WHITEPAPER

DATA PRIVACY FOR THE INFORMATION PROFESSIONAL

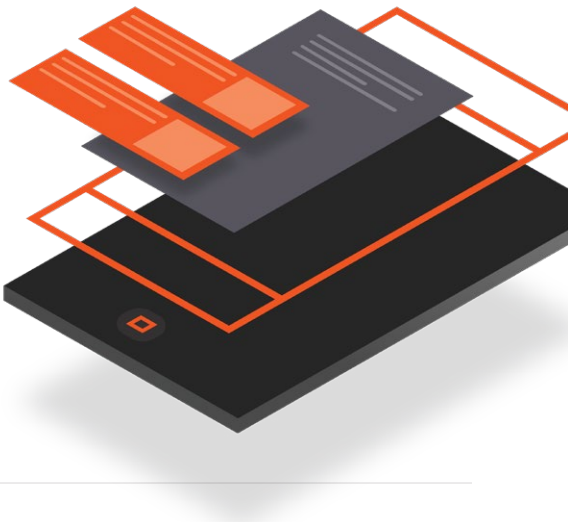
What you need to know about data privacy compliance

If you're in the information governance space these days, in virtually any capacity, you're hearing a lot about data privacy. And unless your organization is either far ahead of the curve—or so far behind that you don't even know it's a concern—there's probably a lot of discussion about what to do to bring your organization into privacy compliance.

Privacy is never a one-off

Bear in mind during your discussions that privacy compliance isn't a single act, something that you do or implement once and think no more about it. Privacy is more of a philosophical position that you must adopt, which will drive outcomes in a wide variety of processes, technologies and data repositories. Some are standard processes and documents, like records retention and retention schedules. But many others, like the need to provide disclosures, obtain permissions before collecting personal data and set retention periods, may be new to your organization, and may require you to develop unfamiliar processes and implement new or revised tools.

Contents



In tackling this daunting problem, it's important to understand that privacy compliance isn't by any means a uniform concept. The outcomes you'll need to achieve are driven by laws, and those legal requirements vary quite a bit. So, if you do business in Europe, you're faced with a much different privacy landscape than if you operate only in the United States.

But even in the U.S., the particular mix of states where you do business will have an assortment of privacy laws that vary by state. These days, it's tempting to assume that in the U.S., the California Consumer Privacy Act (CCPA) is the only game in town, but that would be a mistake. Many other states have privacy laws on the books, and many more are on the way. It's a complex and constantly shifting landscape.

Even the European Union, with its General Data Privacy Regulation (GDPR)—which was supposed to provide a level playing field in E.U. countries—is a complex hodgepodge of rules and regulations for organizations to navigate.

Data privacy principles

The core concept behind privacy as a legal and compliance matter is that virtually all information about a person is owned by that individual who, within some very broad limits, has a right to control how the information is used. There are profound consequences that flow from this concept.

Personally identifiable information, or PII, is any data that can be used to identify a specific person. Examples: full name, Social Security number, driver's license number, bank account number, passport number, phone number, mailing or e-mail address, IP address, social media posts, digital images.

There are several overarching principles to bear in mind that serve as a framework for virtually all privacy laws:

- *If it can be connected to a particular human being, it's personally identifiable information (PII).* Some privacy laws contain laundry lists of specific types of information that are regarded as personal, but many, including the CCPA and GDPR, are far broader and more general—and the landscape keeps shifting. It's not a good idea to assume that a specific bit of personal information is of no concern to you.
- *Less is more, and less is better.* If you don't need a bit of personal information, don't collect it in the first place. If you needed it and are done with it, get rid of it. This notion of data minimization—reducing the amount of PII in your possession—is a central tenet of all privacy laws. And by implication, it tells you that you need to have and enforce a *records retention schedule*, the process by which you dispose of old information.
- *When in doubt, disclose and ask.* You don't always need to disclose why you're collecting personal information, and you don't always need to ask for permission to do the collecting. But if permission is a requirement and you don't comply, you could be making a very expensive mistake. It never hurts to disclose and ask. If nothing else it's good PR, so unless you're absolutely sure you don't need to, ask.
- *No one should see it unless they need it.* Privacy is about keeping secrets, and it's no secret if anybody in your organization can see it. If they can access it now, that needs to stop.

Of course, actually implementing these simple principles is immensely complicated. Start by taking a look around your organization and asking how well these principles are being implemented right now. If you see any gaps, you've got some obvious starting points for your new privacy initiative.

