Gartner

Gartner for Legal, Risk & Compliance

10 External Privacy Policy Updates for 2025 Based on Benchmarking

Overview

Key findings

- Legal, compliance and privacy leaders are updating their external privacy policies in response to recent U.S. and global regulations.
- Many organizations are staying ahead of these new requirements by expanding cookie consent and consumer opt-out options, contextualizing how they share data with third parties and addressing AI.
- Legal, compliance and privacy leaders are using these updates as an opportunity to be more transparent with consumers and employees by making privacy policies easier to navigate through regionalized policies, portals, menus and infographics.

Recommendations

- Review your external policies to assess potential gaps in compliance with current and upcoming privacy laws.
- Review the following top updates and prioritize implementing those that will satisfy common regulatory requirements and those that entail high risks or large penalties.
- Leverage user experience improvements such as navigable menus and privacy hubs or centers to make policies easier to use and understand for customers and employees.

Balance regulatory compliance with greater transparency

Twenty U.S. states currently have strict consumer privacy protections in place, including the California Privacy Rights Act (CPRA) and Colorado Privacy Act (CPA). In addition, many other global privacy regulations have come into play, including the EU's ePrivacy Directive and Artificial Intelligence (AI) Act. As new requirements proliferate, legal, compliance and privacy leaders should consider two ideas when updating their external privacy policies:

1. External privacy policies must comply with an increasingly complex set of privacy regulations.
2. Organizations must grant customers and employees greater transparency into and control over their personal information.

By incorporating the following updates into their external policies, legal, compliance and privacy leaders can work toward compliance with new and emerging state and global privacy laws. These leaders can also maintain a level of simplicity and transparency in their external policy that will drive greater usability and scalability with consumers.

Expanded or added clauses

Top companies have implemented the following updates or new clauses to the content of their external privacy policies over the past few years.

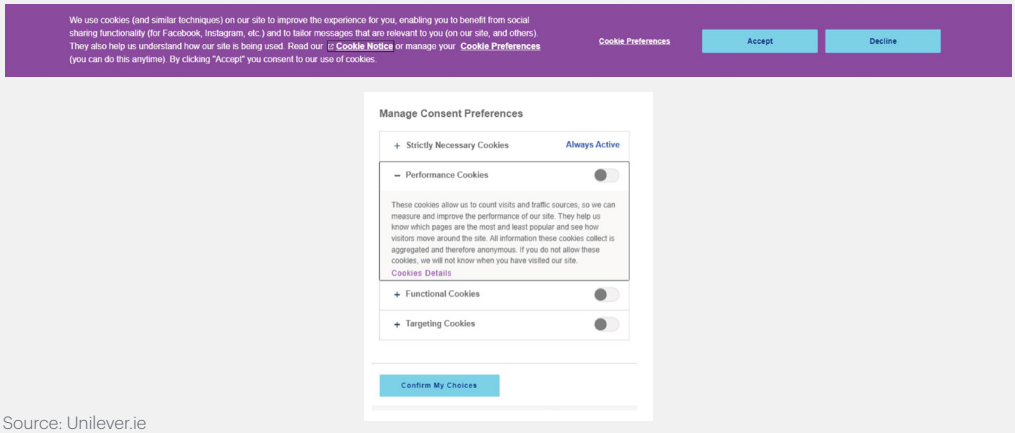
1 Expanded cookie consent options

The EU ePrivacy Directive places new requirements on “service providers,” such as telecommunications, which employ cookies. These organizations must provide clear notice to users when they are collecting cookies, must only collect cookies with active consent, and must provide a real choice for users to deny cookie collection as they proceed to the website. Users can give consent by clicking a button provided in a pop-up window, or by configuring browser settings to accept or deny certain types of cookies.

