SurveyMonkey®

Privacy white paper

GDPR COMPLIANT

EU AI ACT COMPLIANT

CCPA COMPLIANT

HIPAA COMPLIANT

Learn more about how we comply—and help you comply—with key global and local regulations

Foreword

When you choose SurveyMonkey, you're entrusting us with one of your most valuable assets— your data. We take this responsibility very seriously. To demonstrate our comprehensive approach to data privacy we've created this white paper that outlines how we comply—and help 260K+ organizations worldwide comply with—key regulations including the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), the European Union's Artificial Intelligence Act (EU AI Act), and other similar regulations.

"At SurveyMonkey, we prioritize privacy and security throughout the entire product lifecycle, from design to delivery, while continuously refining our existing controls. We also ensure our data protection practices remain aligned with industry standards and expectations through ongoing engagement with global customers and by staying up to date on regulatory developments."

Sally-Anne Hinfey,
Vice President, Legal, SurveyMonkey

Our privacy principles

At SurveyMonkey, we build products with privacy embedded by design. Regardless of where you are or which laws apply, we follow a single high standard that combines global privacy laws—so you're always protected by default.

1 We integrate **privacy by design** into every product and process	Every new feature, every new vendor, and every change in the way that we process personal information is reviewed by our internal privacy and security teams through our data protection impact assessment (DPIA) process. Our privacy practices are regularly audited ensuring we meet legal requirements and industry standards.
2 We empower you to **control and protect your data**	Your account administrators can edit, export, or delete any data collected from your customers and employees to honor data subject rights requests. We offer features like anonymous responses that let you limit identifiable respondent information, and our built-in SurveyMonkey Audience panel enables demographic insights without collecting identifying information.
3 We implement **strict data retention policies**	While your account is active, you have full control over what data you keep and for how long. You can delete individual survey responses when needed, and deleted data permanently cycles out of our backups after 90 days.
4 We are **transparent about our data practices**	Our Privacy Notice clearly describes all categories of personal data we collect, our sources, how and when we share it, and our retention periods. Our Data Processing Agreement (DPA) is our contractual commitment to only use your data in specific ways and to comply with applicable data protection laws. It outlines our security controls, breach response procedures, and cross-border data protection measures.
5 We **allow verification** of our practices	We answer comprehensive security questionnaires from prospective Enterprise customers and provide existing customers with all necessary documentation to independently verify our compliance. For additional information on our security infrastructure, explore our Trust Center and the complementary Security white paper.

Privacy regulations and compliance

Learn how we ensure compliance with GDPR, CCPA, EU AI Act, and industry specific regulations.

GDPR compliance

With our international headquarters in Ireland, GDPR compliance is ingrained in our operations and has formed the basis for our entire privacy and data protection strategy. We view the European Union's GDPR (and the UK and Swiss equivalent laws) not merely as a regulatory requirement, but as the cornerstone of our privacy program worldwide. Here's how we ensure GDPR compliance:

We define and honor our responsibilities

- In most cases, we act as your "data processor," and we process personal data only as directed by you and cannot make independent decisions about how to process it beyond technical implementation.
- In a few cases, we act as a "data controller." For example, we are the controller over self-serve account information, billing data, and panelist information.

We only process personal data with valid legal basis

- We will rely on the following legal bases to process personal data: (i) to fulfill a contract (e.g., to provide you with the service); (ii) to comply with legal obligations (e.g., to secure the platform); (iii) for our legitimate interests (e.g., to bring new features to your attention); or (iv) subject to consent from the data subject (e.g., to use cookies to monitor our site usage).
- Where "legitimate interest" is the legal basis, we conduct a legitimate interest assessment (LIA) to ensure that the fundamental rights and freedoms of the data subject are balanced against the business objective, and all risks are remediated as much as possible. Find more information in section 3 of our Privacy Notice.

We implement strong contractual safeguards

- Our Data Processing Addendum (DPA) automatically incorporates EU, UK, and Swiss Standard Contractual Clauses (SCCs).
- We disclose subprocessors with location and security information and allow customers to subscribe to subprocessor list updates.
- We do a rigorous assessment of all third-party vendors.
- All vendor contracts include equivalent protections to maintain compliance throughout our supply chain.

We safeguard international data transfers

- We're certified under the Data Protection Framework (DPF) treaty between the US, EU, UK, and Switzerland.
- Enterprise customers can choose to store their data in the EU, US, or Canada based on their compliance needs.
- We implemented supplementary measures detailed in our Transfer Statement.
- We offer data processing contract terms, specific to data protection and data transfers, for our EU, UK, Swiss, and Australian customers.

