DSARs & Beyond:

Managing Data Privacy Rights and Responsibilities

TABLE OF CONTENTS

DSARs and Beyond: Managing Data Privacy Rights and Responsibilities

Everyone knows by now that vast amounts of data are being created every day. It is the lifeblood of the information economy. Managing this firehose of data well is what often separates leading organizations from also-rans. How you use it to improve operations, satisfy customers, increase revenues, or find efficiencies often dictates your success in the marketplace.

However, some people may be less aware that the use of data comes with responsibilities, often called Data Privacy Rights. If a person has created data, or that data can be used to identify a person, the use of that so-called personal data (or, sometimes, "personally identifiable information," or PII) is regulated by a variety of international laws that dictate how and when you can use it.

If this is news to you, and you work with a lot of personal-seeming data, you should really get up to speed on data privacy laws and how to comply with them ASAP! Otherwise, you could soon be in for a bad time.

If you're reading this, though, you probably already know that many countries have passed laws saying that you need to get and document consent from people before you collect and/or do various things with their data. If you lead or work at a company of any size, you probably have a cookie banner on your website and a privacy policy people can read. For many organizations, those are the first steps in data privacy compliance.

These laws also grant people various rights to their personal data, however, such as:

- The right to see what data you've collected about them.
- The right to correct it if it's wrong or ask you to delete it entirely.
- The right to keep it from being shared or sold.
- The right to object to automated decision-making based on their data.

Figuring out how to comply with these legal obligations is often the next step. While you might think it's a fantastic service you've provided to people that matches product offerings to their past purchases, it's illegal in some parts of the world to offer such a thing to a person who has asked you not to. How do you accept and process that kind of request? Whose job is it to fulfill that request? How do you make it so one person gets one experience from your organization, and another gets a different one?

But even more basically: How do you know the person asking for their information is actually who they say they are? How do you even find all the information your organization has about that person? This might all sound confusing and hard to manage — and it can be! — but well-trained professionals using smart processes and software tools designed for the purpose are figuring it out around the globe. If they can do it, so can you.

There are plenty of incentives for figuring it out, too. Not only will your organization be protected against regulators of privacy laws, who can levy fines and halt your ability to gather any data at all, but you'll also be avoiding nasty hits to your organization's reputation.

Increasingly, consumers are looking for organizations they can trust when operating in the virtual marketplace. It can be scary in cyberspace (if you're old enough to call it that), and organizations that make it clear they are good digital stewards are rewarded with loyal customers.

Organizations are looking for vendors who share their care and attention to personal data and won't work with those who can't live up to their data privacy standards. You don't want to lose out on business because you've failed to stay up to speed or look like you just don't care about privacy at all.

This handy e-book will focus on helping you understand when your organization has to comply with data privacy rights requests, what those various requests might consist of in various jurisdictions, and how to get started on the path to compliance.

What's a DSAR? And Other Terminology Questions

As with any industry, the industry of people who work with data privacy issues has its own lexicon, with a slate of essential terms and more acronyms than you can shake a stick at. It's important to understand a few of them before grappling with data privacy rights.

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.

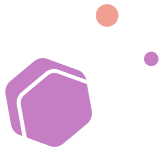
Controller: This organization makes decisions about how to handle personal data. Say, for example, a company used a surveying service to collect information about people. Even though the company doesn't actually possess the data — it's still on the surveying company's servers — the company that sent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

Sensitive Data or 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.



Which Privacy Laws Matter? And Other Legal Questions

Every organization will have a different business plan, collect different sorts of data, have customers in different states and countries, and have a different tolerance for risk. Privacy is a hot topic, however, because some states in the U.S. and countries around the world have passed privacy legislation that tightly regulates the use of personal data and levies significant penalties for violating that law. In general, these three laws are considered the most significant and contain the largest penalties for violations.

GDPR: The European Union's General Data Protection Regulation is generally regarded as the world's most significant privacy law, dictating how you can handle the data of anyone residing within the European Union. It grants many data privacy rights to people living in the European Union. Further, many other countries in the European Economic Area — such as Switzerland and the United Kingdom — have passed mirroring legislation that confers the same rights.