While this regulation does not extend to all companies, many organizations are adopting cookie consent options proactively. Organizations typically offer consumers three choices:

1. Accepting all cookies
2. Denying all but those that are required for use of the website as well as audience measurement, which is not covered under the new law
3. Allowing users to customize their settings

Unilever Ireland’s cookie notice

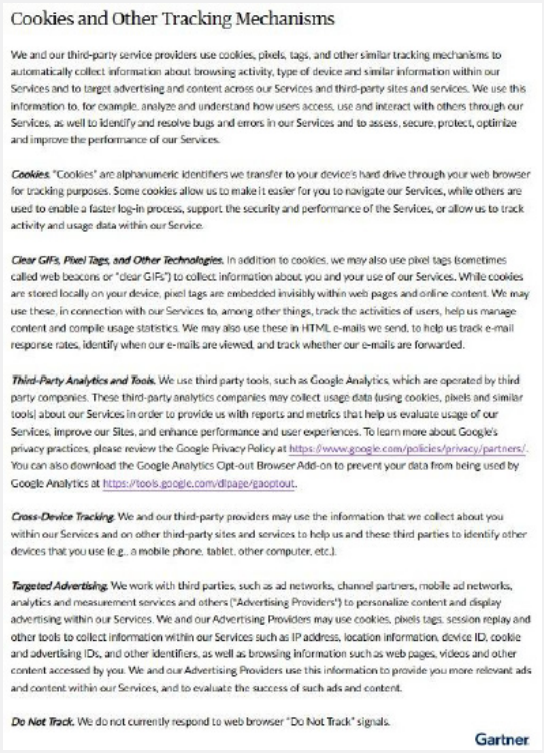


Source: Unilever.ie

Gartner

Organizations taking a more progressive approach enhance customizability by allowing consumers to accept or deny different categories of cookies based on the organization's use case for the data. These organizations have added information to their policies about what cookies are and what they track using cookies. For example, Chubb Limited begins the "Cookies and Other Tracking Mechanisms" section of its policy with an easy-to-understand definition for cookies, as well as what they are used to track and why.

Chubb Limited's cookie and other tracking mechanisms clause



Cookies and Other Tracking Mechanisms

We and our third-party service providers use cookies, pixels, tags, and other similar tracking mechanisms to automatically collect information about browsing activity, type of device and similar information within our Services and to target advertising and content across our Services and third-party sites and services. We use this information to, for example, analyze and understand how users access, use and interact with others through our Services, as well to identify and resolve bugs and errors in our Services and to assess, secure, protect, optimize and improve the performance of our Services.

Cookies. "Cookies" are alphanumeric identifiers we transfer to your device's hard drive through your web browser for tracking purposes. Some cookies allow us to make it easier for you to navigate our Services, while others are used to enable a faster log-in process, support the security and performance of the Services, or allow us to track activity and usage data within our Service.

Clear GIFs, Pixel Tags, and Other Technologies. In addition to cookies, we may also use pixel tags (sometimes called web beacons or "clear GIFs") to collect information about you and your use of our Services. While cookies are stored locally on your device, pixel tags are embedded invisibly within web pages and online content. We may use these, in connection with our Services to, among other things, track the activities of users, help us manage content and compile usage statistics. We may also use these in HTML e-mails we send, to help us track e-mail response rates, identify when our e-mails are viewed, and track whether our e-mails are forwarded.

Third-Party Analytics and Tools. We use third party tools, such as Google Analytics, which are operated by third party companies. These third-party analytics companies may collect usage data (using cookies, pixels and similar tools) about our Services in order to provide us with reports and metrics that help us evaluate usage of our Services, improve our Sites, and enhance performance and user experiences. To learn more about Google's privacy practices, please review the Google Privacy Policy at https://www.google.com/policies/privacy/partners/. You can also download the Google Analytics Opt-out Browser Add-on to prevent your data from being used by Google Analytics at https://tools.google.com/dlpage/gaoptout.

