

# The New US Data Privacy Environment: Are You Ready?



## Introduction

The US data privacy legal environment is not—at this point—an easy one to navigate. Unlike in the EU, there is no federal-level equivalent to the groundbreaking General Data Protection Regulation (GDPR): a single law guaranteeing the privacy of consumer data held by companies. Instead, there are several US data laws that apply to different verticals—primarily the Gramm-Leach-Bliley Act (GLBA) for banking, and the Health Insurance Portability and Accountability Act (HIPAA) for health data.

With a privacy law vacuum at the federal level, US states began a few years ago to fill the void with their own local laws. This effort has been led by California with its Consumer Privacy Act (CCPA) and by Virginia, which recently passed its Consumer Data Protection Act (CDPA). Other states are also planning their own privacy laws—the list includes New York, Massachusetts, Illinois, and Colorado.

It certainly makes US privacy law more than a little confusing. While we wait for federal privacy legislation, these state laws give consumers credible data privacy rights on par with the GDPR: consumer control over their personally identifiable information (PII), and legal restrictions on how that data can be used.

Interestingly, the EU GDPR has had a direct impact on the evolving US privacy environment. First, the GDPR affects US multinationals doing business in the EU. Whether the US company registers its subsidiary in say Ireland or Germany, it would, of course, have to abide by the single GDPR law.

This fact alone has nudged major companies, such as Microsoft, to adopt the tougher GDPR privacy standards in the US in anticipation of new privacy laws to come. And in fact, with CCPA, which many consider “GDPR-lite,” US companies are forced to comply with its stricter privacy rules if they wish to do business in the world’s fifth largest economy.

Second, the language and ideas of the GDPR have influenced privacy policy makers at both state and federal levels. Congress is now considering several privacy laws that borrow heavily from the GDPR framework, incorporating terminology and key principles. It makes sense then to first look at the EU to begin to understand US data privacy.

## Brief Review of GDPR's Privacy Requirements

The GDPR is a sprawling legal document with rules spread out over 100 separate sections or “articles” along with a long introductory “recital” setting the legal context. Unlike the CCPA, it is both a data security and a privacy law. For the purposes of this white paper, we'll just focus on its privacy aspects. But before we dive into the specifics, let's go over some basic terminology used in the document.

In the GDPR, personal data means any information that relates “to an identified or identifiable” data subject. A data subject is “an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used” by someone. The GDPR legislators intentionally devised this abstract definition rather than enumerating specific identifiers.

In effect, the GDPR's personal data encompasses obvious identifiers such as phone numbers, addresses, and account numbers as well as new Internet-era identifiers, such as email, biometric, online handles, IP addresses, and new identifiers yet to — anything that relates to the person.

This definition also accounts for what's known as *quasi-identifiers*. These are multiple data fields, typically geo and date information, which taken together and with a little bit of extra processing can be used to re-identify the individual. In any case, GDPR's personal data is what companies are supposed to keep private and secure.

### *Data Controller and Data Processor*

The GDPR also uses the terms data *controller* and data *processor*.

A data controller is anyone or entity that determines the “purposes and means of processing of the personal data.” It's another way of saying the controller is the company that makes the decisions to initially collect data from the data subject.

A data processor is any entity that processes data for the controller. By the way, the GDPR specifically mentions storage as a processing function, taking into account cloud-based virtual storage.

The reason for these separate definitions is that the GDPR has language that covers security and privacy requirements for *data processors*: it closes a loophole that would have allowed outsourced data processing of personal data to escape the GDPR rules, especially if the processors are not within the EU.

The GDPR rules affecting data processors have not gone unnoticed by cloud computing providers such as Google or Amazon AWS: they have proclaimed their compliance with the GDPR on their websites

It's also worthwhile to point out that *data controllers outside of the EU zone* can also fall under the GDPR. Its controversial Article 3 (“Territorial scope”) would apply to e-commerce companies and websites that may not have an *actual physical presence* in the EU but still collect their personal data as part of a transaction over the Internet.



If a US e-commerce company's web copy is, for example, written in the *local language and accepts the local currency* it would be considered to be doing business in the EU! US web-based business that localize their websites can indeed fall under the extraterritorial reach of Article 3.

## GDPR Consumer Privacy Rights

Let's now drill down into the GDPR's privacy requirements.

In Article 6 ("Lawfulness of processing"), consumers have to give explicit consent for the "processing of his or her personal data for one or more specific purposes." No consent, no processing.

