Trustpilot

Version 2.7
March 2022

Security Whitepaper

Security Practices for Trustpilot Review Invitation Services

Contents

1. Purpose of this document

We're committed to safeguarding our platform and protecting personal data belonging to our customers, reviewers and consumers.

The purpose of this document is to provide companies with an overview of our security and privacy practices. In line with that, we refer to companies who use Trustpilot in this document as "you" and "your".

We make this document publicly available by publishing it on our website and we share it with all of our employees (including our temporary workers and contractors), and our vendors.

Reviews of this document and our information security framework are completed at least annually by our Chief Information Security Officer (CISO) and are approved by our Chief Information Officer/Chief Technology and Product Officer (CIO/CTPO).

1.1. Our business

We operate an open online review community where consumers can share their buying and service experiences to help others make informed decisions when shopping online and at the same time help businesses learn from their customers.

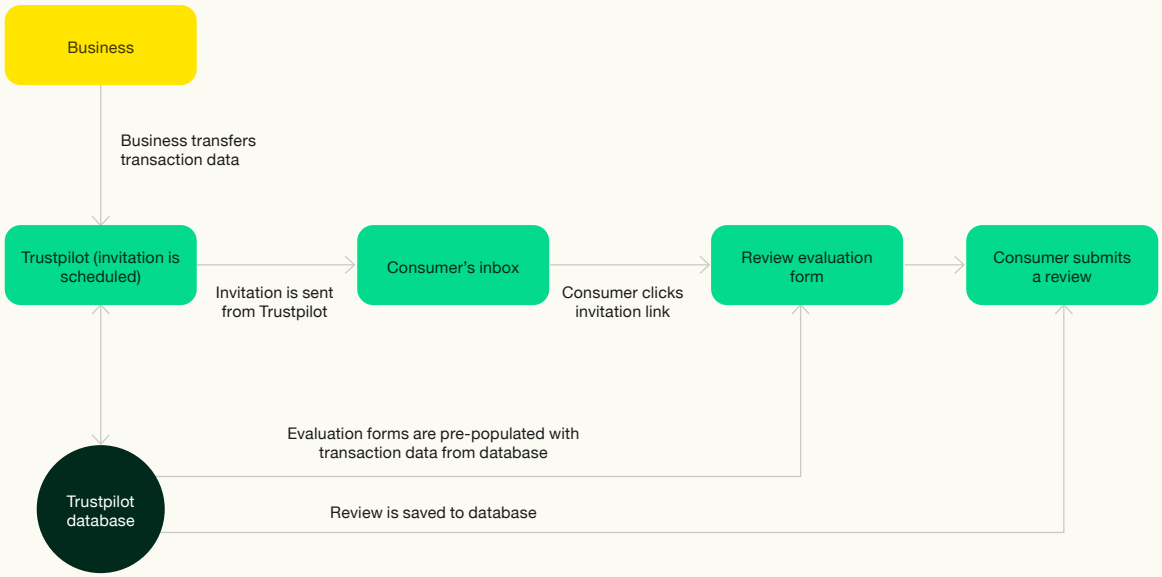
Our review community is available to the public, and the services that facilitate consumer-business dialogue are free. We give consumers a voice by letting them publish genuine reviews about their experiences instantly, without moderation, and for free. Businesses can choose between Trustpilot's free or paid services, both of which let them reply to reviews and engage in open conversations with their customers.

Trustpilot displays reviews for each company using a company profile that aggregates reviews and generates a star rating and TrustScore for each reviewed company.

