



SurveyMonkey and GDPR

How we're helping our customers stay compliant

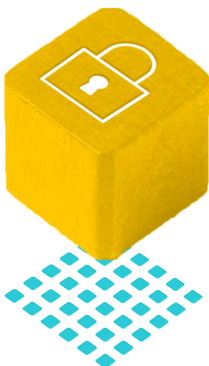


GDPR

The General Data Protection Regulation (GDPR) took effect on May 25, 2018. It addresses the vast changes which have taken place in the tech arena over the past two decades and seeks to harmonise the approach to data protection matters across Europe by establishing a single set of pan-European rules.

It replaces the Data Protection Directive which has been law across the European Union for the past 20 years. At SurveyMonkey, we don't see GDPR as just a legal obligation or another compliance box to tick. Rather, we're excited to help our customers understand how we're approaching this change. GDPR When the European Data Protection Directive was introduced in 1995, the law makers were addressing the risks posed to personal data that existed during the formation and early years of the Internet. In order to ensure that the protection of personal data remains a fundamental right for EU citizens the aim of GDPR is to modernise outdated, and unfit for purpose privacy laws.

Why is GDPR so important?



The impact of GDPR is significant as it affects any business that collects data in Europe (whether they are based in Europe or not). It has effectively introduced the first global privacy standard. GDPR puts a greater weight of responsibility on individuals and organisations whose businesses involve the collection of personal data, and requires those businesses to give individuals greater visibility into, and control over the data they provide to those businesses. GDPR also provides greater protections for EU citizen data by imposing strict obligations on data handling, while making businesses more accountable for how they handle data. Very significant fines of up to €20,000,000 or 4% of global annual turnover, whichever is greater, may be levied on organisations who fail to meet their obligations with respect to handling data under GDPR.

What SurveyMonkey has done



With 98% of the Fortune 500 using our platform, we've always been keenly aware of the importance our customers place on privacy and security. As a global organisation, we have been operating in the EU for a number of years, with our international headquarters based in Dublin, Ireland. Making continual adjustments and improvements to ensure we are best positioned to meet our legal obligations, and to assist our customers to do likewise is an integral part of how we operate on a daily basis. Our customer relationships along with the trust they place in us, are at the very heart of our business, and are never taken for granted. We see GDPR as affording us yet another opportunity to continue our legacy of protecting customer data. Outlined in this white paper are some specific aspects of our approach to GDPR.

Security

As SurveyMonkey continues to make the security of data entrusted to us a priority, and in light of GDPR, we have included more detail on the specific measures we have in place in our customer-facing [Security Statement](#). Some highlights include the following:

- Access Control (Authentication and Authorization)
- Single-Sign On support
- Data Encryption at rest and in transit
- SOC 2 accredited Data Centers
- Continuous Network and Security Monitoring
- Vulnerability Management
- Incident Response and Recovery
- Security Awareness Training
- Periodic Independent 3rd Party security reviews and penetration testing
- EU-US Privacy Shield Certified
- PCI DSS and HIPAA Compliant
- Multiple data centers to guarantee a secure and highly available service at scale
- Select group of trusted security partners, to ensure our customers are always protected with the best-in-class security

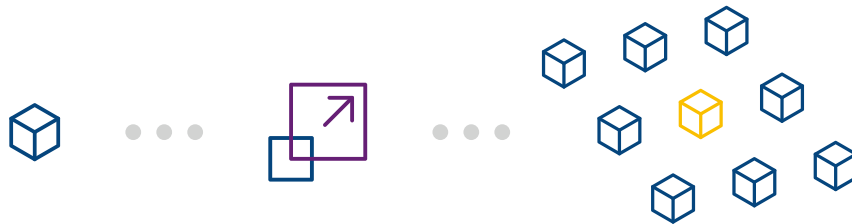
Our Security team has drafted a Security White Paper containing more granular detail for our SurveyMonkey Enterprise customers. Please [contact us](#) if you would like to receive a copy. We're also hoping to secure ISO 27001 certification as part of our security program for certain aspects of our business and will be providing updates as this progresses.

Security incidents

Despite best practises and security standards, no service on the internet is impervious to risk of security incidents. However, we have detailed security incident policies and procedures in place and frequently review these procedures. We are committed to keeping our customers fully informed of any matters relevant to the security of their account and to providing customers with all the information necessary for them to meet their own regulatory reporting obligations under GDPR. SurveyMonkey Enterprise customers can also monitor and understand user activity across their account such as usage, activity, surveys deployed, the number of responses collected, and more.