For more on applying data privacy principles to retention, check out this webcast recording:
Privacy and Retention in the 21st Century – Not Your Grandpa's Retention Schedule

Tackling the data privacy challenge

Privacy isn't just a series of things you do; it's a philosophy that drives what you do to implement a privacy program. Embracing that philosophy up front is your starting point through the maze of compliance issues you have to face.

Privacy by design

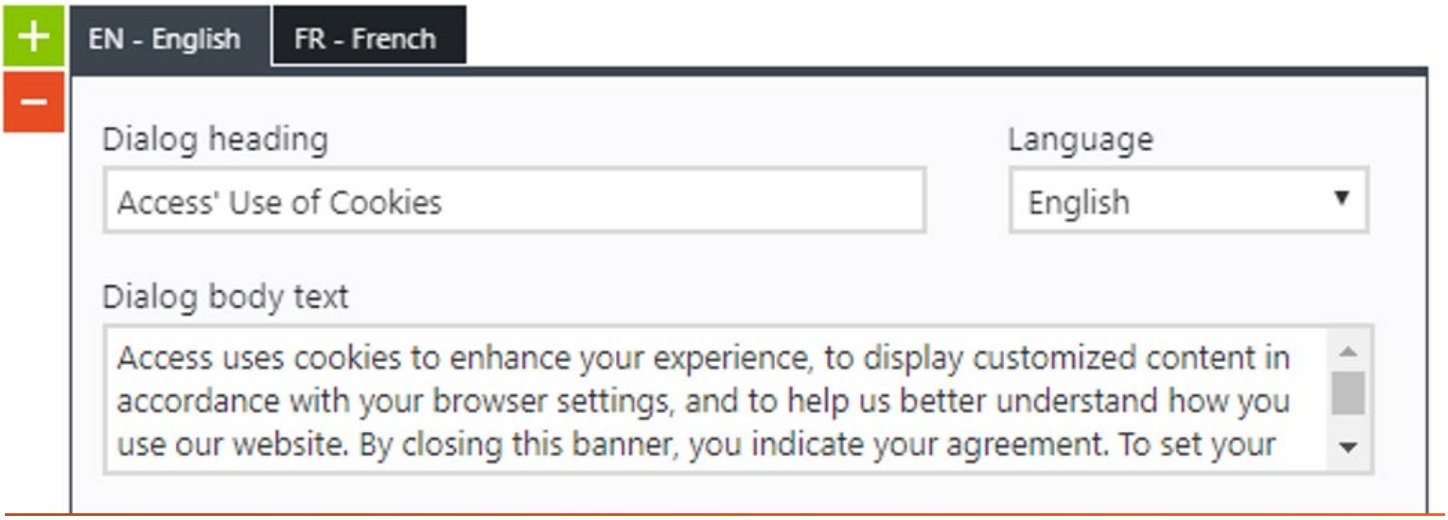
Let's start with the act of collecting PII. Because people own it, you can't just acquire it: you need to obtain permission first. Individuals have a right to know what you're going to do with their information before they allow you to collect it—and, in any case, are under no obligation to grant that permission.

In the past, your website may have collected information without explicitly informing people you were doing so. Customer reps on the phone might have been gathering data without telling people they were keying it into a computer system. No longer—people must be given reasonable notice of what you're doing, and *must be given the opportunity to refuse to provide information*. That may prevent you from completing a transaction. You can legitimately decline to do so in most cases, but you can't hide the ball.

