onetrust

Contracting with OneTrust®

Our goal is to provide an overview of what your company is purchasing from OneTrust, in order to support your review of the OneTrust Master Terms of Service ("**Master Terms**") and associated documents such as the OneTrust Data Processing Addendum ("**DPA**"). We also aim to highlight certain key provisions and principles in the Master Terms along with OneTrust's approach to privacy and security. This content is provided for informational purposes only and is not part of any contract.

OneTrust Master Terms

Why should customers use OneTrust's Master Terms?

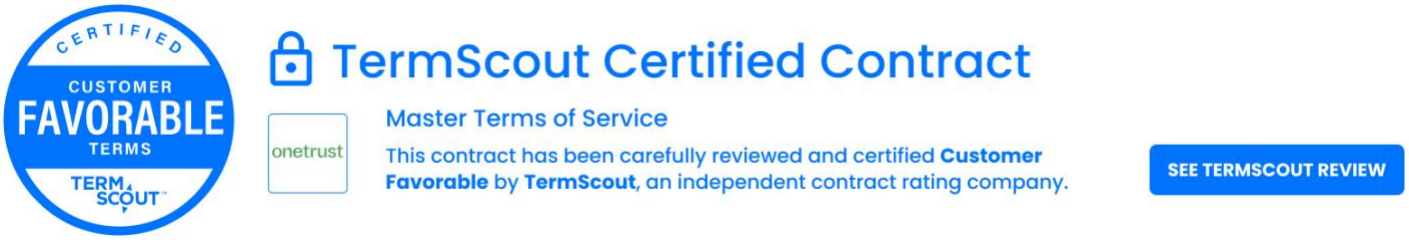
The Master Terms reflect the one-to-many delivery model of the OneTrust services, meaning our services, operations, and controls are the same across our entire customer base. This directly translates into the efficiencies and value we pass on to our customers.

We take great care to include industry-standard protections in the Master Terms which are mutually beneficial to customers and OneTrust. We conduct regular benchmarking of the industry and our competitors to anticipate changes in our offerings, industry, and data protection regulations with an eye towards maintaining a customer-friendly and compliant approach to contracting.

The Master Terms are tailored specifically to OneTrust services and our business model. Customer purchasing templates are typically much broader and generic in scope, and therefore require substantial investments of time by all parties through multiple rounds of negotiations and exchanges of redlines to align the template to reflect OneTrust's services and business model.

In our experience, using the Master Terms increases the speed (by over 300%) at which customers can conclude the contract review process and move on to implementation of our services, while ensuring a reasonable allocation of risk.

But don't just take our word for it — the OneTrust Master Terms have been independently assessed and certified by TermScout.



onetrust

OneTrust's Master Terms are TermScout Certified™ – what does that mean?

TermScout is a contract review platform that enables customers to gain insights into contracts.

Using a combination of artificial intelligence and experienced legal professionals, TermScout analyzed over 750 data points in the Master Terms and benchmarked the terms against more than 1,500 similar vendor contracts.

After an extensive quality control review from a committee of human experts, the Master Terms received a rating of 70% Customer Favorable! In addition, we were given a 100% score against "Buy-side Deal Breakers," meaning the Master Terms don't contain any egregious terms (such as complete disclaimers on liability) that should deter customers from signing them. The Master Terms comply with 75% of the World Commerce & Contracting Principles and was assessed to have a "High Clarity" of contract language.

What am I purchasing from OneTrust?

Cloud Services Subscription. OneTrust offers a pre-built software-as-a-service platform with subscriptions that enable customers to access services through the platform. OneTrust provides access to its cloud services on a shared architecture, codebase, and infrastructure for each customer to utilize for its internal business and compliance purposes. This operating model does not allow OneTrust to provide customized cloud services or software development services. However, the cloud services do feature customer-controlled configurations allowing customers to make implementation decisions based on their own regulatory needs, industry, data, and use cases.

Intellectual Property. Customers retain ownership of all data and information they input into the OneTrust cloud services. OneTrust does not create works made for hire, develop software or code, or provide any other custom work for customers.

Hosting Options. The data our customers use in connection with the could services is stored in a logically-separated cloud database. Customers can choose from various geographic hosting locations for their tenant environment. OneTrust also offers HIPAA and PCI-compliant environments for customers with specialized requirements.