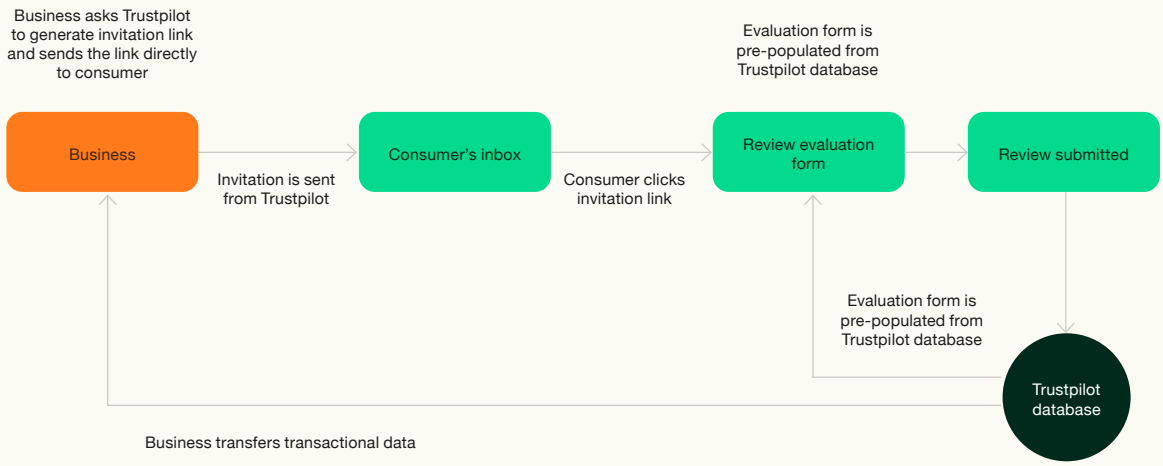
1.2. Our review invitation services

Our review invitation services include the sending of emails to consumers on behalf of businesses, where those emails invite consumers to leave a review on Trustpilot. There are several ways to send review invitations to consumers:

1.2.1. We send out review invitations to your customers on your company's behalf through our email delivery service. For us to create and send the emails, we need you to share personal data about your customers with us.

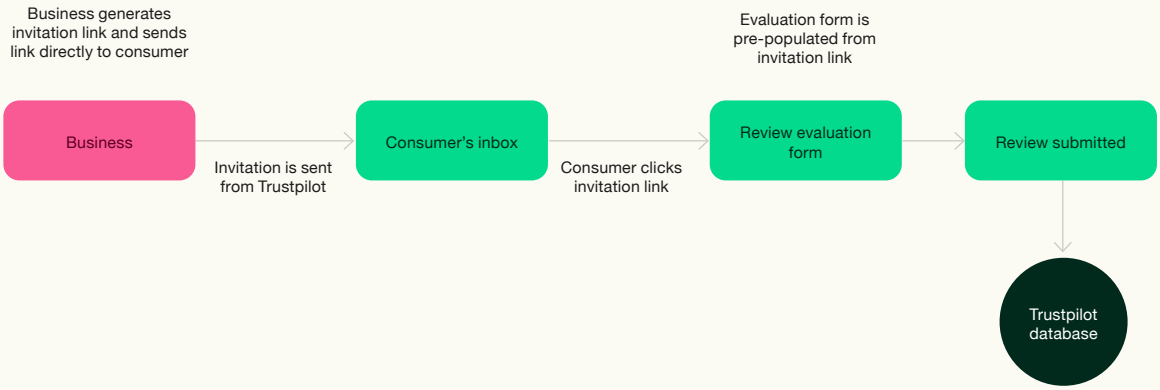


1.2.2. Your company uses your own email delivery service to send review invitations to your customers to write reviews on Trustpilot, where you use our services to generate the invitation link. For us to generate the invitation link, we need you to share personal data about your customers with us.



1.2.3.

Your company uses your own email delivery service to send review invitations to your customers to write reviews on Trustpilot, where you generate the invitation link yourself. This requires your company to share personal data about your customers with Trustpilot, but the processing activity only involves decrypting the payload on our server and prepopulating review form with your customer's name - Trustpilot doesn't store any personal data shared with us while this review invitation method is used.



Our Support Center describes the different review invitation services that we offer and the data processing activities associated with each invitation service.

1.3.

Trustpilot as a data processor

When you share personal data about your customers with us, we act as a data processor and your company acts as a data controller, as defined in the EU's **General Data Protection Regulation (GDPR)**. Both Trustpilot and your company must comply with the GDPR.

The terms "data processor" and "data controller" are defined in Article 28 of the GDPR, and require the data controller and data processor to put in place a "data processing agreement" that describes the data processing activities being carried out.

We've therefore created a data processing agreement (DPA) that meets the requirements outlined in the GDPR and implemented it into all of Trustpilot's customer agreements.

You can find a copy of our data processing agreement on our website. We recommend that you keep a copy of this agreement on file in case you need to show that you comply with Article 28 of the GDPR.

If you want to request a signed copy of the DPA, please send the following information to us at privacy@trustpilot.com:

- The official name of your company
- Your company's address (number, street, city, postal code and country)
- Your company registration number
- The name, title and email of the person who will be signing the DPA on behalf of your company.

2. Information security organization

At Trustpilot, we continuously improve our information security.

As required by the GDPR, we have appointed a Data Protection Officer (DPO) to oversee our data privacy and protection measures.

We also have appointed a CISO, who is responsible for our overall information security practices and makes sure industry best practices are applied.

Staff responsible for Information Security include our Information security team, led by our CISO, and we also engage external resources and experts where appropriate.

2.1. Our security team

We have a dedicated and highly skilled security team who govern our systems and controls, and focus on securing our products and processes.

Our CISO is responsible for Information Security within Trustpilot. Working together with our DPO, CTO, and our VP of Corporate IT, the Team ensures our security practices remain up to date and compliant.