In Article 15 ("Right of access by the data subject"), consumers have the right to request from the data controller at any time information about the personal data being taken, including:

- the purpose of the processing
- the categories of personal data
- the specific recipients (or categories of recipients) of the personal data
- the period for which the data will be stored.

If the personal data is inaccurate, the data subject has a right to correct the data, as spelled out in Article 16 ("Right to rectification"), and the data controller has to carry out the changes without "undue delay."

The right to view and correct the data is powerful, but the GDPR goes even further. Article 18 ("Right to restriction of processing") gives the consumer the right to discontinue processing of their personal data at any time under certain conditions—for example when the data is inaccurate or the processing is unlawful as detailed in Article 6. The controller would have to stop processing until the data is corrected.

The GDPR grants still more consumer control over personal data with probably its most publicized rule, Article 17 ("Right to Erasure"/"right to be forgotten"). The consumer has a right "to obtain from the controller the erasure of personal data concerning him or her without undue delay" as long as any one of several conditions are met.

The reasons for erasure can be that the data is no longer needed for processing, the data was obtained unlawfully, or that the data subject simply withdraws consent. There are free speech considerations that can override these requests—an online newspaper can't necessarily be forced to delete unfavorable stories or news about a data subject. There is also something the GDPR calls "legitimate interests" of the controller that can outweigh the data subject's rights in certain situations.

The "right to be forgotten" is the more controversial part of this article, and covers the case where the controller has shared the information with other processors.

Translating to practical language: it means that internet social media companies would have to not only delete the original data—graphic, post, tweet— but ask other websites that have copied the data to delete as well. In the language of GDPR, they're allowed to take account of "available technology and the cost of implementation, and then take reasonable steps..." to ensure the shared data is removed.

## *GDPR Privacy Obligations for Controllers and Processors*

It should be obvious that the likes of Google, Twitter, and Facebook are not happy about the "right to be forgotten." Nonetheless, it is one of their privacy obligations under the GDPR, and they have responded. For example, Google has a data subject access request ([DSAR](#)) form to allow the public to request deletion. The GDPR's right to access and the right to rectification forces companies to also make available similar online DSAR forms.

There are still other privacy obligations for controllers and processors that would force businesses to put in place even more IT processes and procedures. Some of us may be familiar with the principles of Privacy by Design (PbD), which were first formulated and promoted by [Ann Cavoukian](#) when she was Information and Privacy Commissioner in Ontario in the late 90s. These PbD privacy principles are reflected in many parts of the GDPR.

Specifically, PbD's focus on data minimization—reducing the initial collection, access, and processing—as a data privacy goal can be found in GDPR's Article 25 ("Data protection by design and default"). It's useful to look at the actual gritty details of this article. A data controller is required

"...to implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular .... that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

Minimization of access, processing, and limits on how long the data is stored are good IT principles. The key point is that under the GDPR, it's a law that has to be implemented.

Finally, the data controller and processor are required to inform the consumer as well as EU regulators, known as supervisory authorities, when personal data has been breached and the types of data that have been taken. This has to be done within a tight 72-hour window after discovery. Again, this is yet another rule that would force companies to have in place substantial IT monitoring and data classification software in order to be compliant.



## Existing US Federal Data Privacy Protections

### *US Privacy Act of 1974*

The grand-daddy of all US privacy legislation has its roots in the 1970s. In this pre-personal-computer era, the reigning technologies were mainframes and large databases. Privacy advocates at the time were concerned, and rightly so, about government misuse of this data. Congress passed the landmark US Privacy Act of 1974, which protected public data held by any US governmental agencies. Despite its name, it did not apply to the private sector.

Having already reviewed, GDPR and Privacy by Design, this law's data rights should look very familiar. Let's list them here because it's the first time these rights were explicitly mentioned in US law:

- Right of US citizens to access any data held by government agencies. And a right to copy that data.
- Right of citizens to correct any information errors
- Agencies should follow data minimization principles when collecting data – least information “relevant and necessary” to accomplish its purposes.
- Access to data is restricted on a need to know basis – for example, employees who need the records for their job role.
- Sharing of information between other federal (and non-federal) agencies is restricted and only allowed under certain conditions.

There were strong civil liberties reasons for restricting sharing of personal data between agencies. In fact, the Privacy Act of 1974 came about in response to illegal surveillance revelations from the Watergate investigations.