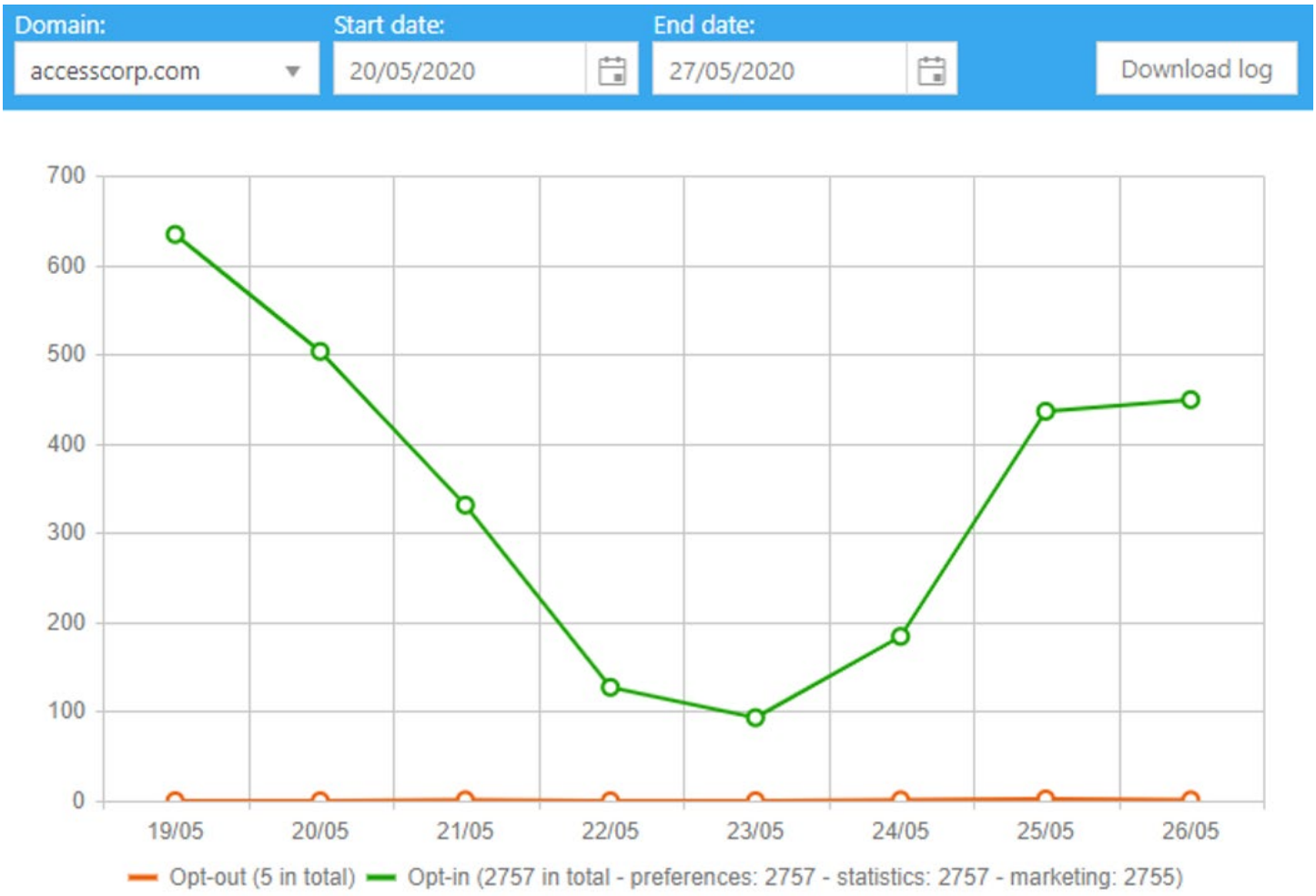
For instance, the EU recently clarified that an action like simply scrolling down a webpage cannot be considered consent to collect cookies, regardless of whatever disclaimers your cookie warning conveys. Affirmative, explicit consent to store or process personal information under GDPR requires a person to *take a specific action intended **only** to provide consent.*

And of course, since you have some liability in the case of noncompliance with privacy regulations, you have to keep track of all the permissions and the language of the disclosures to be able to prove that you did everything right. For multiple-language websites, make sure your declaration is available in every language.

Here's an example of a privacy notice on Access Corporation's website. It appears in French as well as English:

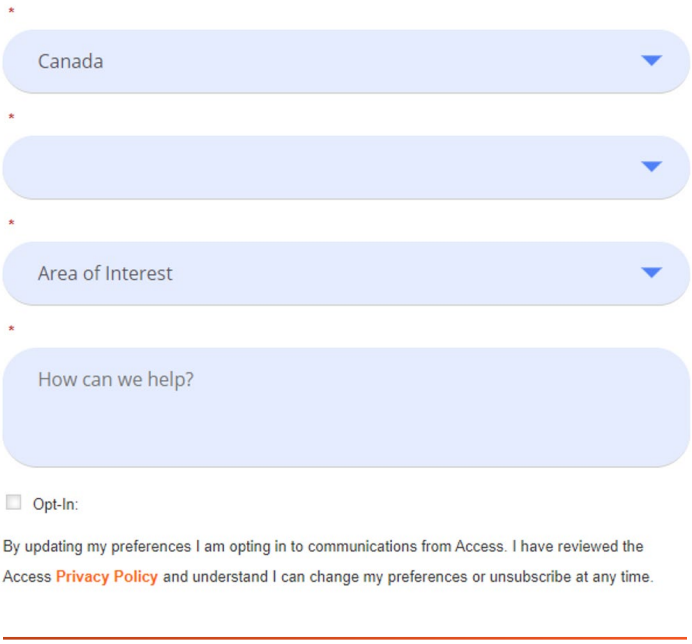


Again using the Access website as an example, here we see the capability to track consent and download logs to prove when consent occurred:



For many organizations, this is an entirely new set of rules that may require significant reengineering, from redesigning websites to updating intake forms to drafting and vetting legal disclosures.