2.2. Programs to improve security

Trustpilot runs a public bug bounty program that we use to continuously improve the security of our systems, increase awareness of our security level and practices, and improve the scope of areas scanned for security vulnerabilities (our “scan vector”).

We openly engage security researchers to challenge our systems, identify and report any vulnerabilities to us so that we can address them.

3. Information security framework

We have security policies and documents that form the basis of our information security framework. Our CISO, CTO, and VP of Corporate IT review these policies on an annual basis.

These policies are complemented by contractual obligations that apply to everyone we work with, and the processes, education and training that we use ensure our employees are also aware of our information security practices.

3.1. Information Security Policy

Our Information Security Policy aims to protect the data that belongs to our users, customers, employees and our business.

We align with current international regulatory and industry best-practice guidance, and we've designed our security program around best-of-breed guidelines for cloud security. In particular, we make use of bodies like the Cloud Security Alliance, and we align our practices with ISO 27001.

You can request a copy of our Information Security Policy by emailing privacy@trustpilot.com.

3.2. Data Incident Policy

In the unlikely event of a data incident, we have a documented policy and firm processes to guide our actions, as well as a dedicated Data Incident Response Team to handle the incident.

Our Data Incident Policy outlines how we should document, investigate and report potential data incidents. In the case of an information security incident, we will contact companies whose personal data is affected.

You can request a copy of our Data Incident Policy by emailing privacy@trustpilot.com.

The Data Incident Response Team will send an alert to all email addresses that the affected companies have registered with Trustpilot via their business account. Companies can also email privacy@trustpilot.com to opt in additional email addresses for such alerts.

3.3 **Business Continuity Policy**

We have a Business Continuity Policy in place to ensure the continuity and timely recovery of critical business processes and systems in the event of a disaster, and to ensure that our critical processes operate at an appropriate level.

Our overall approach to business continuity involves ensuring that all our systems are Software as a Service ("SaaS"), so in the event of a disaster, all Trustpilot employees can work remotely. Our continuity and recovery plans are based on a business impact analysis that we review on an annual basis, at minimum.

We design our products to be highly available, fault-tolerant and fault-resilient. To achieve this, we follow industry best practices which we continuously improve on and review. We use active-active/active-passive database modes, and actively replicate data and services between availability zones at Amazon Web Services in Europe and Google Cloud Services in Europe to minimize the recovery time of our services, among other things.

Continuity is technically tested every time we have a major incident or production-impacting event. Further details of our Business Continuity Policy are confidential.

Contractual obligations

3.4 As a customer, your use of our services is governed by Terms of Use and Sale for Businesses ("Terms").

The Terms set out the rights and obligations for you and Trustpilot, including our obligation to keep your data confidential.

3.4.1. **Code of Ethics and anti-bribery**

We expect those who use our platform or do business with us, including our customers, to make decisions that reflect strong ethics and are consistent with Trustpilot's values. We therefore require our employees, customers, suppliers, and business partners to adhere to the principles set out in our Code of Ethics, available on our website.

As set out in our Code of Ethics, we're committed to maintaining a high ethical standard, and we require that our employees, customers, and business partners comply with all the relevant anti-corruption laws of the countries that we do business in. This includes the US Foreign Corrupt Practices Act (FCPA) and the United Kingdom Bribery Act of 2010.

3.5. **Human resources & information security**

All of our employees need to know what they can and can't do when handling confidential information and personal data. In addition to their obligation to follow our Code of Ethics, employees must observe strict confidentiality with regards to Trustpilot's affairs. This requirement is included in all of Trustpilot's employment contracts.

The obligation of confidentiality includes not only Trustpilot's activities, but also extends to relationships with businesses and customers. It continues to apply after termination of the employment contract.

If an employee breaches their confidentiality obligations, intentionally or negligently, we consider it a material breach of their employment contract that can result in disciplinary action including termination or immediate dismissal.

3.5.1. **Hiring**

As part of our recruitment process for hiring new employees at Trustpilot, we conduct background and reference checks, however as a default, we do not perform any criminal or credit checks for non-US hires. We conduct criminal checks against our US hires

3.5.2. Training

Our new employees go through a new hire training program that includes education and training about how to protect and handle information at Trustpilot. New hires learn about Trustpilot's commitment to information security and our requirements for protecting and safeguarding information.

We also have an eLearning program that trains and tests newly hired employees in our Code of Ethics. We include modules on data security and data privacy awareness, including the GDPR. We provide annual security and privacy training, to educate and remind people about the importance of safeguarding and protecting data, and to ensure they handle it correctly.

3.5.3. Confidentiality

In addition to upholding their employment contract, Trustpilot's employees must read and comply with our Code of Ethics and Code of Ethics Guide & Examples. These documents describe and provide examples of best practices for how our employees should handle and protect the personal data we receive from companies and consumers.

