disclosure while older data is exempt (CCPA);
	• Right to delete requests that may involve:
	  • a legal obligation or content subject to legal hold ; (GDPR and CCPA).
	  • data material to an investigation into security risks or criminal actions (CCPA).

opentext™