opentext™

WHITE PAPER

# Efficient Data Privacy Compliance Using eDiscovery Workflows

Data privacy is rapidly transforming personal information management policy and practices. Technology-assisted programs to comply with and contain the costs of Data Subject Access Rights (DSARs) in the European Union and Subject Rights Requests (SRRs) in the United States is top of mind for affected organizations. This whitepaper discusses how eDiscovery technology used to review and produce documents for investigations, litigation and regulatory compliance matters can be applied to contain subject rights compliance costs.

opentext™

## Contents

opentext™

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]**

## Executive Summary

Data privacy regulations are creating a new mandate for organizations regarding how they manage the personal information of their customers and employees. Organizations must implement 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 4 percent of revenue under the General Data Privacy Regulation (GDPR), payments of $100 to $750 per person whose data is breached under the California Customer Privacy Act (CCPA), and loss of reputation and business for vendors that do not act as responsible stewards of data privacy.

The prescription for developing and implementing compliant policies and programs is well documented. In addition to establishing cross-functional data privacy committees, organizations need to, at a minimum:

understand and adapt to the new consent requirements;

- conduct and maintain an inventory of personal information (both that of employees and customers);
- enhance the ability to detect and investigate data breaches; and,
- implement a technology-assisted program to automate DSAR/SRR requests.

Executable rights are among the most challenging aspects of the new data privacy laws, and have an impact on the appropriate technology-assisted workflows organizations take in response to 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 themselves or a third-party in an accessible format. Adding to the complexity, each executable right has different exemptions that need to be understood so that organizations can deflect some requests to better focus on the volume of legitimate requests that require personal data to be collected, reviewed, analyzed and produced.

eDiscovery 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, redaction and production tools in eDiscovery platforms, such as OpenText™ Axcelerate™ and OpenText™ Insight™, 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.

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

## The new world of data privacy

Since the advent of electronic data, organizations have been collecting digital personal information from their customers and treating that data 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. As just one example, the numerous Yahoo! data breaches from 2012 to 2016, including the 2013 breach of the data from all three billion users, brought the issues home for many organizations and consumers alike.

Regulators are executing on demands for a fundamental shift in data privacy. The core objective of data privacy regulation is to shift 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 rights conferred to employees and customers.

Sitting on the sidelines is not an option. The EU, 13 U.S. states and over 10 other countries have enacted data privacy rules. In the EU alone, over $470 million in fines have been levied under the GDPR between May 2018 and December 31, 2019 alone,[2] and over 160,000 data breaches have been reported in the EU alone since the GDPR took effect.[3]

## Policies and programs: data privacy action areas

There are numerous concurrent and interrelated actions that organizations must take to achieve data privacy compliance. These include a holistic approach to data privacy policy and personal information management. For organizations subject to data privacy laws, some of the steps to compliance include:

- Establishing a cross-functional data privacy compliance team;
- Learning about opt-out and consent requirements and updating the organization's privacy policies, notices, and data collections mechanisms accordingly;
- Creating an inventory of personal information held by the organization including the purposes it is held for, the details of how it is processed, and any third parties that it is shared with;
- Updating the organization's data retention policies;
- Enhancing the organization's ability to detect, investigate and report on data breaches;
- Installing methods for tracking and reporting on all data privacy activities and interactions; and,
- Developing dedicated programs to comply with Subject Rights Requests.

The last action area, Subject Rights Requests, is particularly challenging to comply with because it requires a detailed knowledge of the various rights, the associated exemptions, and the implementation of a new technology-assisted workflow that can automate potentially costly, time-consuming and error prone processes.

Before diving into how eDiscovery technology can be applied to efficiently fulfill data subject requests, we'll discuss essential rights because this is where many of the details of Subject Rights Requests are defined and affect technology-assisted workflows in fulfilling (or rejecting) the requests.

[2] Alpin – GDPR fines list

[3] DLA Piper study

opentext™

## 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 that are further entrenched as specific executable rights that customers can exercise as they please. Data privacy regulations seek to balance individual rights against the organization's legitimate interests and legal requirements through specific exemptions to executable rights.

### Natural rights

The primary overarching natural right conferred by data privacy legislation is the duty placed on organizations to inform customers about how the business collects, manages and processes personal information. Being informed allows customers to make educated choices about whether to sanction the organization to use their personal data as described, or to exercise one of their executable rights to limit or prohibit the organization from doing so. GDPR and CCPA share the same fundamentals that at the time of collection the following must be disclosed: (1) the categories of personal data collected; and, (2) the business purposes for which the data is collected and used.