3.5.4. Leaving

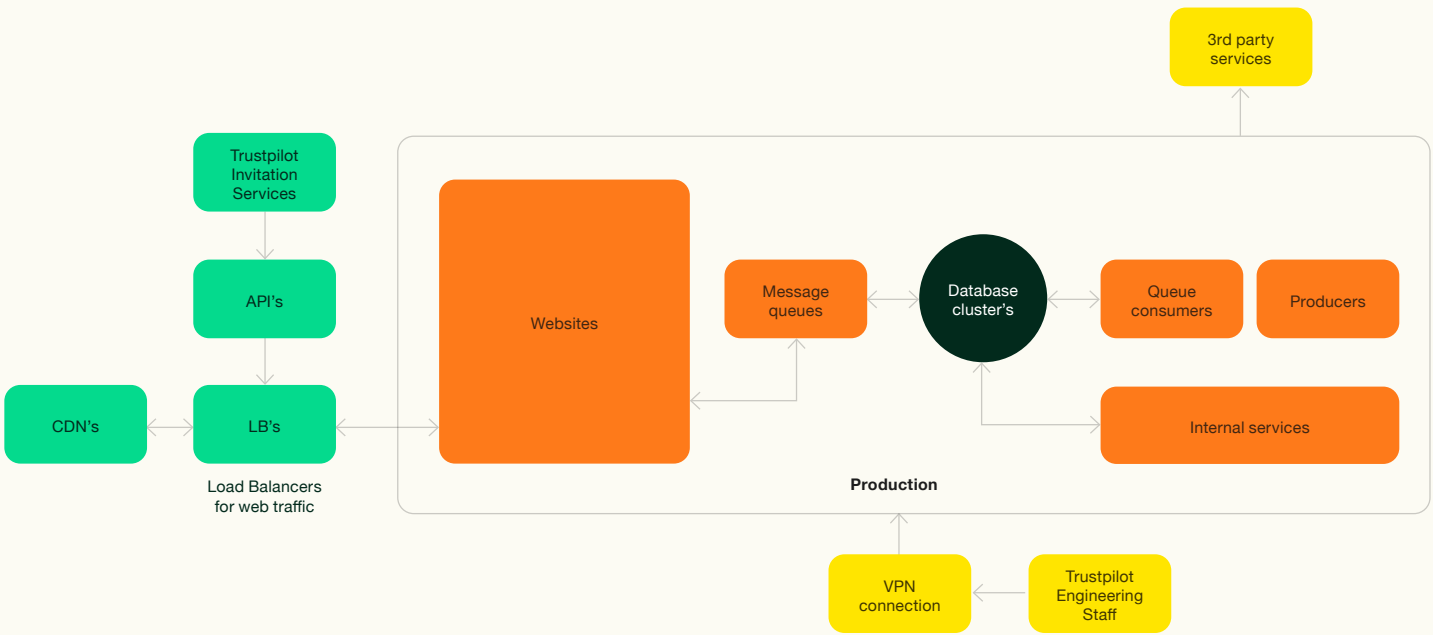
When employees leave Trustpilot, we revoke their access to our systems in a timely manner. For more information about this, please see 5.2, below.

4. Systems design and architecture

We've designed our platform to follow microservices architecture design principles, so our services and their underlying backend are decoupled and stateless. This lets us automatically scale our platform based on demand.

Our backend infrastructure is created directly from code instruction, referred to as "infrastructure as code" (IaC). It's repeatedly replaced to ensure a consistent and stateless environment, or "immutable infrastructure."

See a simplified overview of our architecture on the next page.



4.1. Security in the development of new products & services

We consider security concepts, assessments and techniques fundamental to the development, reliability, and overall improvement of our products and services.

Trustpilot operates on principles of least privilege first, which means that access is limited to those who have a genuine work-related need. All of our backend infrastructure is frequently recreated via code to ensure a lean and clean (or "vanilla") infrastructure that further enhances our immutable architecture.

We run an agile, dual-track software development lifecycle (SDLC) process. We pass all software changes through a formalized code review process, which is approved by the relevant Tech Lead prior to being released into isolated environments. Upon successful automated testing and quality assurance, the changes are promoted into the next environment stage to undergo further testing, before ultimately being promoted into production.

All code changes are version controlled and stored in Github, which is our source code repository management platform.

We do not rely on outsourced development — all of our development is in-house.

4.2. Data sub-processors

In order to provide you — as our customer — with the best possible service, we use specialized service providers who assist us with delivering parts of our services, such as data center and emailing. Pursuant to the GDPR, these service providers are called sub-processors. On our website you can find an overview of the sub-processors we use to deliver our services to you.