Updates. OneTrust periodically issues new releases for the cloud services, including updates, features, fixes, or patches at no additional charge. Updates are automatically available in the customer's tenant environment with notice.

Components. Some of OneTrust's cloud services (for example, Cookie Consent or Data Discovery) are provided with a component requiring implementation on the customer's system or websites, such as object code software or scripts. Customers are provided with a license to use such components in furtherance of their use of the cloud services.

Production and Non-Production Environments. Customers receive a single production tenant environment in which all of the subscribed cloud services are made available. Some subscriptions also include a non-production environment to enable customers to explore features, functionality, and configurations (without inputting production data). Customers may also purchase additional production and non-production environments.

onetrust

Professional Services. OneTrust provides implementation and training services to onboard customers. Each new cloud services subscription includes self-service onboarding. Customers may also purchase additional professional services from a catalog of services tailored to accommodate specific needs, including guided onboarding or in some cases custom services. The professional services are documented in statements of work created by OneTrust.

Support. OneTrust offers various Success Package tiers designed to improve use of the cloud services through support, engagement, and guidance. The Success Package tiers and scope are detailed in the Support Description. As we continue to develop our Success Packages, we may update our Support Description from time to time (while committing to you that the level of Support will not materially degrade during the subscription term).

Can I modify the standard statement of work, Support Description or User Guide?

Due to our business model, we cannot agree to modifications to these documents as we offer standardized packages across our entire customer base. If your company has additional needs in respect of professional services, we may be able to offer a custom statement of work.

What commitment does OneTrust give in relation to the performance of the Services?

We warrant the cloud services will conform to the OneTrust User Guide, that our professional services will be performed as set forth in the applicable statement of work and that our support services will be performed in accordance with the Support Description.

How is liability allocated in the Master Terms?

OneTrust is committed to being a long-term partner to our customers. This means that we fairly allocate risk in our contractual agreements, but we unable to underwrite risks that could threaten the financial viability of our company. Specifically, the Master Terms provide for a cap on each party's liability equal to the total annual fees paid or payable by the customer in the preceding year. This sets OneTrust above most SaaS vendors who typically offer a lower cap linked to the fees for the applicable services in the previous year (rather than the fees for all services in the preceding year). Certain categories of claims such as those arising out of wilful misconduct and intellectual property rights are excluded from the liability cap, meaning in the event those claims arise, liability would be unlimited.

Does OneTrust offer unlimited liability for data breaches?

OneTrust does not agree to uncapped liability for unauthorized disclosure of customer data or for breaches of security, privacy, or confidentiality obligations. Our corporate governance requires the need for proportionality between our liability for data breaches and the annual contract value as a fundamental principle of our business model. While we are not an insurer in a position to accept that our customers outsource the risk of a data breach to us, we are strongly committed to complying with our security and privacy obligations, which are defined by

reference to the mature security and privacy program implemented by OneTrust. This approach will allow OneTrust to continue to act as a long-term and sustainable partner for all of our customers.

What indemnities does OneTrust offer?

OneTrust indemnifies customers for certain third-party IP infringement claims resulting from use of the cloud services. Because such claims are likely to affect many of our customers, we require the right to control the defence and related settlement of such claims in order to allow OneTrust to act consistently and efficiently.

Does OneTrust offer Acceptance Testing?

Because cloud services are offered on a single code base for all customers, and because OneTrust does not perform custom development, there is no need for acceptance testing. Instead, we offer in-depth demos and trials for customers to become familiar with our services before purchasing a subscription. Once a customer makes a purchase, OneTrust warrants that the cloud services will materially conform to the User Guide throughout the subscription term.

Can Customers terminate for convenience?

OneTrust does not agree to termination for convenience in its contracts. Our pricing is conditional upon both parties being committed to the full subscription term.

Security, Data Processing, and the DPA

How is the use of personal data protected and governed?

OneTrust aligns its data protection controls with applicable privacy regulations such as the CCPA (and other U.S. privacy laws), EU GDPR, Swiss FADP, and UK GDPR and industry standards. The Master Terms incorporate the OneTrust DPA. The DPA lays down OneTrust's obligations as a processor to customers as controllers (or equivalent designations under applicable data protection and privacy laws). The DPA is aligned with OneTrust's one-to-many business model, detailing the company's privacy policies and security controls. OneTrust will only process personal data for the limited purposes described in the Agreement and will not buy or sell customer personal data. Customer's users control access to the cloud services, as well as the volume and types of data submitted to the services.