Cross-Device Tracking. We and our third-party providers may use the information that we collect about you within our Services and on other third-party sites and services to help us and these third parties to identify other devices that you use (e.g., a mobile phone, tablet, other computer, etc.).

Targeted Advertising. We work with third parties, such as ad networks, channel partners, mobile ad networks, analytics and measurement services and others ("Advertising Providers") to personalize content and display advertising within our Services. We and our Advertising Providers may use cookies, pixels tags, session replay and other tools to collect information within our Services such as IP address, location information, device ID, cookie and advertising IDs, and other identifiers, as well as browsing information such as web pages, videos and other content accessed by you. We and our Advertising Providers use this information to provide you more relevant ads and content within our Services, and to evaluate the success of such ads and content.

Do Not Track. We do not currently respond to web browser "Do Not Track" signals.

Gartner

Source: Chubb Limited

To do:

- Update your cookies notice to provide users with clear information on what cookies are and how they are used by the organization.
- Give users a clear option to either deny or accept cookies at the initial pop-up.
- Provide easy-to-access customizable controls that explain how different types of cookies are used, as well as easy-to-use options (e.g., radio buttons or toggles) to opt out of each type.
- Work with customer-facing parts of the business to surface and eliminate menus, websites or other user-facing design elements that intentionally trick or manipulate users into making choices they otherwise would not have. [1]

Gartner

2 Increased opt-out rights

A host of new privacy regulations have expanded consumer rights to opt out of sale, sharing and use of certain types of personal information. California Privacy Rights Act (CPRA) requirements provide individuals the right to opt out of sales (included in the California Consumer Privacy Act [CCPA]) and sharing of personal information, as well as use of their sensitive information for targeted advertising. California law also requires organizations to treat user-enabled privacy controls, such as browser plug-ins or privacy settings, as valid requests for opting out.

The costs of noncompliance are high. The California Attorney General's office recently issued a $375,000 fine to DoorDash for selling its California customers' personal information without providing notice or opt-out rights. [2]

Requirements are not limited to California. The Virginia Consumer Data Privacy Act (VCDPA), for example, requires companies to notify individuals when they will be subject to automated decision-making processes and to offer an easily visible, easy-to-use way to opt out (e.g., a link or a button). Similarly, the Colorado Privacy Act (CPA) requires businesses to provide opt-out mechanisms to all consumers and opt-in consent in cases where cookies collect sensitive personal information or children's data.

Top organizations include a section about opt-out rights in their policies as well as an option to opt-out in cookie consent banners. Many companies have also added a "Do Not Track" (DNT) section to their policies, which typically tells customers that they do not respond to DNT signals sent from internet browsers. This makes it even more important for customers to be able to control the use of cookies through opt-out rights.

To do:

- Offer visible, separate buttons or links users can click to opt out of the sale and/or sharing of personal information.
- Work with IT or infosec partners to learn which metadata is collected from user browser settings and to ensure that signals are treated as valid opt-out requests.
- Offer opt-in consent when necessary.
- Consider adding a DNT section to your policy.

3

Contextualized personal information use and collection

The CPRA defines sensitive personal information as:

- Customer financial information (such as debit or credit card numbers)
- Information on individuals' Social Security number or other state identification number
- Geolocation
- Race
- Ethnic origin
- Religious or philosophical beliefs
- Health
- Sex life or sexual orientation
- Labor union affiliation
- Contents of consumers' personal correspondence (unless the business is the intended recipient)

California requires organizations to allow individuals to limit businesses' use of this data solely to provide products and services, so businesses must inform consumers how they are using this information as part of their privacy policy. The state also requires all businesses to publish retention information for different categories of personal or sensitive information they collect, manage, store, share or sell. In instances where retention periods are not fixed, best-in-class organizations share clear principles for how they retain data according to different customer activities or purposes for that data.