Consent laws differ by geography, so make sure to know when explicit consent requires its own checkbox. Here's an example of a Canadian opt-in statement now required by law:



Having told people what you are planning to do with their information, you have to make sure you actually do it. That's another heavy lift.

Dealing with exceptions

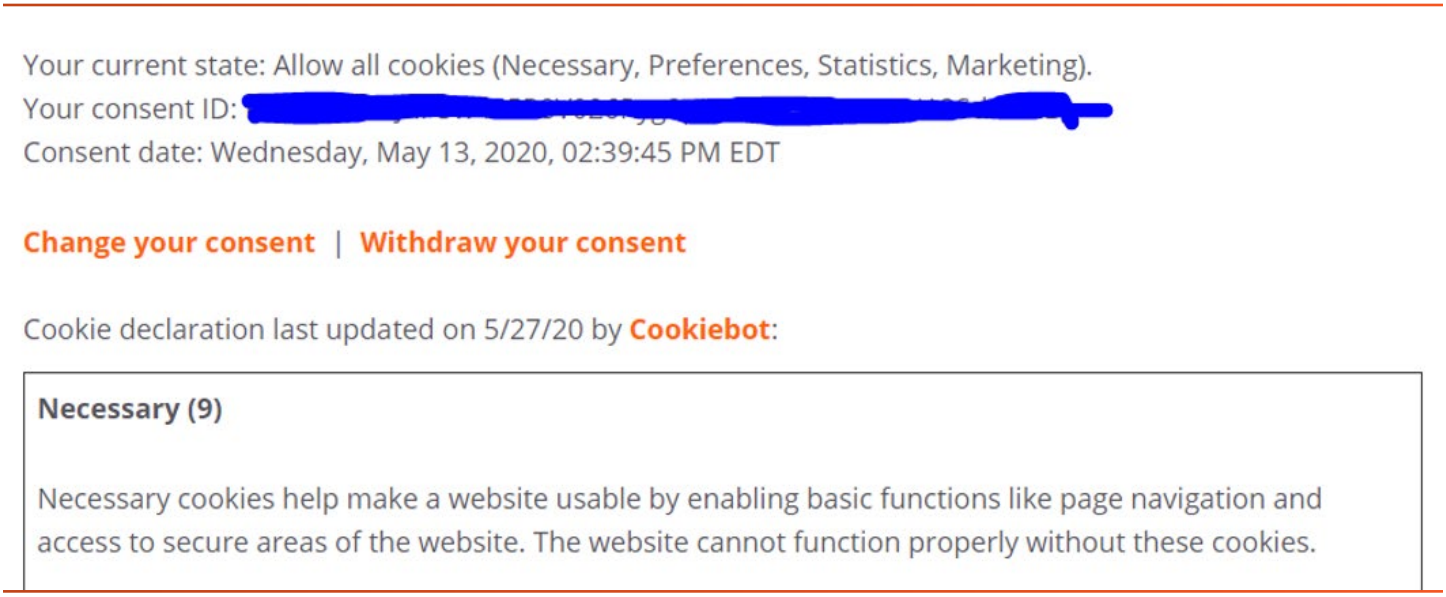
There are exceptions to the permission requirements—employment information, for example. You can't really hire someone without collecting a lot of personal data. Neither one of you has any real choice in the matter: much of the information is required by law. The rest is a practical necessity, since you can't pay employees or provide them with health insurance without knowing some things about them. Even then, however, disclosing the uses to which you intend to put the information is mandatory in many places, and is certainly good practice everywhere.

Retaining and protecting information

Since you cannot keep personal information forever, storing it away in a database or filing cabinet, you must have a *retention schedule*. You'll have to figure out how to apply that schedule in an electronic system that might not be designed for the purpose or a messy physical filing system.

And then there's access: your disclosures should contain some access restrictions specifying who is allowed to look at the information and why. The very nature of the information—say personal medical information or bank account numbers—may clearly imply the need for access restrictions and data security. Either way, you now need to build or alter some processes to assure reasonable protections for the data. For other kinds of personal information, self-service access to the data you collect and granular control over that information can be enabled by technology.

