

DSAR TERMS EVERY BUSINESS NEEDS TO KNOW

To help businesses navigate the DSAR and compliance landscape, we've assembled a list of key terms and their definitions.

Data subject

This is how people in privacy often refer to a person. A "data subject" is the person to whom the personal data you've collected belongs.

DSAR or DSRR

Standing for "Data Subject Access Request" and "Data Subject Rights Request," respectively, these are the two most common terms used to refer to the act of a person exercising their privacy rights with an organization. If you "receive a DSAR," that means a person has requested access to the data you hold about them and (potentially) asked that you do something with that data, such as delete it, correct it, or not use it in some way.

Controller

This is the organization that makes decisions about how to handle personal data. Say, for example, a company used a surveying service to collect information about people. Even though the company doesn't actually possess the data — it's still on the surveying company's servers — the company that sent out the survey and asked people for their information is the "controller" of the data.

Processor

This organization handles data on behalf of another organization. In the example above of the company conducting a survey, the service that collects the data on the company's behalf is the data "processor."

Third party

You and the data subject are the first two parties; a third party might be a vendor, purchaser of data, or anyone else who accesses the data subject's data after they have provided it to you or you have collected it.

Automated decision-making

This is the process of using personal data to affect the experience a person has interacting with your organization. Generally, these are computer algorithms that take in demographic and other data and spit out specific user experiences. It might be as simple as, "last time you visited our website, you bought a couch, so we're going to show you ottomans you might like."

Profiling

If you automatically process a data subject's personal information to evaluate or predict their behavior, then you engage in profiling. Closely associated with automated decision-making, profiling is used to analyze or predict data subject behavior across a range of domains, like their work performance, personal preferences, location or movements, and the like. Under most data privacy regulations, consumers can make a DSAR/DSRR to opt out of profiling.

Personal information

Could a piece of data be reasonably linked to a particular consumer or their household? If so, most data privacy regulations would say that's personal information. This could include addresses, names, driver's license numbers, and the like.

Sensitive personal information

Not all personal data is created equal. Some data, such as "phone book data," like phone numbers and addresses, has fewer regulations. Sensitive data, however, is data like health data, sexual orientation data, or genetic data that could lead to serious harm to a person if it falls into the wrong hands. Some jurisdictions even define data like union membership or political party affiliation as sensitive. Generally speaking, this data must be handled more carefully, requires special permissions to collect, and triggers higher penalties if mishandled.

Portability

Many of the rights data subjects have are no-brainers, like the right to access, correction, or deletion. But data privacy regulations also feature a right to "portability." Essentially, this means that you can't give a data subject their data in an excessively complicated format. If you receive a DSAR/DSRR where the data subject requests access to their data, then you have to provide it in a structured, commonly used and machine-readable format that can be easily transmitted. This could be, for example, PDFs or an Excel spreadsheet, rather than an obscure file format that requires special software to access.




MAKE DSAR COMPLIANCE EASY

Securely managing DSARs, finding personal information across multiple data sources, and doing it all within a mandated timeline — these aren't easy tasks. That's why organizations interested in becoming compliant quickly and minimizing the interruption that DSARs can have on the flow of business use Osano.

Osano makes it easy to verify a data subject's identity, assign inbound requests to the correct person, and deliver results to the data subject in the timeframe required by law. Our AI-driven data discovery capabilities automatically finds, classifies, and evaluates all your data across every one of your systems, streamlining the process of acting on a consumers' DSAR.

[Schedule a demo](#)



 @osano
 [linkedin.com/company/osano](https://www.linkedin.com/company/osano)
 [http://facebook.com/osanoatx](https://www.facebook.com/osanoatx)
osano.com

About Osano

Osano is a complete data privacy platform trusted by thousands of organizations around the world. Its platform simplifies compliance for complex data privacy laws such as GDPR, CCPS, LGPD, and more. Features include consent management, subject rights management, data discovery, and vendor risk monitoring. Osano is the most popular cookie compliance solution in the world, used on over 900,000 websites to capture consent for more than 2.5 billion monthly visitors.