Before we engage a new sub-processor, we perform due diligence as part of the contract discussions. Among other checks, we evaluate privacy and security aspects and practices, and perform a risk assessment of the personal data that will be shared with them. If the new sub-processor has adequate organizational and technical security measures in place, our Legal Team performs a mandatory review of the contract and ensures that a data processing agreement is in place. It is only after these checks have been made that they will be granted access to systems and data.

We repeat the due diligence process annually. In between reviews, we conduct spot checks to ensure ongoing compliance.

When sub-processors are no longer contracted with us, we immediately remove their access to our systems and data.

4.2.1. Trustpilot subsidiaries

We are a global company, which means that employees from our subsidiaries may be involved in processing your data, for example when providing support outside of normal local business hours.

We list our subsidiaries in the overview of our sub-processors on our website and also include them as a chart in section 6, below.

We list our subsidiaries in the overview of our sub-processors on our website.

4.2.2. Data centers

We host all data with Amazon Web Services and Google Cloud Services. Amazon Web Services is SOC 1, SOC 2, SOC 3 and ISO 27001 certified. Google Cloud Services is SOC 1, SOC 2, SOC 3 and ISO 27001 certified. We don't use any other data center facilities and we don't host data ourselves.

Amazon Web Services and Google Cloud Services host our data in their data centers within the European Union.

Their data centers are highly secure and use state-of-the-art electronic surveillance, intrusion detection and multi-factor access control systems. Trained security guards patrol the data centers around the clock, and access is authorized strictly for those who have a genuine business need (following the principle of least privilege). The environmental systems are designed to minimize the impact of disruptions to operations.

Amazon Web Services and Google Cloud Services have designed their data center infrastructures to provide optimum availability while ensuring complete customer privacy and segregation.

We use a three data center configuration with Amazon Web Services. We run on all the data centers simultaneously, with automated and seamless recovery at outage of a data center. We may choose to increase the number of data centers in the future. All our data centers are hosted in Ireland, which we plan to change once Amazon Web Services supports it, so we increase the physical distance between the data centers, however still limited to data centers within the European Union. All users of our platform run within this configuration.

We build our backend infrastructure with code and follow infrastructure as code principles, which means that we can frequently rebuild our infrastructure to ensure that it's always complete, lean and clean. We've chosen this design to enhance our "immutable architecture", as described above.

All of our operating systems, databases, and applications have been hardened to reduce any vulnerabilities and maximize their security.

Your data is kept secluded from other data, separated by a unique ID for each entity and administrative interface on our platform.

Our network and instances in the data centers can only be accessed through VPN. Only authorized employees with a work-related need are granted access to the data centers. Our VP of Engineering and/or CISO currently approves all access. VP of IT and Operations and/or CISO approves access to Trustpilot internal services.

We host our staging and test environments with Amazon Web Services and Google Cloud Services. We don't use production data in these environments.

4.2.3. Emailing platform

We use SendGrid as our provider for sending and receiving emails. For example, when you use our Automated Feedback Invitation service:

- We use SendGrid to pass review invitation request emails from you to us
- We use SendGrid to pass review invitation emails from us to your customers.

SendGrid works as a transient service, keeping your data only for as long as it is technically needed by the integration between Trustpilot and SendGrid, and never for more than 32 days.

SendGrid also provides Trustpilot with information about review invitation emails that are received, opened, clicked on, or have bounced, etc., so we can make this information available for you inside our product.

SendGrid is SOC 2 certified.

We secure the emails we send with:

- Sender Policy Framework (SPF), which we have configured restrictively so that we only send emails from our domain.
- DomainKeys Identified Mail (DKIM), which ensures that the content of our emails remains trusted and hasn't been tampered with or compromised.
- Domain-based Message Authentication, Reporting and Conformance (DMARC), which ties the first two protocols together with a consistent set of policies.

4.3. Security

4.3.1. Infrastructure

We constantly monitor our infrastructure and product for errors so that we can detect and address these quickly.

We use Amazon Web Services and Google Cloud Computer security groups, and VPC peering for firewalls to protect against internally generated attacks.

We frequently conduct third party automated security scans against our products, and we run a bug bounty program — all with a strong focus on addressing web vulnerability, OWASP and security risks. The summary results of these scans can be made available to companies under NDA.

You are welcome to conduct your own security scans and penetration tests against our services, as long as these are of a non-malicious nature and you write to us (contact Trustpilot A/S) beforehand for pre-approval. Asking for pre-approval gives us time to make sure we have the resources available to react to any anomalies in our monitoring that might follow from your scans or tests.

Trustpilot's server instances at Amazon Web Services and Google Cloud Services are only accessible through VPN. The physical security of our cloud infrastructure is handled by Amazon Web Services and Google Cloud Services. You can request compliance reports directly from Amazon Web Services or Google Cloud Services.