We maintain dedicated privacy governance

- We appointed a Data Protection Officer registered with the Irish Data Protection Commission.
- We conduct regular compliance audits and we look for continuous improvement of privacy controls and procedures.
- We run a data stewardship programme to democratize data privacy governance and compliance.

We help you fulfill your data subject rights obligations

- Our platform includes GDPR-friendly features, like Response Manager (available for Enterprise customers), that help you respond to data subject requests easier.
- Upon request, we provide documentation to assist with your controller obligations.

> **“SurveyMonkey checked off two buy-in factors: SurveyMonkey understands GDPR. SurveyMonkey gets Salesforce. That’s huge for us.”**
>
> **Matt Schoolfield,**
> Senior Manager of Commercial Analytics and Voice of the Customer, Greyhound

TRUSTED BY LEADING EUROPEAN ORGANIZATIONS

RYANAIR

DANONE
ONE PLANET. ONE HEALTH

NHS England

CCPA compliance

SurveyMonkey has implemented a robust compliance program that meets California Consumer Privacy Act (CCPA) requirements. Our focus is protecting consumer privacy rights, establishing data governance practices, and ensuring transparent data processing.

We protect consumer rights	We honor California residents' rights to access, delete, and correct their personal information, opt out of targeted advertising, limit sensitive data use, and receive non-discriminatory service.
We safeguard sensitive personal information	We collect only necessary sensitive data (login credentials, email contents, voluntary demographic information) and we use this data solely to provide requested services.
We never sell your data	We don't sell personal information. Even though under CCPA's broad definition, our cookie usage for interest-based advertising qualifies as "sharing," California residents can opt out via our cookie banner or footer link.
We ensure survey privacy	No advertising or third-party cookies are used on survey pages, protecting respondent privacy.
We commit to transparency	We maintain clear privacy notices, including region-specific information for California residents, and we provide notice of financial incentives for our panelist programs.
We enforce data protection	We implement de-identification practices and extend CCPA obligations to vendors through contractual commitments.

TRUSTED BY LEADING CALIFORNIAN ORGANIZATIONS

cisco box upwork salesforce wrike

EU AI Act compliance

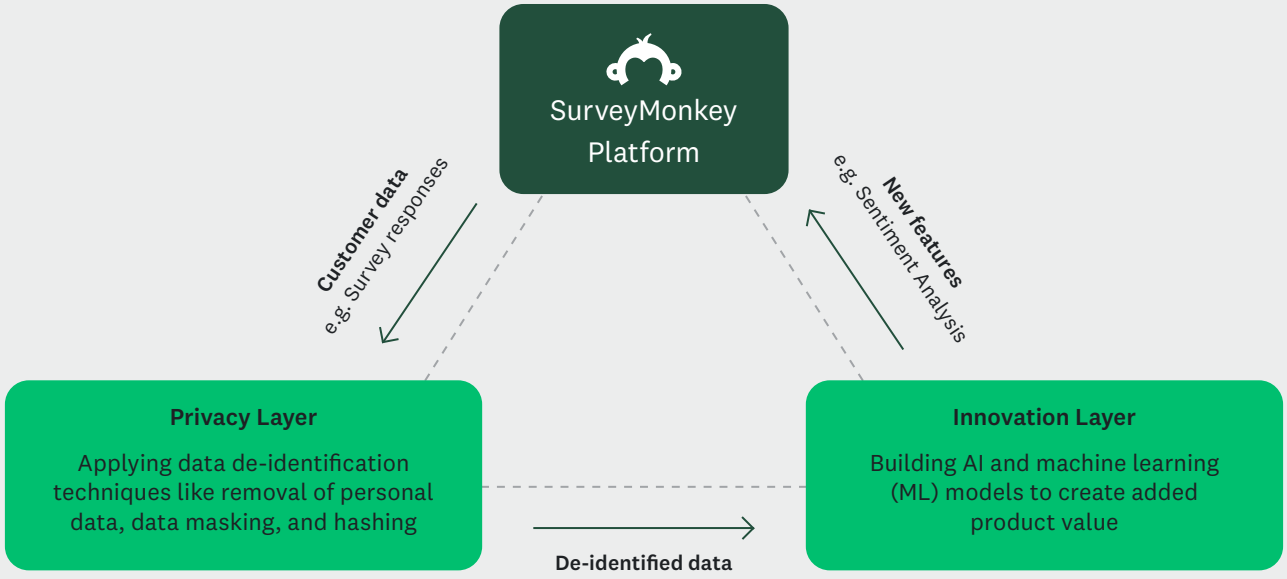
The EU AI Act (effective August 1, 2024 and with full implementation in 2026) marks the world's first comprehensive AI regulation. SurveyMonkey is implementing compliance measures early, treating this European legislation as a global standard—similar to our GDPR approach—to provide all customers the highest protection regardless of location.