In the past few years, top organizations have expanded the categories of personal information they collect and have more explicitly stated how it is being used. For example, Chubb Limited added a "Detailed Use Cases" section to its privacy policy to provide a more comprehensive list of purposes for using personal information, including actuarial analysis, business transfers and compliance with legal obligations. Other companies have added similar policy sections, such as "Manage Your Data," "How to Protect Your Personal Information" and "What Happens if You Don't Give Us Your Data."

Many organizations share information about personal data use and collection by providing lists of the data categories they collect alongside uses for that data without drawing a one-to-one connection between the two. Progressive organizations go a step further, making it easy for consumers to make informed choices by providing contextualized use cases for each category of data.

Sample table for personal information use and collection to include in external privacy policy

Activity type	Data category	Collected	Purpose(s) for collection and processing	Sold (or transferred for valuable consideration)	Transferred for business purposes only
All sales and service transactions	Name and contact information	Yes	[To fulfill contractual and service obligations to our customers, provide service follow-up]	Yes	Yes
All sales and service transactions	Commercial information (purchase history and details of transactions)	Yes	[To fulfill contractual obligations to our consumers, and for our own financial and legal reporting purposes]	No	Yes
All sales and service transactions	Financial information (e.g., credit or debit card, bank account number)	Yes	[To process payments when purchases]	No	Yes
Purchases through our website or app	Website browsing activity	Yes	[To understand how you interact with our website and make improvements, and to detect and prevent fraud]	Yes	Yes
Purchases through our website or app	Location data collected from our mobile app ("geolocation data")	Yes	[To better understand our customer base and to provide tailored services based on your location]	No	Yes
Applications for employment	Name and contact information	Yes	[To fulfill our legal obligations, perform necessary background checks and maintain contact throughout the interview process]	Yes	Yes
Applications for employment	Employment history	Yes	[To perform our employment contract and perform necessary background checks to verify employment eligibility]	No	Yes
Applications for employment	Education history	Yes	[To perform our employment contract and perform necessary background checks to verify employment eligibility]	No	Yes
Applications for employment	Biometric data	Yes	[To perform our employment contract and perform necessary background checks to verify employment eligibility]	No	No

Source: Gartner

To do:

- Provide explicit, detailed information about what personal data you collect, how and why it is being used, and whether and with whom it is being shared.
- Publish general principles around data retention that include whether or not you have fixed or variable retention periods in place, reasons for retention and, when applicable, triggers for disposal.

Gartner®

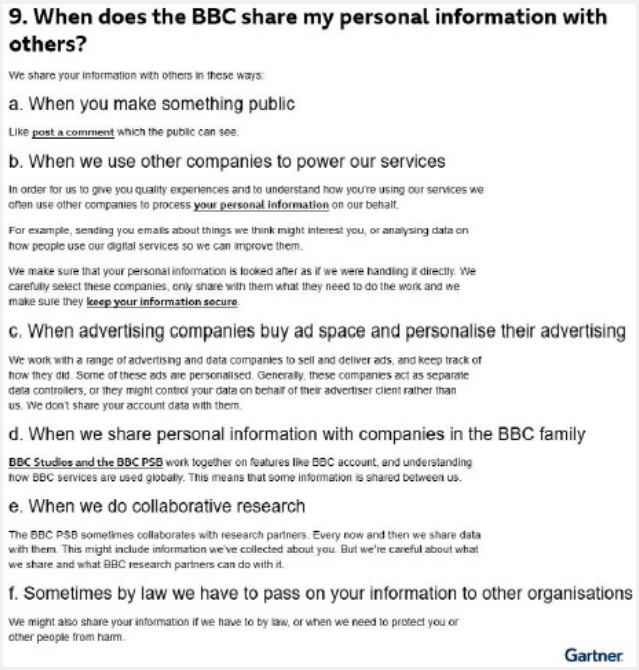
4 Heightened transparency into third-party sharing

Third-party risk management (TPRM) has become increasingly important in recent years as regulatory expectations around sustainability and human rights in supply chains heighten and data breaches become an increasing concern for consumers. Nearly half of all cybersecurity breaches in 2024 involved customer personal identifiable information (PII). [3]

Many privacy laws directly address the concept of sharing consumer data with third parties. For instance, the GDPR mandates that companies establish data processing agreements (DPAs) with third-party vendors that handle personal data for them. Similarly, the CCPA requires organizations to perform due diligence when selecting and working with third parties.

