Celebrating Data Privacy Week 2023 - Data Subject Access Requests

Legal Alert
January 26, 2023

Related Services

Privacy, Cybersecurity & Data Protection

State and international laws provide consumers and employees (including job applicants and former employees) with certain rights, such as the right to find out what personal information a business has about the individual, the right to correct inaccurate personal information, the right to delete personal information, the right to opt-out of certain uses of personal information, and the right to "port" or transfer personal information.

A business will need to decide if it wants to provide responses to all individuals who make a data subject access request ("DSAR") regarding these rights or only when required by law. If the business decides to only respond when required by law, it will need to determine which laws apply to it and if any exceptions apply (such as, under certain laws, if a business is a non-profit organization). Legal counsel can help your business determine which laws apply and which rights are given to individuals under those laws. This guide is intended to provide general information about how to handle a DSAR.

Establish a Process

First, a business should establish a process to handle incoming DSARs. For example, if a customer-facing employee receives a request for information from a consumer while on a phone call with that customer, how should the employee respond? It helps to have a dedicated employee or email address as the point of contact for managing, tracking, and responding to DSARs.

Verify the Request

Before providing personal information in response to a DSAR, verify that the person making the request is the individual to whom the personal information relates or is someone authorized to act on behalf of the individual. Providing personal information to an unauthorized individual is a data breach that requires

notice to the individual to whom the personal information relates.

The verification process should not be unduly burdensome for the requestor and any information collected in order to verify an individual should not be saved or used for any other purpose. As much as possible, a business should use information already in its possession to verify an individual's identity. For example, a business that has a log-in feature can require that an individual make a DSAR when logged in to the individual's account.

Timing

Timing varies based on the applicable law. For example, under the GDPR, businesses have one month to respond to a DSAR. If a business receives a complex request or has a high volume of requests, it can take a two-month extension to respond, provided it gives notice to the individual within one month of receiving the DSAR. Under California and Virginia law, businesses have 45 days to respond to a DSAR. If a business receives a complex request or has a high volume of requests, it can take a 45-day extension to respond, provided it gives notice to the individual within 45 days of receiving the DSAR. When Colorado's and Connecticut's laws go into effect on July 1, 2023 and when Utah's law goes into effect on December 31, 2023, they will follow the 45/45-day timing.

Fees

Generally, a business may not charge a requestor any amount to recoup the cost of responding to a DSAR. If requests are unfounded, excessive, or repetitive, there may be exceptions. How often an individual can make a DSAR is set out by law. Generally, submitting a DSAR twice per year is not considered excessive.

Respond to the Request

Data minimization is a key component to being able to respond to DSARs. While California law requires a business to only produce information from the prior 12 months, other laws do not have any time limitation. A business that limits its collection of personal information and follows strict data retention policies to properly dispose of personal information will have limited information to disclose; transfer; or opt-out of the sale, sharing, or other processing when it receives a DSAR.

Prior to providing or deleting information in response to a DSAR, a business should consider its responsibilities and legal obligations under other laws. For example, a business may need to retain tax records and cannot delete them, even upon an employee's deletion request. Additionally, a business is not required to provide personal information of any other individual; responses that might include such information should be redacted or withheld. For sensitive personal information (such as Social Security number, financial account information, account password and security questions), a business should seriously consider whether to provide this information to a requestor. Providing such information may be prohibited by law and it may be

sufficient to only provide categories of information, rather than the specific numerical values.

A business' response to a DSAR should be in an easily readable format.

Denying a Request

An appropriate response to a request may be to deny it, rather than to provide or delete information. If a business denies a request, it must inform the requestor of that decision and explain why the decision was made (e.g., we were unable to verify your identity and therefore are denying your request to obtain the specific pieces of personal information we hold regarding an individual named John Smith). The business also needs to provide information about how to file a complaint about or appeal the denial, depending on the applicable law.

Audit Log

Best practices include keeping a log of the request date, the response date, and who completed the response. It can also be helpful to keep a record of the applicable law, in the event a business needs to respond to a regulatory authority investigation.

Why Comply?

Although it may be costly and time-consuming to respond to DSARs, it may be more costly to ignore them. A violation of GDPR can cost up to 20mil Euros or 4% of a company's worldwide annual revenue from the prior year, whichever is higher. A violation of California law can cost $2,500 per violation or $7,500 for each intentional violation. A violation of Virginia law can cost $7,500 per violation. Beginning July 1, 2023, a violation of Colorado law can cost up to $20,000 per violation and a violation of Connecticut law can cost up to $25,000 per violation. Beginning December 31, 2023, a violation of Utah law can cost up to $7,500 per violation.