We use a synchronized time-service protocol to ensure all systems have a common time reference.

4.3.2. Malicious code management

Because our backend infrastructure is created directly from code and is frequently and automatically rebuilt, we don't use antivirus or anti-malware software on our server instances.

4.3.3. Software security patch management

We use automation to apply security patches to all of our infrastructure programmatically.

4.3.4. Encryption

Data to and from our cloud infrastructure is encrypted during transit, and data on our cloud infrastructure is encrypted at rest using industry-standard AES-256 algorithm. Data stored on our cloud infrastructure is protected by firewall and housed within multiple isolated Virtual Private Clouds (“VPCs”).

To safeguard the traffic between our users and our platform, all web communication is 128-bit encrypted as minimum. All of our websites use Transport Layer Security 1.2 (TLS). Trustpilot only supports data sent via web submissions that use HTTPS/SSL.

To safeguard personal data, we send emails using Transport Layer Security (TLS). If the receiving client doesn’t support TLS, we use the next highest secure protocol supported by them.

We use instant messaging systems where data is encrypted during transit.

Our Business Generated Links invitation service uses 256-bit AES encryption.

4.4. Data

4.4.1. Classification

We classify and label data to ensure that it is assigned to the proper access and retention model. For example, we classify your data as personal data, which means that we will make sure that only authorized Trustpilot employees have access to it.

Our classification model is reviewed at least annually by our security team.

4.4.2. Backups

Our backup procedure includes, at minimum, a daily full backup which is carried out automatically.

We use Amazon Machine Images to create backups, and then transfer and store these electronically on separate availability zones at Amazon Web Services within Europe. Only our Site Reliability Engineers have access to the backups.

We perform backup recovery tests regularly.

Our backups are stored in a secure, tamper-proof manner, and cannot be manipulated or changed. We retain backups for 45 days, after which they are destroyed automatically.

4.4.3. Logging

All of Trustpilot's backend infrastructure ships logs to a centralized solution where they are aggregated, reviewed, and analyzed. We do not store logs locally to further enhance our immutable architecture.

Our engineering team and team members are only granted access to our logs based on their work-related needs, which we monitor continuously. The engineering team can only access the logs using a dedicated VPN.

Examples of logged activities are:
- Application exceptions
- Stack trace
- Traffic statistics
- Backend changes and deployments
- Malicious activity and exceptions

Our logs are confidential and not made available outside Trustpilot. They are stored in a secure, tamper-proof manner and cannot be manipulated or changed.

We keep our logs available for a maximum of 14 days, after which they are archived for a further 31 days. After that, they are destroyed by means of automation, unless we are legally required to keep specific log data for a longer period of time.

4.4.4. Data retention

4.4.4.1. Requests to send out review invitations

We need access to your customers' personal data for us to send review invitations to them on your behalf. This data belongs to your company. We use this data to construct, send, and track the review invitation emails. Depending on the service that you use, you may send this data to us as uploaded files, BCC emails, or through our API.

We keep the data for a maximum of 30 days, then delete it automatically from our databases.

4.4.4.2. Review invitations data

When we send review invitation emails to your customers on your behalf, we retain data about the review invitation(s) as invitation history in your Trustpilot business account. By default, we retain this data for a maximum period of three years, after which we delete the data from our databases.

When you send review invitation emails and ask us to generate the invitation links, we retain the data you send to us so we can prepopulate the review evaluation web page when the user clicks the invitation link in your email. By default, we retain this data for a maximum period of three years, after which we delete the data from our databases.

If you need to delete your company's data sooner, you can do that yourself. For example, you may want to delete all data older than six months. Please note, however, that deleting data can disable the link in any review invitation emails already sent to your customers. This will prevent them from using the link to leave a review.

If you choose to discontinue your subscription to our paid services, your company will be moved to a free subscription. This will not impact the retention of your data and the data retention rules stated above continue to apply, as well as your ability to delete the data at your convenience.

If you decide to stop using our services altogether, you can contact us at privacy@trustpilot.com to ask us to delete data owned by your company and we'll carry out your request as soon as possible. Please note that we only delete data concerning your invitation history and business account. Even if

you stop actively using our services, we don't delete company profiles from the Trustpilot platform.

4.4.4.3. Your customer data

If your company has engaged Trustpilot to assist with sending out review invitation emails and collecting feedback from your customers, it's likely that your company will share personal data about customers with Trustpilot.

Article 28 of the GDPR requires that the data controller and data processor put in place a data processing agreement that describes the data processing activities being carried out. Therefore, we've included a Data Processing Agreement that meets the requirements outlined in the GDPR in all of Trustpilot's customer agreements. This also applies to companies on our Free plan.