To address third-party sharing, top organizations have updated or added sections to their privacy policies that address how they may disclose personal information to different types of third parties and why they do so. Since 2022, BBC has expanded sections of its privacy policy to account for increased third-party sharing. One section, titled “When does the BBC share my personal information with others?” includes a list of six potential use cases for third-party sharing, along with which types of third-party information would be shared for each situation.

BBC's third-party sharing clause



9. When does the BBC share my personal information with others?

We share your information with others in these ways:

a. When you make something public

Like **post a comment** which the public can see.

b. When we use other companies to power our services

In order for us to give you quality experiences and to understand how you're using our services we often use other companies to process **your personal information** on our behalf.

For example, sending you emails about things we think might interest you, or analysing data on how people use our digital services so we can improve them.

We make sure that your personal information is looked after as if we were handling it directly. We carefully select these companies, only share with them what they need to do the work and we make sure they **keep your information secure**.

c. When advertising companies buy ad space and personalise their advertising

We work with a range of advertising and data companies to sell and deliver ads, and keep track of how they did. Some of these ads are personalised. Generally, these companies act as separate data controllers, or they might control your data on behalf of their advertiser client rather than us. We don't share your account data with them.

d. When we share personal information with companies in the BBC family

BBC Studios and the BBC PSB work together on features like BBC account, and understanding how BBC services are used globally. This means that some information is shared between us.

e. When we do collaborative research

The BBC PSB sometimes collaborates with research partners. Every now and then we share data with them. This might include information we've collected about you. But we're careful about what we share and what BBC research partners can do with it.

f. Sometimes by law we have to pass on your information to other organisations

We might also share your information if we have to by law, or when we need to protect you or other people from harm.

Gartner

Source: BBC

To do:

- Clearly identify and list the types of third parties with whom the organization may share data.
- Describe the specific purposes for which personal data is shared with third parties.

Gartner

5 Integration of AI

Top organizations are proactively aligning their policies to emerging AI regulations, such as the EU AI Act. Officially implemented in August 2024, the EU AI Act is the first comprehensive regulation on AI by a major regulator and requires organizations to establish robust governance frameworks for high-risk AI systems. [4] In the 2024 legislative session, over 45 states, along with Puerto Rico, the Virgin Islands and Washington, D.C., introduced bills related to AI. Out of these, 31 states, Puerto Rico and the Virgin Islands either passed resolutions or enacted new laws. For example, Colorado enacted the Consumer Protection for Artificial Intelligence, which requires developers of high-risk AI systems to use reasonable care to prevent algorithmic discrimination. [5]

AI presents many privacy implications for businesses. In particular, AI systems often require large datasets to function effectively, which can lead to extensive data collection, including personal and sensitive information. AI algorithms are also complex which makes it more difficult for customers and employees alike to understand how data is being processed.

The most progressive privacy policies directly address AI and its influence on the organization. Doing so allows companies to build trust with their customers and demonstrate a commitment to ethical AI and data privacy. While this can be done in a preexisting privacy policy, many organizations, like IBM, have taken it a step further and established separate AI policies. [6]

To do:

- Explicitly outline how AI is used in data processing and decision making at your organization.
- Describe the scope of AI applications, such as whether AI is used for personalization or predictive analytics.
- Provide users with clear options to opt out of AI-driven processes where feasible.
- Inform users about their rights related to AI, such as the right to understand the logic behind AI decisions and the right to contest decisions made by AI systems.

