SURVEY PROGRAM INFORMATION SECURITY

Data Privacy

The security and privacy of data shared with ClearlyRated is of utmost importance to us. We have taken the following steps to ensure that the privacy and security of all data shared with ClearlyRated is maintained:

- Implemented an industry standard Information Security Program and Policy that all employees are trained on and required to follow.
- Self certify into the EU-U.S. and Swiss-U.S. Privacy Shield programs (https://www.privacyshield.gov/welcome), which are stricter data privacy frameworks than is required by US law.
- Fully GDPR compliant privacy policy - https://www.clearlyrated.com/solutions/privacy-legal/
- Applied industry best practices on the storage and security of the data within our database servers and employee computers, including full hard drive encryption of all employee computers.
- Restrict access to production servers that store confidential information to the small number of employees needed to maintain those systems.
- All transfer of confidential information is fully encrypted at all times.

Any further questions relating to privacy and confidentiality of personal information can be directed to Nathan Goff the Chief Technology Officer at ClearlyRated. He can be contacted at ngoff@clearlyrated.com.

GDPR Compliance Statement

First and foremost as an organization we have always taken very seriously the protection of the data our clients entrust us with. From the beginning of ClearlyRated we have had in place security measures and policies that address the protection of all of the data our clients share with us. It is core to our DNA to balance the needs of our clients and the customers they serve, which we believe that balance is in the best interest of both parties. This doesn't stop when it comes to the privacy and protection of our clients customer data.

All of our servers are located within the US so all data processing is happening here. To address the transfer of EU data to US servers we became certified under the EU-US Safe Harbor framework in 2010 and to show compliance with GDPR we have certified into the EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield frameworks.

In the context of a satisfaction survey our clients have a legitimate interest in gathering feedback from their clients or employees to assess how that relationship is going. Therefore, we believe all satisfaction survey related data falls under the 'legitimate interest' category of the GDPR. It therefore does not require any additional consent to collect feedback with our tools so long as no questions are added to the survey that could be used primarily for sales and marketing purposes.

Here is what we have done to be in compliance with GDPR:

- Completed a full inventory and mapping of how all personally identifiable data makes it into our system and how it flows through it.
- Consulted with our legal council that has expertise in GDPR to help us identify what we need to do for compliance.
- Updated our privacy policy to be GDPR compliant.
- Submitted privacy policy to the FTC as part of our application to self-certify into Privacy Shield. Certification was accepted and approved - https://www.privacyshield.gov/participant?id=a2zt00000008RCHAA2&status=Active
- Completed audit of all of our 3rd party vendors that come into contact with GDPR subjected data in the process of providing services to us and confirmed that they are Privacy Shield certified.
- Confirmed that existing policies and procedures for prior Safe Harbor certification set us up for a small amount of change to be GDPR compliant. Completed the small changes necessary to be compliant.
- Completed documenting process for responding to requests from EU and UK citizens to know what data we have on them and to delete it if requested.
- Initiated a project with outside data security experts to complete an audit of our environment and identify anything we should address. This is not required for GDPR compliance, but is an extra step we feel is important to show how much care we take with our clients data.

Technology Environment Details

At ClearlyRated, we take information security very seriously. This sheet provides technical details for ClearlyRated’s survey system and provides answers to common IT Department questions.

Servers

- All production survey fielding and reporting applications are hosted on leased dedicated hardware with Rackspace in their Chicago datacenter.
- All leased managed server hardware employs industry best practices for hardware redundancy around disks, power, and network.
- See http://www.rackspace.com/about/datacenters for full details on this datacenter and the certifications it has received. Sampling of some of the certifications this datacenter has received are: SOX, HITRUST, PCI-DSS, ISO 2700-1
- Application and database servers are dedicated to those functions and do not operate both on the same server.
- All of these servers are dedicated and managed hardware not within cloud or shared hosting environments.
- All production servers run a supported and managed version of Red Hat Enterprise Linux.

Networking

- All production server hardware is behind a managed Cisco firewall.
- Only ClearlyRated leased hardware is attached to the firewall.
- Industry standard protocols are followed to provide very limited direct access to firewall and the servers behind it.
- DNS services managed by Cloudflare.
- See http://www.rackspace.com/about/datacenters for full details on network uptime SLA.

Redundancy

- All production application servers have managed backups on a daily basis.
- All production database servers have a real-time replica with daily full backups.
- Rackspace managed services provides redundancy to all other aspects of the infrastructure.

Email

- Emailing infrastructure provided by Mailgun.
- All email sent on a dedicated IP.
- Email certification provided by ReturnPath.