Access provides granular cookie consent management for all website users on its cookie policy page:



Your current state: Allow all cookies (Necessary, Preferences, Statistics, Marketing).
Your consent ID: [redacted]
Consent date: Wednesday, May 13, 2020, 02:39:45 PM EDT

Change your consent | **Withdraw your consent**

Cookie declaration last updated on 5/27/20 by **Cookiebot**:

Necessary (9)

Necessary cookies help make a website usable by enabling basic functions like page navigation and access to secure areas of the website. The website cannot function properly without these cookies.

As you can see, there's a lot of process engineering, and re-engineering, involved in assuring data privacy, and we've only just begun. Accommodating the basic concept of privacy compliance—asking for permission and disclosing the uses of the data—involves substantial effort, and may require an equally substantial budget. If you're implementing a privacy program, you need to bear this in mind.

The philosophy may sound simple, but the implementation rarely is. Keep a firm foot on the accelerator.

For more on how to ensure PII is collected responsibly, check out this webcast recording:
Webcast: Privacy Impact Assessments – Why You Need Them, What You Need to Know

How fewer records end up leading to yet more records

Let's look at some other key aspects of privacy.

As we have discussed, PII is the property of the person it's about, and you need to get permission to use it *after* clear disclosure of what you intend to use it for. Since you can keep it only so long as your organization needs it for that original purpose, it's a good idea to state the retention period in the original disclosure.

The problem of provability

So far, so good—it sounds like a simple and perfectly reasonable proposition. But, in most cases, that simple proposition is enforced by a legal regime that imposes penalties on the collecting organization for failing to disclose intended use and retention period. Those penalties may be arbitrarily large as in the E.U., where the local Data Privacy Authority (DPA) can impose pretty much whatever penalties it sees fit, or seemingly small penalties can be imposed by statute according to some schedule. Here's the rub, though, about that seemingly small penalty: *a small number multiplied by a large number*

equals a much larger number. A $100 fine per violation might seem like it's not worth bothering too much about, but if each individual person is a violation and the violation involves 50,000 people, the aggregate penalty balloons very quickly. Failure to collect all of the needed permissions could easily result in an alarmingly large number.

As a practical matter, this means that it's not enough to make the disclosure and obtain the permissions: you have to be able to prove you did so. And that means keeping records of it.

The irony of it all is that laws that require you to keep as few records containing PII for as short a period of time as possible, also pretty much require you to create new records to prove compliance, even if they don't explicitly say so. Those new records, of course, contain PII, showing as they do that you made a particular disclosure to a specific person and obtained the permission of that person to collect and use their information. Likewise, your new permission and disclosure records are subject to the same privacy laws as your other records containing PII, and you can keep them only as long as needed. You therefore need to determine and enforce a retention period for them.

In practice, this requirement can lead to a lot of records. Even very small businesses with a web presence or a heavily customer-facing business model can touch a lot of people, and will have reasons to collect information about as many of them as possible. Nor are customers and prospects the only people you need to think about. In some places, you must make pretty much the same disclosures to employees and others. Very quickly, it gets way past the "we'll-track-it-on-a-spreadsheet" phase and into an automated management regime that, for example, tracks the people who opt in to information collection on a website.

The disclosure requirements apply to any sort of web-enabled fill-in form, and most of us have encountered web forms with disclosures and opt-in check boxes concerning privacy. The owner is undoubtedly tracking your opt-in for exactly the reasons we just discussed. If you were to file a complaint—and people do—the organization would respond by producing a record of the date and time you opted in, and probably a copy of the language of the disclosures and permissions.

Establish a "reasonable" retention period

The inevitable question is, how long do we keep this stuff? The answer: a reasonable period, whatever that is. In the absence of a hard requirement that may or may not exist, you need to determine what the applicable statute of limitations is for privacy violations in the jurisdiction(s) in question. It might be a specific statute of limitation for privacy violations, or it might be a more general one. Whichever, that's your starting point. Remember, you're allowed to keep these records long enough to defend yourself in a legal action or administrative investigation, but if you think you might want to keep them longer than that, do so advisedly, and make sure your reasoning is sound and strong.

The last thing you need is a privacy violation for trying to avoid a privacy violation!

Access

1.877.345.3546

AccessCorp.com

About Access

Access is the largest privately-held records and information management services provider worldwide, with operations across the United States, Canada, Central and South America. Access provides transformative services, expertise, and technologies to make organizations more efficient and more compliant. Access helps companies manage and activate their critical business information through offsite storage and information governance services, scanning and digital transformation solutions, document management software including CartaHR, CartaDC and CartaDC Essentials, and secure destruction services. For 11 consecutive years, Access has been named to the Inc. 5000, the ranking of fastest-growing private companies in the U.S.