6 Inclusion of notice of changes

Several key privacy laws require organizations to keep their privacy policies updated. For example, the GDPR requires updates when there are changes in data processing or when new data protection rights are introduced. Similarly, Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) calls for updates when there are changes in how personal information is handled or when offering new services.

Fines for incorrectly or illegally changing privacy policies are a real possibility. In 2020, the FTC fined a genetic testing company, 1Health, for retroactively expanding the list of third parties it may share sensitive personal data with, without notifying consumers who had previously shared personal data with the company or obtaining their consent to share such sensitive information. [7]

Benchmarked organizations not only update their policies when necessary but also inform consumers of the changes they make. This can be done through email messages, website pop-ups or just a simple note at the top of the policy with the date of the most recent update.

To do:

- Update your external privacy policy at least once a year, or when a material change, such as a new regulation, technology or security breach, occurs.
- Explicitly state the "date of most recent update" at the top of your policy and/or include a log of changes at the end.
- Send email messages (or app messages, pop-up notices, etc.) to consumers if important changes to your policy are made, such as how the organization uses personal information.

Improved usability and scalability

While companies must ensure compliance with applicable privacy laws, the most progressive companies also focus on making their policies clearer and easier for customers to understand. This approach not only helps customers but also makes it simpler for companies to update their policies regularly. Here are some options to make policies more consumable and scalable.

7

Improved subject rights request portals

Several new U.S. state laws provide customers the right to access, delete and correct their data. Additionally, the CCPA requires organizations to publish subject rights requests (SRR) metrics, including the number of requests received, fulfilled and rejected, as well as the average number of days to fulfill each request type. Best-in-class programs publish these metrics in their privacy notice.

While organizations subject to the GDPR and applicable U.S. state laws must offer customers a way to register a request, progressive organizations use their SRR websites to develop a completely digitized and streamlined way to gather requests from consumers. This includes the standard fields for name, address and telephone number, as well as a CAPTCHA to guard against bots and an option to include proof of identity to eliminate an employee follow-up with the customer for identification.

To do:

- Consider making a case for developing an easy-to-use SRR portal if you're at an organization where many customers request access to their data.
- Link the SRR portal to your policy, as well as on your company website.
- Publish SRR metrics for public consumption.

8 Navigable menus or graphics

While customers and employees are increasingly concerned about how their personal data is used, they are often not interested in all facets of the organization's privacy policy. Eighty-two percent of 2,000 surveyed American adults report that they are somewhat or very concerned about the amount of personal data being collected by businesses. In addition, 75% of respondents are somewhat or very concerned about the increasing use of AI in businesses. [10]

Top organizations make it simpler for consumers to quickly access information they are typically interested in, such as:

- The types of information collected for different customer activities or interactions
- How each type of information is used
- With whom the data is shared and why
- How personal data is secured
- Who to contact in the event of additional questions

Organizations can make privacy policies more navigable by including anchor links to different sections of the policy at the top of the webpage, or by adopting accordion menus to allow readers to expand the portions of the policy they are interested in reading. Some privacy policies incorporate infographics to make the information presented more consumable. Accordion menus, anchor links or graphics are relatively quick and low-cost ways to make navigation of privacy policies easier for your customers, employees or other stakeholders.

CelcomDigi's customer-friendly privacy notice

Source: CelcomDigi

To do:

- Insert anchor links or accordion menus to reference important sections of your policy so clients can easily navigate them.
- Use infographics to present high-level, key information for your policy, such as visualizing data collection, usage or third-party sharing practices.