While its rules apply only to government agencies, the Privacy Act was ahead of its times in articulating core privacy rights—right to view, correct, and control data—and anticipates the new wave of privacy laws in the US today.

### *US Privacy Act of 1974*

In 1996, the Health Insurance Portability and Accountability Act was enacted by Congress to regulate the health insurance sector. It also included (at the time and still to this day), the US's most comprehensive data protections. HIPAA's mission is summed in the following language: “to maintain reasonable and appropriate administrative, physical, and technical safeguards to ensure the integrity and confidentiality of the information, and to protect against any reasonably anticipated threats.”

Like the GDPR, HIPAA has both data security and data privacy regulations. They can be found, respectively, under The [Security Rule](#), and The [Privacy Rule](#).

If you've ever filled in a form at a US doctor's office allowing spouses and other family members to review or see your health information — what HIPAA refers to as protected health information (PHI) — you're seeing the Privacy Rule in action.

The Privacy Rule contains complex criteria and rules deciding on who gets to see PHI. But in short, a healthcare provider or other “covered entity” more or less has permission to use patient data if it’s related to “treatment, payment, and health care operations.” However, using the data for marketing purposes or selling the PHI requires *explicit authorization*.

HIPAA’s [minimum necessary requirement](#) is a good example of PbD principles applied to the sharing of PHI. It says that covered entities that share data for marketing purposes other than the ones mentioned above should limit who gets to access it. Health organizations are supposed to evaluate their data and practices and put in place safeguards to limit “unnecessary or inappropriate” access to PHI. In effect, HIPAA requires role-based access control for PHI.

HIPAA is also unique in federal privacy laws in having a breach notification rule, which was later added in 2009. It requires covered entities to notify affected individuals following the *“discovery of a breach of unsecured protected health information (PHI).”*

For breaches involving more than 500 people, the covered entity has to report the breach to the Department of Health & Human Services (HHS) where it posts the incident on its online [wall of shame](#). HHS also has the power to investigate and fine covered entities for violations—this often involves [unauthorized access](#) to PHI by employees

To learn more about HIPAA compliance, read our [white paper!](#)

### *Gramm-Leach-Bliley Act (GLBA)*


The Gramm-Leach-Bliley Act is another enormous piece of US late-90s legislation, in this case regulating the banking and financial sectors. Similar to HIPAA, but not nearly as strict, it has embedded in it important data privacy and security requirements. Its protections of personal information were a major improvement over the existing consumer financial data laws.

GLBA protects non-public personal information (NPI), which is defined as any “information collected about an individual in connection with providing a financial product or service, unless that information is otherwise publicly available” — essentially PII with an exception for any widely available financial information such as, for example, property records or certain mortgage information.

In the US, banks are required to periodically mail out data privacy notifications, explaining the categories of NPI that are being collected and shared, along with special opt-out instructions. We’ve all received these notices, and likely ignored them. In any case, this mailing is a direct consequence of GLBA’s somewhat limited privacy protections. Consumers can opt-out if they don’t wish the information to be sent to a “non- affiliated” third party.

However, for third-party companies affiliated with the bank or insurance company — part of the bank’s expansive “corporate family” — consumers have no legal privacy controls under GLBA to restrict the sharing of the NPI. That’s quite a large loophole, and GLBA is by no means a model for an Internet-era privacy law.





The GBLA also does not have an explicit data breach notification rule, and it's up to various agencies charged with enforcing the law—including the Federal Trade Commission (FTC), Securities and Exchange Commission (SEC), and the US Federal Reserve—and to decide whether protecting the data against unauthorized usage involves notifying consumers and other organizations whose data has been exposed.

### *Children's Online Privacy Protection Act (COPPA)*

Back in the early days of the Internet, the Children's Online Privacy Protection Act took a giant step to regulating personal information collected from minors. The law specifically prohibits online websites that are "directed to children" from asking for PII from those 12-and-under unless there's verifiable parental consent. COPPA is enforced by the FTC, which can seek civil penalties

Updates to COPPA's regulatory rules a few years ago effectively expanded the reach of the law and broadened the type of PII to be protected, including screen names, email addresses, video chat names, as well as photographs, audio files, and street-level geo coordinates.

These updates also extended privacy and security coverage to third parties that use the children's data. The originating website operator must take "reasonable steps to release children's personal information only to companies that are capable of keeping it secure and confidential." The PII that's collected and third-parties that can receive the data has to be displayed in clear language on the website or app. Parents can always opt out of third-party data sharing if they so choose.