Privacy basics

SurveyMonkey, founded in 1999, initially served consumers by way of a survey tool, utilising a freemium model. We have since evolved into a trusted enterprise platform with over three million customers using our services daily. We updated our [Privacy Policy](#) to reflect this and to address the evolving needs of our all our customers, both self serve and Enterprise. Transparency and accuracy are our key drivers in making these changes, and we believe the more succinct and easily navigable policy which applies to all our services, will be useful to our customers.



International data transfers

Personal data can only be transferred outside of the EU to countries where the European Commission determines there is “an adequate level of protection” in place. There are currently 11 countries deemed by the European Commission to provide “an adequate level of protection”. For transfers of data to all other countries, we are happy to offer most customers our Data Processing Addendum, incorporating the EU Commission-approved Standard Contractual Clauses, in order to meet their legal obligations for the transfer of data from the EU to all countries not covered by an EU Commission adequacy finding. In addition, we are also [Privacy Shield](#) certified. For more information and to access our DPA (which includes GDPR and SCC clauses), visit our [Help Center](#).

International data centre

In addition to the initiatives highlighted above, we are aware that many of our customers with EU users and EU affiliates would prefer that their data be hosted in the EU, notwithstanding the methods for lawful data transfer that we provide.

Updates to legal terms

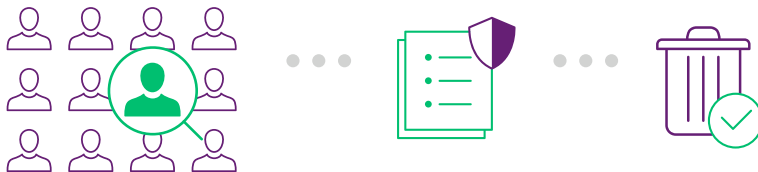
In addition to the changes to our Privacy Policy, we have made changes to our customer-facing legal terms (e.g. Master Services Agreement and Data Processing Addendum and our website terms of use) to include GDPR clauses.

Data minimisation and accuracy of your data

Privacy by design and privacy by default are an intrinsic part of our product planning and development. One example of how we can help customers address their obligations under GDPR while using SurveyMonkey is through the admin control panel. Through the control panel your account administrator can edit, export, or delete any data collected from your customers and employees. For more information, see our [GDPR Help Center article](#).

Data retention

We have company-wide data retention policies. Furthermore, we empower our customers to control their data through their account. As long as your account is active, you have full control over the specific types of data, and length of time you hold such data. For example, you can delete a single individual survey response from your account if required to do so, as long as you can identify the correct respondent. These features are readily accessible to all of our customers. We honour all deletions from an account, and after a short period of time (90 days), all account data which has been expunged by you is permanently deleted from our back-ups. The intention is to reduce this deletion period to 25 days and when this is done we will be updating our [customer-facing information on retention periods](#).



Our employee training program

We pride ourselves on the exceptional completion rate for our employee GDPR training program. Our program is designed to ensure all employees across all functions within the company understand the obligations on SurveyMonkey and on our customers under GDPR. In addition to the general training program we continually run privacy and security education programs internally for different functions across our organization. Data is our business so we work hard to ensure our employees are educated on best practices around treatment of data.

Data Protection Officer

We have appointed a Data Protection Officer and they are responsible for all matters related to GDPR. The DPO can be contacted through dpo@surveymonkey.com.

Sub-processors

No SaaS provider is fully self-sufficient and so use of trusted third parties is essential to maintain our business. If you are located in the EU, we provide a list of sub-processors who assist SurveyMonkey in the provision of the services. In order to obtain this list, please [contact us](#).

SurveyMonkey - a tool for tracking compliance

SurveyMonkey is happy to offer a new [Quiz Template](#) to help companies measure their compliance with GDPR. This template is available for SurveyMonkey customers to download and utilize within or outside of their organisations.

How can SurveyMonkey help you unlock the value of your data?

Looking for an enterprise plan for your team, or want to consolidate SurveyMonkey usage across your entire organization? We offer flexible plans and pricing to fit your needs.

[Contact us to learn more](#)

Learn more about [SurveyMonkey and GDPR](#).

For questions regarding SurveyMonkey and GDPR,
please contact: privacy@surveymonkey.com

Disclaimer: We hope you find this white paper useful but please be aware that this information is not to be construed as legal advice or representative of our interpretation of privacy laws, but instead is intended to help our customers understand our approach to GDPR in practical terms. If you are in doubt as to your legal obligations or require advice on any of the areas covered, we urge you to seek independent legal counsel.