GDPR imposes numerous additional requirements, including the need to identify:

- The legal name of the data controller;
- Contact information of the Data Protection Officer for the data controller;
- Whether the data will be transferred or sold to third parties;
- The retention period for the data;
- The consequences of not providing the data if it is included within a contract;
- Any automated decision making involved including the details on how automated decisions are processed; and,
- An explicit statement of the right to complain and the name of the Data Protection Authority to whom to send complaints.

CCPA requirements are more truncated but add:

- A redirect to a "do not sell my personal information" page if the data is intended for sale;
- A list of all categories of data collected or sold by the business in the previous 12 months; and,
- A broad set of provisions that protect the customer from discrimination or retribution for exercising any of their executable rights.

### 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;
- the right to have their data delivered to themselves (GDPR and CCPA) or others (GDPR);
- and the right to have their data deleted.

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

GDPR and CCPA 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 Subject Rights Requests but protects them from unintended use of the laws.

## Developing a defensible and cost-effective subject rights request workflow

Two concurrent facets of DSAR/SRR workflows need to be considered. These are: (1) the policy-related aspects including rejecting requests that meet an exemption, and (2) the core programmatic aspects of completing the majority of requests that require fulfillment.

While this white paper focuses on the programmatic aspects and the application of eDiscovery technology to the core of DSAR/SRR workflows to collect, cull, review, de-risk, and produce reports in response to legitimate requests, understanding what the exemptions are and applying them is an important component of a holistic DSAR/SRR workflow.

### Deciding when exemptions apply

Some exemptions can be determined without knowing the specific details of the data involved. These typically involve requests that conflict with the organization's legitimate need to continue to process the data. 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. There are also several exemptions where the relevant data needs to be collected and reviewed to determine if the exemption applies, such as compliance with legal obligations that supersede the individual's request to delete their information.

### Investigations disguised as DSAR/SRR requests

To manage risk, organizations need to understand the motivation behind the request. Sometimes the type of request suggests that it is better suited to an investigation framework and likely exempt for legal risk reasons. A common example is when customers or employees request to know the details about them in email and other communications related to a perceived service failure, or employment issues. In both cases, the request suggests legal exposure for the organization and may be exempt. In some circumstances, these requests would be addressed as part of a broader-scoped investigation.

### Requests submitted by agents

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.

opentext™

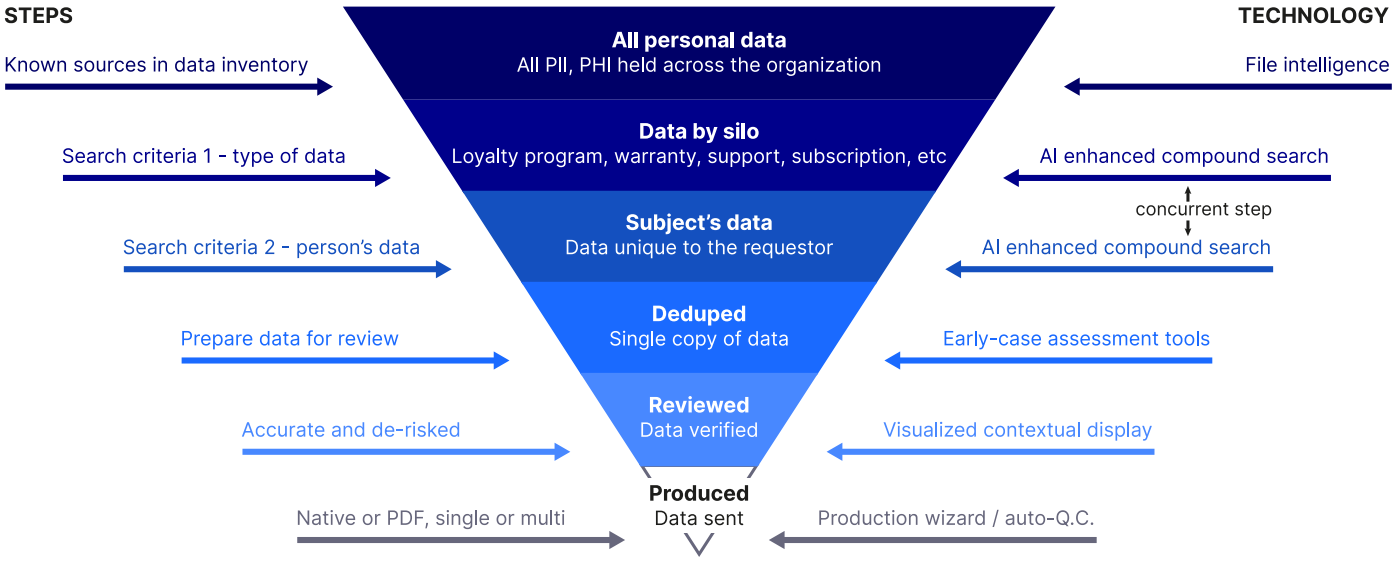
### DSAR/SRR Workflow Framework

Data subject access requests follow identical workflows to that of a litigation response requiring eDiscovery. 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 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 conducting reviews becomes even tighter. Turn-key connectors such as those in OpenText Axcelerate and OpenText Insight 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 eDiscovery technology can surface relevant data from large document sets quickly and efficiently.