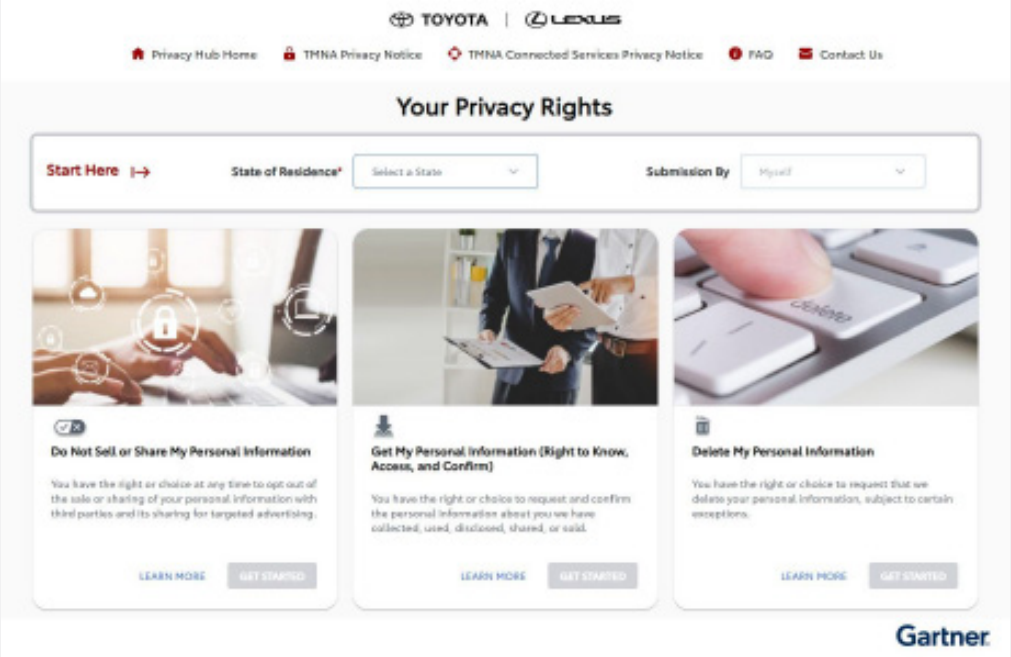
Gartner

9 Advanced privacy portals or hubs

Other companies have taken transparency and navigability a step further by developing portals or centers devoted specifically to customer (and sometimes employee) privacy. These go beyond traditional privacy policies by including resources to educate customers and offer them greater accessibility to their personal data.

Traditionally, privacy portals have been adopted by companies that adopt privacy as a marketing tool or strategic differentiator, such as Apple. However, many other companies have adopted privacy portals or hubs. Toyota's privacy hub provides all-in-one space for consumers where they can input their state of residence and then submit a privacy request in a number of different categories, such as "Get My Personal Information" or "Delete My Personal Information."

Toyota's privacy hub



Source: Toyota

Gartner

Privacy portals or hubs do not only increase transparency. They also offer customers self-service tools and information to help them protect help them protect their own data, emphasize the organization's adherence to privacy principles and reinforce privacy or ethics-related brand messaging. However, privacy portals' development and maintenance make them cost-prohibitive for some. Organizations in need of more extensive privacy portals or hubs are ones that:

- Emphasize privacy as a marketing or strategic differentiator
- Manage large volumes of personal information
- Use personal data management practices that have come under recent scrutiny

To do:

- Ask the IT team or other senior leaders if creating a privacy portal or hub is feasible for your organization.
- Consider making the case for a privacy portal or hub to optimize the user experience if privacy is particularly important to your organization or industry.

10 Regionalized scope of policies

Twenty U.S. states have passed comprehensive consumer privacy laws and 17 more have draft bills in progress. In addition, many geographic regions outside of the U.S., such as Europe, Asia and Brazil, have enacted or updated privacy regulations. As the privacy landscape becomes more complex, adding multiple addenda to privacy policies becomes confusing for users and inefficient for privacy teams. The most progressive companies — particularly those that operate globally — are scaling their efforts by defining a global standard and making changes for certain regions as needed. Consider adopting OvalRevolution's four-part test to distill which regulatory framework to use for the privacy rights you offer to all consumers versus ones that should be offered on a regional basis.