Even if your company has no physical presence in these countries, you are subject to their laws if you market to the people living there. Violations of the law can trigger fines of as much as 4% of annual revenue or 20 million euros, whichever is higher.

You generally have 30 days to comply with a privacy rights request.

CPRA: The California Privacy Rights Act is an update to the California Consumer Privacy Act and comes fully into force in July of 2023. It confers several privacy rights to people residing in California if the companies that hold their data meet certain thresholds.

You should consult a lawyer if you have questions, but your company must comply with the CPRA if it is a for-profit that does business in California and:

- Buys, sells, or shares the personal information of 100,000 Californian people or households.
- Creates 50% or more of its revenues through the sale or sharing of personal information.
- Had $25 million in gross revenue in the preceding calendar year (so January 1, 2022, to December 31, 2023, to start).

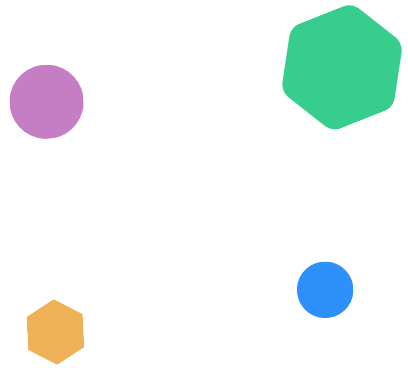
Violations can trigger fines of up to $7500 per offense, depending on whether the California Privacy Protection Authority (CPPA) or the state's Attorney General determines your violation is purposeful. And if a whole database is affected, for example, each person affected counts as an "offense." That adds up quick.

In general, you have 45 days to comply with a privacy rights request.

LGPD: Literally standing for "Lei Geral de Proteção de Dados Pessoais" in Portuguese. The LGPD is commonly known as Brazil's General Personal Data Protection Law and is primarily the same as the EU's GDPR, granting similar privacy rights. As with the GDPR, you are subject to Brazil's privacy law if the people whose data you are collecting reside in Brazil and you do business there on purpose.

Like the GDPR, fines can be as high as 2% of annual revenue or 50 million reais, whichever is higher.

The LGPD provides the shortest time of the significant laws for complying with a data subject access request: 15 days.



What Privacy Rights Do People Have, Anyway?

Contemporary privacy laws have begun to coalesce around a set of data privacy rights that are mostly the same (with a few exceptions) from California to the EU to Brazil and are being proposed or are in place in other jurisdictions but with fewer penalties or less regulatory authority and oversight.

Let's take a look at them and understand what responsibilities they confer on organizations that collect and handle personal data.

Right to Know/Access (CPRA, GDPR, LGPD): Data subjects have a right to know that you have their data and see every piece of personal data you have about them. Yes, data subjects can include your employees, depending on the law in question.

Right to Deletion (CPRA, GDPR, LGPD): Data subjects have the right to ask you to delete any and all of the data you have about them. California is somewhat unique here in that it also requires companies to inform everyone they have shared data with of that deletion request and tell them to delete it, too. In Europe, this is often called the "right to be forgotten." Note that everyone has exceptions for fulfilling contracts, protecting human life, and performing certain research. California has an exception for exercising free speech, generally in a journalistic manner.

Right to Correction (CPRA, GDPR, LGPD): Data subjects have the right to correct or complete any data files you have about them.

Right to Data Portability (GDPR, LGPD): Data subjects have the right to ask you to provide all of the data you have about them to another organization of their choosing.

Right To Know with Whom You've Shared Their Data (CPRA, GDPR, LGPD): This one's pretty self-explanatory. Data subjects have a right to know with whom you've shared their data and which data you've shared. This is mainly limited to the business categories with which you've shared the data in California. In the EU and Brazil, you have to be specific.

Right To Opt-Out of Sharing and Selling Personal Data (CPRA): While similar to revocation of consent, this right is specific to California and dictates that people must be able to opt-out of your ability to sell their data to, or share their data with, a third party. And they must be able to do it via a button on your website.

Right To Withdraw Consent (CPRA, GDPR, LGPD): Even if they consented to you to collect and process the data in the past, data subjects have the right to withdraw that consent at any time. In the EU, they even clarified that it has to be as easy to withdraw the consent as it was to give it.