It follows from Article 13 of the GDPR that a data controller must provide its data subjects with specific information about how it processes their personal data. If you share personal data about your customers with Trustpilot, we recommend that you update your privacy policy to state that Trustpilot acts as your data processor and explain why you share information with us.

As defined in Article 17 of the GDPR, your customers have the right to ask you to delete the data you have about them. If your company uses Trustpilot review invitation service and you receive a request from a customer to have his/her personal data deleted, you can use our delete invitation data functionality. This functionality allows your company to delete your review invitations data up to a certain date or about a specific customer using your business account. For more details on how this works, please see this article.

If your customer has left a review on Trustpilot, they will have been asked to accept our Terms & Conditions and Privacy Policy before posting their review — and before we save information about their review. From the point that the reviewer accepts our terms, all information that we collect about them is in our capacity as a data controller. Therefore, if the reviewer has any questions about how we handle their personal data, they're welcome to contact us directly by sending an email to privacy@trustpilot.com.

4.5. Access for companies

You can access your company's profile on Trustpilot when you claim it.

Depending on which subscription plan you have with us, one or more of your employees may have been granted access to work with your company profile in our product. All paying customers also have the

ability to use role-based access control methods, to allow for greater granularity of access for your employees.

There are two ways you can log in to our business portal: using a native login, or by logging in with a Google account. We don't currently support single sign-on (SSO) through SAML2.

All business portal users have the option to setup 2-Step verification, as an additional layer of authentication.

Depending on which subscription plan you've signed up for, you may also have access to data via API. API access requires an API key and secret, which are unique to your business account.

Please refer to our Privacy Policy for details on how we collect, use, disclose, transfer and store your personal data when you create a business account on behalf of your company.

You can choose to give (and revoke) consent to Trustpilot employees to access your account on your behalf so we can assist you with setting it up and maintaining it.

We log all actions that users perform in our business portal, including actions performed by Trustpilot employees on your behalf, however these logs are confidential and not made available outside Trustpilot.

4.6. Privacy

When you share personal data about your customers with us, we expect you to limit what you share to only what we need to construct and send emails on your behalf, and to link the resulting invitation and any review with your own systems. Please don't share sensitive personal data with us.

When consumers write a review on Trustpilot, they are required to accept our Terms & Conditions and Privacy Policy, including our User Guidelines. From the point at which they accept our terms, we collect and process information about the review and the consumer, and we assume the role of data controller for this information.

In our GDPR-compliant Privacy Policy for users, we set out what types of information we process, including information about our cookies, and how we process personal data.

If you have any questions about the data processing activities that we carry out on your company's behalf, you're welcome to contact our DPO at privacy@trustpilot.com.

4.7. System status & maintenance

You can see and subscribe to up-to-date information about our security and data incidents, and about the operationality of our systems, at https://status.trustpilot.com/. We also use this site to inform users about planned maintenance.

5. Corporate IT

Our Corporate IT department has employees across our offices in Denmark, the UK and the US. They work as a team, in cooperation with the rest of the organization, to streamline and improve our security and protection measures.

Aside from maintaining and owning our office network infrastructure Corporate IT helps us with managing our accounts, password security, access to systems and data, and protecting our IT assets - including hardware and software.

5.1. Account provisioning

All Trustpilot employees are granted an individual “@trustpilot.com” user account. We don’t allow any two employees to share or use the same user account.

Access permissions for individual systems and user roles are granted from our role-based access control model (Trustpilot’s RBAC) using least privilege first principles and according to work-related needs. Before we grant access, the internal owner of the respective system must approve the assignment of access rights and roles. We require a segregation of duties between the person requesting access and the person who approves it.

Access to our operational systems is restricted. Access is only given to authorized employees after approval from the member of our top management team who is responsible for information security.

5.2. Access review and removal

Access rights to our systems and data are reviewed at least quarterly by dedicated staff, and employee access is removed or downgraded when it is longer required to carry out duties and responsibilities.

When an employee leaves, their user accounts are immediately disabled and, once they are no longer subject to other legal requirements, deleted. Any information security and legal responsibilities held by the employee remain valid after they leave our employment.

5.3. Passwords

All internal user accounts are protected with a password which must meet the rules described in our Information Security Policy.

We use Azure AD as our internal identity directory, where we have enforced multi-factor authentication. Our internal systems are configured to authenticate with Azure AD. When this isn't possible, we enforce multi-factor authentication on systems that cannot authenticate with Azure AD.

5.4. Office networks

Every Trustpilot office location is equipped with a dedicated, secure wired and wireless network for Trustpilot employees and contractors, and a wireless guest network dedicated for Trustpilot guests and employees using their own personal devices. We keep these separate — there's no connection between our secure network and our guest network.

The electrical and network cabling in our offices is installed and maintained by locally certified personnel.