While COPPA is limited in scope—no detailed rules on how the data is to be protected and no breach notification requirement—it is unique among US privacy laws in that it acknowledges internet-era technology, and protects PII outside of medical and financial usage.

## **The State of US State Privacy Laws**

Lack of direction from Washington—at least until recently—has led US states to draft their own privacy laws. After the GDPR was finalized in 2016, its privacy concepts—explicit consent, right to access, and "right to be forgotten"—had a direct influence on privacy policy makers in the US, both at the state and federal level. But it was the states—California to be specific—that first granted comprehensive privacy protections to consumers.

In 2018, the groundbreaking California Consumer Privacy Act (CCPA) was signed into law, giving its citizens something close to GDPR-like privacy. Other states soon followed drafting their own "copycat" legislation. However, as of early 2021, only one other state, Virginia, has signed GDPR-level privacy legislation into law. Let's look at California and Virginia's law first and then review a few other key states proposed privacy features.



## California Consumer Privacy Act (CCPA)

Under the CCPA, consumers in California have GDPR-level privacy rights. They include:

- Right to know the categories and specific pieces of personal information that will be held by covered businesses as well as the reasons for collecting this data. The consumer has to be notified of this information “at or before the point of collection.”
- Right to request a report of all personal data currently held by the business. This information shall be provided free of charge, and delivered by mail, or electronically in a portable format. This is accomplished through a “verifiable” request.
- Right to request the business delete all information about the consumer. Like the GDPR’s “right of erasure”, this is not an absolute right, and there are some exceptions.
- Right to correct inaccurate information. Businesses have to inform consumers of this right, which corresponds to GDPR’s “right of rectification.”
- Right to know what categories of business information being sold to third-parties. The consumer has to be given the right to opt out before this personal data can be sold.
- Right to opt out of data shared or sold to third-parties. This right can be exercised any time.


These rights, of course, require that California business have in place the technical infrastructure to support the DSARs implied by these rights. With the right to delete, it also means that IT department would have to enable searching file systems for specific personal data, and then be able to remove personal data references—not something that can be effectively accomplished on an ad hoc basis.

Another striking innovation within the CCPA is its very broad definition of personal information. It is similar to the GDPR’s own expansive view of personal data. The CCPA does indeed contains a traditional list of identifiers it considers personal information, including biometric, geolocation, email, browsing history, employee data, and more.

But it’s not an exhaustive list. Instead the CCPA more abstractly defines personal information as anything “that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.” It’s essentially a GDPR-style definition of PII, and the list of identifiers are provided as merely current examples.

Even more interestingly, CCPA defines a concept of “probabilistic identifiers” that can be used to determine a “consumer or a consumer’s device to a degree of certainty of more probable than not” by using personal information. It’s effectively the quasi-identifiers that we referred to above in describing the GDPR’s personal data. This has been more of a security researcher’s concept, but with CCPA quasi-identifiers are now explicitly written into law, broadening the scope of what’s considered identifiers!





Another significant aspect of the CCPA is that it may have, like the GDPR, an extraterritorial reach beyond the state borders. The law technically applies to any company that “does business” in California, and this can be interpreted to apply to companies that don’t have physical presence but collect personal data through a website. It’s very similar to the remote GDPR data collector example previously discussed.

Overall, CCPA have given its residents control over their personal data, and is the first US state to legislate a credible right to privacy for data. So far, so good. But does CCPA have more bark than bite?

The state Attorney General can sue on behalf of residents and seek civil penalties of \$2,500 for each violation or \$7,500 for each intentional violation. The business, thought, has to be first notified and given a 30-day opportunity to correct the action. The CCPA has a far more potent incentive to ensure companies comply by granting its citizens a “private right of action”— they can sue businesses directly through class actions.

The class-action suits can only be taken if there’s been a data breach involving unauthorized access or data theft. With huge data breaches a common occurrence these days, the CPPA could spawn settlements potentially adding up to millions of dollars. Be warned: California law firms are currently testing this law in the courts.

### *Virginia’s Consumer Data Protection Act (CDPA)*

After California, Virginia is currently the only other state to pass a credible privacy law. In fact, its Consumer Data Protection Act goes even further than the CCPA. Besides including all of the CCPA’s privacy rights (right of access, right to correct, right to deletion, right to opt-out of the sale of personal data), and its abstract definition of personal data, Virginia’s CDPA puts business under a more formal privacy and security framework.