**DSAR / SRR Funnel—Homing In Quickly to Contain Costs**

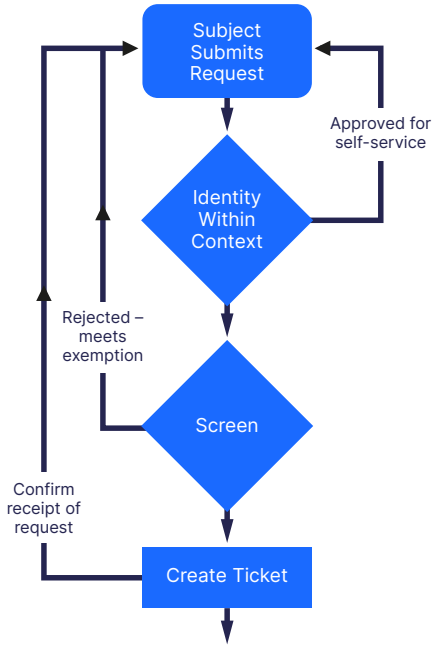


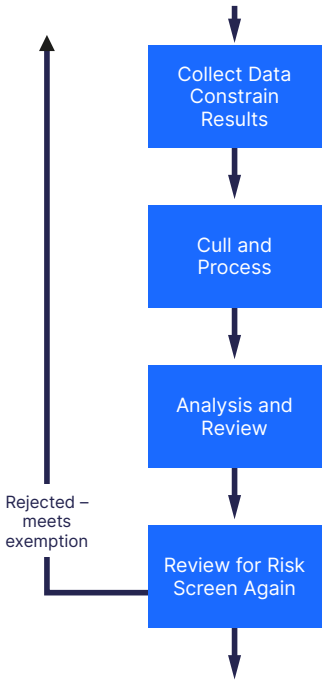

Efficient use of eDiscovery technology to winnow down large document collections to the relevant personal data

opentext™

Below is an example of specific eDiscovery technology tools that can help organizations efficiently meet data privacy requests. eDiscovery 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.

| eDiscovery 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 Axcelerate 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 that relevant to the requestor and topic area. |
| **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, which learn from human review decisions to predict the search terms and parameters that are most likely to uncover relevant data. | 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" every document for efficiency and improving accuracy. | Prioritize the most relevant documents containing personal information for review. |
| **Entity Identification** | Integrated detection tools that automatically surface the names of people and places. | Quickly and easily 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, we take a look at each stage of the DSAR/SRR process and how eDiscovery tools are essential to efficiently fulfilling the requests.

### Gather, Screen and Stage Requests for Action

**Subject submits request:** Forms (web-based or filled-in by staff) identify the type of request and collect sufficient detail to provide enough context to respond correctly via the most efficient workflow.

**Identity within context:** GDPR and CCPA state that requestor identity must be verified in proportion to the sensitivity of the data that he/she is requesting so context must be known from the outset. The type of request also determines whether it can be selfserved or requires further processing. Right to know and right to amend requests from customers and employees will sometimes mask the desire for self-access. The test of whether self-service is appropriate is if the data is private to the individual but not otherwise restricted.

**Screen:** Assess the request against the exemptions specific to each regulation. Deflect some requests before they are even submitted by: stating the exemptions around legitimate ongoing interests; stating that transfer requests only involve data submitted by the individual; and advising that right to transfer requests may create risk for the requestor if sensitive data is involved.

**Create ticket:** For requests that require action, inform the requestor of the status at this time and within the 10-day (CCPA) or 30-day (GDPR) window to provide a receipt of request. If third-party processors are involved, provide a copy of the ticket for them to take action on in parallel.

### 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 eDiscovery 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 eDiscovery 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.

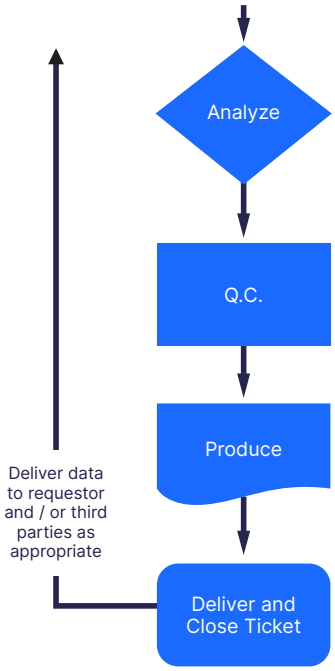
*Relevant eDiscovery tools:* Predictive coding/ technology-assisted review.