We adhere to a risk-based approach	All of our AI and machine learning (ML) product features present minimal or no risk.
We govern AI responsibly	We are guided by the following core principles when developing and reviewing AI projects: interpretability, reliability, accountability, data privacy, compliance, human agency, security, and fairness.
We implement organizational controls	We've established a Working Group for AI with representatives from privacy, product, security, IT, engineering, AI/ML, data science teams to review AI risk for all new vendors and projects.
We prioritize training and expertise	We offer AI training to all staff members, and representatives of our AI Working Group have obtained the IAPP Artificial Intelligence Governance Professional certificate.
We ensure ethical product development	Our diverse machine learning leadership team adopts an ethical and inclusive approach to AI research and product development.

We protect data privacy

We use de-identified customer data or synthetically generated data to train our proprietary AI models, employing a privacy-by-design approach with strict data minimization, retention limitations, and access controls.

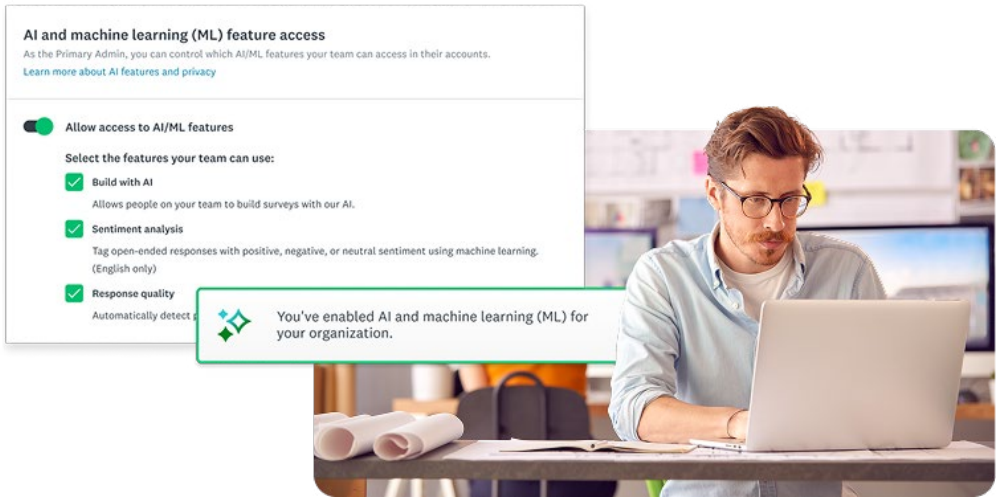
How SurveyMonkey innovates with AI while protecting customer data



Key privacy and security controls: TLS data encrypted at rest | Least priviledged access | Short retention policy

We maintain transparency

We clearly communicate our AI-powered features on our website and announce new AI features on our What's new page.



Admins on Team and Enterprise plans can manage AI feature access for several AI-powered features.

Industry-specific considerations

Industry	Healthcare	Education	Finance
Regulation	**HIPAA**	**FERPA**	**DORA**
How SurveyMonkey complies	We offer HIPAA-compliant features as an add-on to help you meet your compliance needs. This add-on is only available to SurveyMonkey Enterprise customers. Learn more about HIPAA compliance at SurveyMonkey, including how to sign a Business Associate Agreement with us.	SurveyMonkey can be designated a "school official with legitimate educational interests" under FERPA to ensure FERPA-subject customers in the third-level/ university sectors comply with their legal obligations (subject to our Acceptable Use policy and terms as regards data collection from minors). When collecting student information through SurveyMonkey Apply and other products, you can be confident that we maintain administrative, physical, and technical safeguards to prevent unauthorized access to confidential student data.	We offer DORA-compliant features through our Terms of Use for self-serve customers and more comprehensive protections in our Governing Services Agreement for Enterprise customers. Our compliance includes termination rights, audit processes, clear documentation, transparent subprocessor management, strong data protection measures, and regulatory cooperation commitments.

Carrot collects valuable HIPAA-compliant data

"We're able to demonstrate, through surveys, that we are positively impacting our members' decision-making processes and easing their burden as they face complex, life-changing moments."

carrot

Laura Lee,
Product Manager, Carrot

McKESSON · University of Notre Dame · Wellstar Health System · Abbott · NHS England · athenahealth · Tufts Medicine Tufts Medical Center

For additional information on our security infrastructure, explore our Trust Center and the complementary Security white paper.

Unlock insights—and comply with data privacy regulations—with SurveyMonkey Enterprise

We offer flexible plans and pricing to fit your needs, including robust features that support compliance with global privacy regulations.

Explore SurveyMonkey Enterprise or contact sales to learn more about how we can support your specific compliance requirements.

Get started