It borrows GDPR terminology of data controllers and data processors and directly places several obligations on both, mirroring the GDPR’s Article 5 (“Principles related to processing of personal data”). They include as follows:

- **Data Minimization** — Controllers can only collect personal that is “adequate, relevant and reasonably necessary in relation to the purposes for which the data is processed.”
- **Limitations and consent** — Controllers require consent to process data beyond what is “reasonably necessary” to the purposes initially disclosed to the consumer. In short: the controller can’t use data in ways the consumer is not aware of unless it’s been approved.
- **Reasonable data security** — Very much in the spirit of the GDPR, the controller is explicitly required to implement “reasonable administrative, technical, and physical data security practices.” What reasonable means here will have to spelled out by the regulators.
- **Assessments** —In effect, controllers have to undertake risk assessments with respect to special classes of personal data: data used in “targeted marketing,” data that is sold to third-parties, and “sensitive data” involving racial or ethnic origin, religious belief, medical information, and sexual orientation.

- **Processor contract** — Similar to the GDPR, the Virginia laws requires controllers to have contracts with processors to ensure that they too are protecting consumer privacy. The contracts are required to contain specific legal terms.
- **Additional processor obligations** — Data processors are also required to assist the controllers with consumers' rights requests—that is, DSARs—as well as informing the controller of a data breach.

Unlike the CCPA, there is no private right of action for violations of the act: only the Virginia attorney general has exclusive enforcement authority. The attorney general can seek injunctive relief, and civil penalties of up to \$7,500 per violation.

Overall, it's a step closer to what a federal-level that aspires to be less burdensome version of GDPR—a goal of some of the proposed legislation currently kicking around Congress.

### *New York and the Rest*

While there are data privacy legislative efforts in several states, they are all currently stalled in committee—in New York, Massachusetts, Colorado, Illinois, and more. Reviewing these copycat bills becomes an exercise in comparing and contrasting to the CCPA — variations of the California laws and more often than not they lack the power of the CCPA.

For example, New York's Senate Bill S567 has many but not all of the basic ingredients of the CCPA: right of access, right to opt-out of sale of personal data, and right to know categories of data being collected. It also has a generalized definition of personal information— "information that identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked" to any person or device.

However, a right to correct and right to delete inaccurate information is lacking in the current Senate bill. Interestingly, there is potent private right of action allowing for class-action suits in which consumers can sue for alleged violations, including technical non-compliance. Penalties start at \$1000 per violation, and unlike the CCPA there doesn't first have to be a data breach!

Below is a table summarizing the major rights found in privacy laws in several key states, along with their status. For a current picture of these bills, which are still in flux, review the [IAAP's State Privacy Legislation Tracker](#).



State	Bill	Status	Right of Access	Right of Deletion	Right to correction	Right of private action	Risk assessment
California	CCPA	passed	✓	✓	✓	✓	✓
Virginia	CDPA	passed	✓	✓	✓		✓
Colorado	SB190	pending	✓	✓	✓		✓
Connecticut	SB 893	pending	✓	✓	✓		✓
Illinois	HB 1310	pending	✓		✓		✓
Mass.	SD 1726	pending	✓	✓	✓	✓	
Minnesota	HF 1492	pending	✓	✓	✓	✓	✓
New York	SB 567	pending	✓			✓	✓
New Jersey	AB 3283	pending	✓	✓	✓		✓

### *A Look at the Information Transparency and Personal Data Control Act*

With a possible future of many differing and conflicting privacy laws at the state level, it's not surprising that the private sector, particularly tech companies, would favor a single federal law. In 2019, the CEOs of 51 tech companies, including Amazon, IBM, and Salesforce, sent an [open letter](#) to Congress asking for just that: "a comprehensive consumer data privacy law that strengthens protections for consumers and establishes a national privacy framework."

It's not as if the US Congress hasn't been considering a privacy law. There are several laws that have been proposed in recent years, among them Senator Markey's [Privacy Bill of Rights](#), Senator Cantwell's [Consumer Online Privacy Rights Act](#), and Senator Wicker's [Consumer Data Privacy Act](#). All of these grant consumer basic data privacy rights to access, correct, and delete data. The Federal Trade Commission would also be given enforcement and regulatory powers.