Do we need to provide personal data to use the Services?

OneTrust processes personal data of customer's users accessing or interacting with the services in order to provide the cloud services. The personal data needed to use the services is limited to the categories of data specified in the DPA. OneTrust does not have specific access to the data customer' chooses to submit to the cloud services. Most of the services we offer are customizable as to the personal data that is captured and

stored beyond identification data (such as name, email, or IP address). Some services include built-in functionalities for data minimization (for example, auto-deletion and retention periods) and OneTrust encourages its customers to configure the services to reduce the amount of personal data stored in the OneTrust environment at any given point.

Does OneTrust use subprocessors?

OneTrust engages subprocessors to aid in delivery of the cloud services. Each subprocessor has an obligation to protect customer's personal data consistent with the standards required by applicable data protection law. The list of OneTrust subprocessors is maintained on the Subprocessor Page. Updates to the subprocessors list are made available to customers at least thirty days in advance (except in an emergency). If a customer does not approve of a change to the list based on reasonable data protection grounds, OneTrust may provide an alternative provider or allow termination of the impacted subscriptions.

How does OneTrust protect my data when transferring it across borders?

For transfers of EU, Swiss, or UK-protected data, OneTrust relies on the applicable adequacy decisions (including through participation in the Data Privacy Framework) issued by the competent authorities or, in their absence, standard contractual clauses and other supplementary measures, as required under applicable data protection and privacy law. OneTrust has self-certified its adherence to the Data Privacy Framework. For data transfers from other countries imposing data transfer restrictions OneTrust will cooperate with customer to enable the valid transfer of personal data.

How does OneTrust respond to data breaches?

OneTrust notifies customers of loss, alteration, unauthorised disclosure of, or access to customer data without undue delay in accordance with applicable data protection laws. In addition to taking actions necessary to mitigate the effects of a breach, we keep customers informed of material developments in connection with the breach. OneTrust will also cooperate with customers and provide reasonable information so customers may fulfil reporting obligations required by applicable data protection and privacy law.

How does OneTrust handle requests from government and law enforcement agencies?

OneTrust does not voluntarily disclose or grant access to any personal data of our customers to government authorities unless required by law. OneTrust's policy on dealing with government or law enforcement requests for data and our transparency report related to such requests are found in the Transparency Report.

What is OneTrust's approach to the security of customer data?

OneTrust places great importance on maintaining the security of customer data. OneTrust LLC has obtained ISO 27001, ISO 27017, and ISO 27701 certifications for its privacy and security programs. OneTrust also

undergoes an annual independent SOC 2 Type II audit. Further, all data input into a customer's environment is encrypted both at rest and in storage with AES-256 and backups are stored encrypted with Azure Transparent Data Encryption AES-256, while a minimum of TLS 1.2 is used for data in motion. OneTrust's data security obligations are detailed in Appendix 1 (Information Security Controls) of the DPA. More information on our security controls can be found on the Trust Page.

Can OneTrust attach a customer's form data processing or security annexes to the Master Terms?

No, as OneTrust operates a shared security and privacy model for all customers which requires standardization of operations, it is not feasible to agree to customized security and privacy requirements. However, we continuously update our security controls in line with industry standards.

Does the customer retain ownership of its data?

Yes. Customer retains ownership of the data it inputs into the cloud services.

Can customers audit OneTrust?

Yes. OneTrust provides customers with the information reasonably necessary to demonstrate its compliance with its obligations in the DPA. Where additional review is needed to ascertain OneTrust's compliance with the DPA, OneTrust will, upon a customer's request (for a reasonable fee), submit to a review of applicable procedures and documentation. OneTrust will also partner with customers to make available relevant information in response to a request by a competent supervisory authority.

How can a customer get its data back if the contract ends?

Customers can elect to delete or export a copy of their data (in a structured, commonly used and machine-readable format) at any point during the subscription term and for up to 60 days following termination. After such time has passed, OneTrust will delete all data remaining in the cloud services in accordance with its destruction policy.

Does OneTrust use Artificial Intelligence in the services?

Yes. OneTrust's policy on use of AI is detailed in our AI Systems Transparency Report which is available upon request.