Right To Object (GDPR): The GDPR makes broad allowances for data subjects to make sure you're processing their data lawfully. If they object, you have to stop using their data until you can establish a legal right to do so. If they object to your use of their personal data for direct marketing, you have to do so immediately; if it's for research purposes, you have to demonstrate the use of the personal data is in the public interest.

Right to Restriction of Processing (GDPR, CPRA): The data subject may object to your use of their data if they believe it is incorrect (giving you time to correct the data before using it again); if they believe you have it unlawfully, but don't want you to delete it; and if they don't want you to use it, but they want it available because of a pending legal matter. In this case, you have to save the data somewhere, but make sure not to use it. In the case of California, people may request that you not share or process their sensitive personal information. This means you must be able to discern their "normal" personal information from their sensitive data.

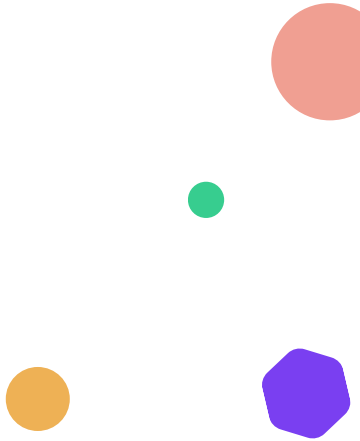
Right to Not Be the Subject of Automated Decision-Making (GDPR): Companies must acquire explicit consent to use automated decision-making.

Right to No Retaliation (GDPR, CPRA, LGPD): All three major laws say that you can't penalize customers for exercising their data privacy rights. This means you can't charge them extra or otherwise restrict their access to service just because they have chosen to exercise their privacy rights.

Right To Be Told Their Right Not To Consent (LGPD): While the CPRA and GDPR require you to get consent for everything you're going to do with a person's data and say you can't penalize people for not providing it, the LGPD explicitly says you have to explain a person's right not to give consent to process their data, while still receiving their desired service, at the time of request for consent.

Finally, don't take this as a complete list of everything these laws require. For example, all three laws have a long list of pieces of information you must provide at the time of collection of personal data. Most people don't consider that a matter of "data privacy rights" per se, but they are things you need to do to comply with these privacy laws. There may also be carve-outs for defense and public health reasons whereby the rights don't apply.

When in doubt, talk to a privacy professional before doing something with personal data when unsure of the legalities.



How Do We Actually Comply With These Data Privacy Rights?

One of the core principles of the CPRA and a general expectation of privacy regulators around the world is that it be easy for people to exercise their privacy rights and that they not be penalized for doing so.

So, in short, you can't charge people money for the "service" of complying with their requests regarding their privacy rights. And you can't bury the ways for them to exercise their rights on some backwater page of your website (or just give them a phone number with a voice mailbox that no one ever checks).

That means you need to operationalize your privacy program. Most companies do this with a mix of human resources and software automation tools. Due to the complex nature of data privacy — where the type of data, the jurisdiction where the person resides, and the use of the data can all vary wildly — it is virtually impossible to create a fully automated fulfillment process. Still, most organizations have found they can automate large portions of the process and use the software in other ways to streamline their operations.

Here's how to get started:

1 - Attach metadata to all of the data you store at your organization.

Without some kind of tagging system, you're flying blind. It's vital that all of your organization's data be marked as personal or not and that all of your personal data be further tagged for the type of personal data it is and whether it's sensitive or not (and that definition might be different depending on where the person you collected it from is residing, so you better tag by geography as well).

And, of course, make sure all data is tagged back to the person to which it belongs.

This can be done relatively easily in most modern database systems, but you'll find there are all sorts of hairy examples of situations where it's not so easy. How do you tag information stored in paper, video, or audio files? One paper intake form might have numerous types of data, some of it very personal.

Your team will have to develop a process for storing and managing nontraditional data formats. You'll also likely want a data mapping or PII-identification tool to identify personal data in your systems that you may have misplaced, never known about, or only existed in legacy systems.