The Trustpilot product treats our office networks like any other Internet network, and doesn't apply any extra level of access to a device or user connecting from our networks.

Individuals who use our networks are not allowed to carry out unauthorized downloads, store or share copyrighted or intellectual property material, or install or run unauthorized, untested, or unlicensed software.

We manage network device security patches centrally. We follow a review and release process when upgrading devices to the latest, most secure firmware version.

5.4.1. Secure network

Our secure network acts as an Internet access point for Trustpilot-owned laptops and desk phones, and other local services to employees such as scanning, printing and meeting room conferencing.

No application or file storage services are provided on our secure network, which we enforce by not having such servers in our offices. We instead use collaborative cloud services such as Google G Suite, Salesforce, and Box.com that we can access securely from anywhere.

Access to our secure network is only granted to a Trustpilot employee who successfully logs in with valid credentials from a Trustpilot-owned device that has a valid certificate.
Our secure wireless network uses WPA2 with 802.1x authentication.

5.4.2. Guest network

Our guest network acts as an isolated and segregated Internet access point, where users authenticate using a unique, randomly generated key that expires after one day.

5.5. Assets

We broadly define our network equipment, stationary devices, mobile devices, software, and removable media as IT assets.

We identify, register, and assign owners for all our IT assets.

5.5.1. **Devices**

We enforce a centrally managed network login on all Trustpilot-owned laptops, stationary PCs, and stationary MACs.

Centrally managed disk encryption is enforced on Trustpilot-owned laptops, stationary PCs, and stationary MACs. Our Corporate IT team controls the encryption keys.

Centrally managed screen lock timeout is enforced on Trustpilot-owned laptops.

Centrally managed virus and malware detection and protection software is enforced on all Trustpilot-owned laptops, stationary PCs, and stationary MACs. The client and definitions are updated daily, and a full system scan is completed once a week on Windows systems and bi-weekly on macOS systems.

Patching of operating systems on all Trustpilot-owned laptops, stationary PCs, and stationary MACs is enforced and managed centrally.

We use training, policies and company messaging to make employees aware of their responsibility to protect our equipment, including unattended devices.

5.5.2. **Removable media**

As a general rule, we don't use removable digital media such as USBs, DVDs, or portable hard drives to store personal or confidential information. In special situations we use USBs, but only under supervision of the Corporate IT team who ensure that the USBs are wiped before and after use.

5.6. **Physical security, papers and hardware**

Our offices cannot be accessed directly from the street and we require visitors to register before allowing them access. CCTV surveillance is also in place in our offices.

We maintain a paper-free environment and documents are not printed unless necessary. When disposed of, all documents containing sensitive information are shredded. We also have a clean desk policy and information is not stored on on-premise media.

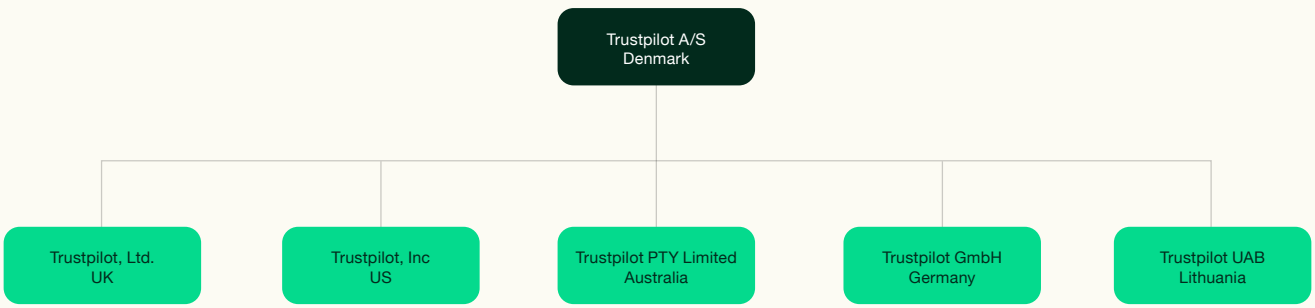
After use, our hardware is recycled. We use an IT disposal company that collects printers, laptops, and other equipment and dismantles everything, including wiping hard drives. This process is recorded with certifications.

Physical security measures are reviewed and evaluated on an annual basis.

6. Company information

Trustpilot's parent company — Trustpilot A/S — was established in 2007 by our CEO, Peter Holten Mühlmann, and is located in Copenhagen. It has company registration number 30276582.

The Trustpilot company structure consists of a Danish-domiciled parent company and subsidiaries in different countries, as shown here:



6.1. Contact us

If you have any questions or concerns about our security practices; our data privacy practices, you are welcome to send an email to privacy@trustpilot.com.

You can find more on data privacy and our security practices in our online Support Center.


Trustpilot