**Screen again:** Assess for the exemptions where the data was required to make a determination, including: the age of the data (CCPA); legal obligations (GDPR and CCPA); and if the data is required for an investigation (CCPA).

*Relevant eDiscovery tools:* Not applicable

**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 eDiscovery 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 eDiscovery 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 eDiscovery 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 eDiscovery 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, eDiscovery 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 – employees and customers 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 response can be applied to DSAR/SRR, allowing efficient compliance.

OpenText provides comprehensive, automated and flexible technology that enables organizations to respond to DSAR/SRRs rapidly, leveraging its eDiscovery review and investigations platforms (Axcelerate and Insight) to streamline the time involved in responding to requests and the overall resource overhead associated with compliance.

OpenText eDiscovery technology 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, thus 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 collection services, managed document review services leveraging Axcelerate or Insight review technology in secure OpenText locations, and DSAR/SRR processing consulting expertise.

opentext™

## Appendix

### 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:**<br>• The types of data covered in right to know requests mirrors the breadth of data needed to fulfill the right to be informed, listed above.<br>• 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.<br>• As discussed above, GDPR and CCPA provide different levels of granularity in regard to the amount of detail that needs to be provided. | **Right to know exemptions:**<br>• 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.<br>• 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.<br>• CCPA further restricts right to know requests to data collected within the past twelve months and limits the frequency of requests to twice per year per individual. |
| **Right to opt out:**<br>• GDPR is much broader than CCPA in terms of the right to opt out.<br>• Under GDPR, individuals can opt-out of allowing their data to be used by an organization by withdrawing their consent at any time.<br>• 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.<br>• Organizations must make the effort of opting out as easy as the consent to opt in.<br>• The CCPA includes the right to opt out but only in regard to 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.<br>• 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:**<br>• 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.<br>• 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.<br>• Under CCPA, the right to prohibit the sale of personal information is absolute – there are no exemptions. |

opentext™

| Executable rights | Exemptions |
|---|---|
| **Right to have data transferred:**<br>• 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.<br>• CCPA only goes so far as obliging organizations to provide the data to the requestor.<br>• GDPR places a further onus on organizations to send the data directly to third parties dictated by the customer. | **Right to data transfer exemptions:**<br>• For both GDPR and CCPA, the right to data transfers only applies to data collected directly from the data subject.<br>• This is further restricted under CCPA as the data provided by the customer within the past twelve months.<br>• 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.<br>• 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:**<br>• The CCPA and GDPR are consistent in providing the right to individuals to request that their personal information be deleted.<br>• 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.<br>• Because of the irrevocable nature of deletion, this right comes with an extensive set of exemptions. | **Right to deletion exemptions:**<br>• Under the CCPA and GDPR, deletion requests can be denied if the data is:<br>  • reasonably aligned to the customer's ongoing relationship with the organization;<br>  • required to fulfill a legal obligation and / or is subject to legal hold; or,<br>  • necessary for ongoing research that supports the interests of public health.<br>• CCPA adds several other reasons to deny deletion requests if the data is:<br>  • material to an open or anticipated investigation into illegal activity;<br>  • required as part of a security investigation into malicious, deceptive, or fraudulent activity; or,<br>  • part of a contract between the business and customer.<br>• GDPR adds that deletion requests can be denied if deleting the data would compromise freedom of expression and free speech. |

opentext™

| 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.** | **Purpose: Protecting against legal risks and limiting the number of requests that need a report to be produced.** |
| • Right to know requests that are repetitive, spurious, or excessive in scope;<br>• Right to opt-out requests that are aligned to the legitimate and ongoing interests of the organization;<br>• Right to transfer requests that includes data beyond what was submitted by the customer; and,<br>• Right to delete requests where the data is material to an ongoing relationship, included in a contract, or part of public health research. | • 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);<br>• Right to delete requests that may involve:<br>  • a legal obligation or content subject to legal hold; (GDPR and CCPA)<br>  • data material to an investigation into security risks or criminal actions (CCPA). |


OpenText eDiscovery

OpenText Axcelerate

OpenText Insight


## About OpenText

OpenText, The Information Company, enables organizations to gain insight through market leading information management solutions, on-premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit: opentext.com.

## Connect with us:

- OpenText CEO Mark Barrenechea's blog
- Twitter | LinkedIn

**opentext.com/contact**