It's also possible, sometimes, to anonymize data if you don't need it to be related to the person who provided it to you. This can open all sorts of possibilities for the use of the data, but be careful: It can be easier than you think to re-identify data, and regulators are aware of these capabilities.

2 - Make sure someone is in charge of fulfilling privacy rights at your organization.

While the GDPR and LGPD require a data protection officer, and California doesn't, it's best to have someone heading up privacy efforts. That person should report to the highest levels of the organization and have both budget and authority to make certain data privacy rights are being managed and fulfilled.

Most organizations then have a team under that person, many of whom they embed within various other departments — HR, marketing, sales, IT, product development, etc.

Unless someone owns this process, it's doubtful it will go well.

3 - Have a way to authenticate someone's identity.

How will you ensure that the person making a request is the person to whom the data belongs? Organizations have a variety of methods they use — from sending an email to an address on file to requesting national identification cards — but your privacy rights compliance must have something in place, or you could find yourself in a bad situation.

Deleting or changing a person's information at a scammer's request or because you thought this Jane Smith was a different Jane Smith can result in a severe privacy law violation. You could also enable serious harm should you provide personal information to a domestic abuser or someone else who means a person harm.

4 - Automate the "easy" pieces so you can put person-hours toward the hard parts.

Assuming you have some kind of data governance in place, you should centrally store personal information. Then, provide modern software tools access to that database or databases to quickly produce a Data Subject Access Report — the single file that provides a person with all the data you have about them.

The tool might look like a form on your website, with an email address, phone number, and physical address for folks who want to make a request in those formats. Sometimes the tool is fully automated for some "easy" requests; other times, the tool always has a human being in the middle to ensure the fulfillment is correct before the data subject sees anything. It often depends on the sensitivity and volume of the data in question.

That same tool should allow data subjects to make requests for deletion or correction easily. They're just updating a file! Of course, you likely don't want to give them the power to change your master database, as you may have legitimate legal reasons to keep certain data and contest changes. Still, these tools at least allow people to make requests that you can have a person adjudicate and approve (or not).

Similarly, that tool may allow people to quickly object to processing, object to automated decision-making, withdraw consent or ask for restrictions. Sometimes, those sorts of less-frequent requests all come in via a provided email address or phone number. Regardless, you need to have a process in place, and it needs to be easily findable by the data subjects who visit your organization's site.

5 - Track the requests that come in and analyze them.

Some large organizations (those that process the data of 10 million or more consumers) in California need to, by law, produce statistics about the requests they receive and how long it takes to fulfill them. While you may not be subject to that requirement, it's still a good idea.

You need to understand how long it's taking you to fulfill requests, how many requests you're receiving in a given time period, how many person-hours are going into fulfillment, and how often you're failing to live up to your responsibilities. That way, you can constantly adjust your process and understand your risk.

And, of course, documentation of requests and fulfillments will be necessary should a regulator come calling.

No organization will be perfect, but you're taking on significant risk if people are regularly not receiving satisfaction in the required time periods. Regulators will take notice, and the penalties can be severe for non-compliance.

Further, all three significant laws in question ramp up their penalties for grossly negligent or willfully negligent organizations. Neither ignorance nor incompetence is an excuse that regulators will tolerate. Nor will business partners be interested in working with organizations that can't fulfill privacy rights requests, as partner organizations often have to communicate with one another to make sure data is rectified or deleted by everyone to whom it's been shared or sold.

Want to learn more or get a copy of this in a handy checklist? Download your copy here:

→ **Access Your Copy**

Conclusion

Simply put, fulfilling data subject rights requests isn't easy. If your organization is like most, you'll have data in all sorts of places and with little metadata attached. Just getting to the point where you're confident you can even find all of the data about a particular person can take a long time — potentially years.

However, many organizations are in a similar situation, and most privacy regulators have frequently said that they look for effort and dedication to compliance, not perfection. If you've invested in people and tools and have a documented process for compliance, that will go a long way with regulators who are still in the early days of enforcement.

With the right people and tools in place, you can make sure your customers and employees have a good experience when asking for their data and create a trusted relationship that will go a long way toward a more successful organization as a whole.

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 website to capture consent for more than 2.5 billion monthly visitors.