OvalRevolution's four-part test to determine which regulation to set as the global standard

Four-part test to determine which regulation to set as the global standard
Notice provision analysis, illustrative

Management

Consent

Notice

	GAPP	GDPR	CCPA
1 **Adoption:** Does the regulation or guidance address this principle? (Yes/No)	Yes	Yes	Yes
2 **Inclusion:** Is the requirement similar to the requirements in other jurisdictions where we operate? 1 (outlier standard) to 5 (very similar)	3	4	4
3 **Enforcement/clarity:** To date, to what extent has this standard been enforced by relevant authorities? 1 (little) to 5 (significantly) In the absence of clear case law: Is there sufficient guidance to interpret this standard? 1 (unclear) to 5 (clear)	n/a	2	1
4 **Specificity:** How prescriptive is the requirement? GAPP: How well does GAPP cover? 1 (general) to 5 (very specific) 1 (doesn't cover) to 5 (fully covers)	3	5	5
Analysis: Use GDPR format for enterprise notices, include CCPA as needed.	**Minimum**	**11**	**10**

Source: Adapted From OvalRevolution*
* Pseudonym

To do:

- Assess applicable privacy laws in the jurisdictions in which the organization operates.
- Consider the extent of operations, volume of customers and employees, and potential for enforcement in each jurisdiction in deciding whether to offer a distinct privacy policy for that region.
- For each distinct region, assess each element of your policy to derive a regionwide standard for your privacy policy.

Conclusion

Implementing these updates into their external privacy policies allows legal, compliance and privacy leaders to address the evolving regulatory environment, as well as heightened consumer needs for transparency and usability. As these factors continue to shift, leaders should adapt their policies accordingly and keep consumers informed on major changes.

Evidence

This research was conducted using a qualitative analysis of publicly-available privacy policies and company websites.

[1] FTC, ICPEN, GPEN Announce Results of Review of Use of Dark Patterns Affecting Subscription Services, Privacy, Federal Trade Commission.

[2] Attorney General Bonta Announces Settlement With DoorDash, Investigation Finds Company Violated Multiple Consumer Privacy Laws, State of California — Department of Justice — Office of the Attorney General.

[3] Cost of a Data Breach 2024, IBM.

[4] Up-to-Date Developments and Analyses of the EU AI Act, EU Artificial Intelligence Act.

[5] Artificial Intelligence 2024 Legislation, NCSL.

[6] AI Ethics, IBM.

[7] FTC Says Genetic Testing Company 1Health Failed to Protect Privacy and Security of DNA Data and Unfairly Changed its Privacy Policy, Federal Trade Commission.

[8] The Digital Personal Data Protection Bill, 2023, PRS India.

[9] Data Act Enters Into Force: What it Means for You, European Commission.

[10] The Rising Concern for Data Privacy Among American Consumers, USA Today.

Actionable, objective insight

Position your function for success. Explore these additional complimentary resources and tools for legal, risk and compliance leaders:

Webinar

Join a Virtual Event

Hear the latest insight from Gartner experts at an upcoming or recorded event.

Watch Now

Report

Legal and Compliance Risks Report

Future-proof your organization against 12 emerging legal and compliance risks.

Download Now

Research

Develop Privacy Training in a Hybrid Work Environment

Discover best practices to advance your privacy training in a hybrid work environment.

Download Now

How We Help

Gartner for Legal, Risk & Compliance Leaders

Discover how we can help you tackle your mission-critical priorities.

Learn More

Already a client?
Get access to even more resources in your client portal. Log In

Connect With Us

Get actionable, objective insight that drives smarter decisions and stronger performance on your mission-critical priorities. Contact us to become a client:

U.S.: 1 855 811 7593

International: +44 (0) 3330 607 044

Become a Client

Learn more about Gartner for Legal, Risk & Compliance

gartner.com/en/legal-compliance

Stay connected to the latest insight

Gartner®