As always, the devil is in the details, and lawmakers will have their work cut out. One contentious issue is under what situations federal privacy law can pre-empt a state-level law. The above bills take differing approaches with Wicker's bill allowing for complete pre-emption and Cantwell's instead pre-empting only when the state law conflicts with the federal. The real tension is that a federal law might ultimately weaken more powerful state law, particularly the CCPA and CDPA.

In any case, all the current legislation has been strongly influenced by the GDPR. One very recent example of this, which has been making the news, is Representative DelBene's Information Transparency and Personal Data Control Act (ITPDCA). It's a short bill —thankfully not nearly as complicated as the GDPR—and it's worthwhile to scan it just to get a sense of what these Congressional privacy bills are like.

The ITPDCA proclaims basic privacy rights to:

- “exercise control over the personal data companies collect from them and how they use it”.
- “access and correct personal data in usable formats, in a manner that is appropriate to sensitivity of the data”.
- “reasonable limits on the personal data that companies collect and retain”.

More specifically the ITPDCA gives consumers “affirmative, express, and opt-in” consent when their data is collected, transmitted, stored or sold. Consumer can also opt-out of data that is shared with third-parties at any time. Surprisingly, the bill does not have a right to delete. It also doesn’t have a GDPR-like definition of personal data: it merely lists identifiers, which include Internet-era PII (geolocation, web-browsing history.)

The bill though explicitly uses the GDPR terms data controllers and processors, and like the GDPR forces these two to have a contractual arrangement in which the processor requires the direct approval from the controller regarding any data processing decision.

Interestingly, this bill places audit requirements on both controllers and processors. They would have to obtain from an independent, qualified third party an assessment of their “privacy, security, and data use controls.” It’s not an obligation seen in state data privacy laws, and there’s no such requirement in HIPAA or the GLBA!

Finally, there’s no private right of action to sue companies,

What about penalties?

The Federal Trade Commission is charged with enforcement, and the ITPCDA would allow it to penalize violators under the FTC’s unfair or deceptive acts or practices powers, which are substantial. It should be noted that the FTC fined Facebook \$5 billion under just those powers when Facebook lied about its privacy protections. By the way, this bill pre-empts all state privacy laws, so there would be no escaping the FTC.

No one knows what the final form of a US privacy law might be. It’s a good bet that in trying to escape the complexity of the GDPR, something like the ITPCDA might become law, with the FTC taking the lead as the enforcer and given regulatory powers to create rules as needed.

## Closing Thoughts on US Privacy

Companies that are large enough to have multinational operations or have a web presence in the EU are already dealing with the GDPR. For them an eventual US privacy law would be taken in stride. The same could be said for companies doing business in California and Virginia: they too should have no problem in complying with a federal-level law.





Of course, that leaves a huge swath of corporate America that never before has had to face a federal-level data privacy law. Ultimately the key issue for them is knowing in depth, perhaps for the first time, *low-level details of the PII they hold*, including the basics of how much, where its located, and who has access. With even smaller corporate file systems reaching ever closer to the zettabyte level, IT managers would have their hands full just finding out these basics.

To comply with these laws, they'll have to put in place the infrastructure to meet DSAR requests for access, correction, and deletion. The problem of course is finding the metaphorical needle in the haystack: locating files that contain the *specific* PII associated with the requester! In addition to meeting DSAR requests, these proposed laws often contain language requiring businesses to also implement "administrative, technical, or physical safeguards" for protecting the data.

In short, they're expecting privacy and security controls, and the documentation to show they are working and adjusted when there are shortfalls.

Obviously, privacy laws with teeth "up the game", making in-house solutions a less than satisfactory approach to compliance. With enforcement of these laws including monetary penalties, there are real bottom-line consequences. Data privacy is no longer just a good idea, but will soon be the law, likely, with a real bite to it.

To learn more about how Lepide can help with a [data privacy solution](#) to meet the coming US federal law, schedule a [demo](#) with one of our engineers or start your [free trial](#) today!

## ABOUT LEPIDE

Lepide are the fastest growing provider of data-centric audit and protection solutions to enterprises all over the world. The award-winning Lepide Data Security Platform enables you to put your data at the heart of your security strategy; mitigating the risks of data breaches and helping to meet compliance requirements.

Protecting the Data of Thousands of Organizations Worldwide



Western Connecticut  
Medical Group

**HOGG · FENTON**



**FIRSTLEGAL**



GE Healthcare

**FUJITSU**

**NHS**

**Deloitte.**

