Privacy & Data Protection Practices

Commitment

IRB sincerely believes that the protection of personal data of panelists or survey participants is the primary responsibility of all the Market Research companies who possess or process the data.

IRB keeps auditing it's data protection mechanism regularly and follows the best practices outlined by international and local laws and leading Market Research Associations to ensure the compliance.

Assurance

IRB has a strict privacy policy in place which is based on the laws of the countries where it has panel and/or conduct surveys.

IRB is firmly committed to protect the privacy of survey participants and avoid the dissemination of their personally identifiable information, in accordance with international regulations including, but not limited to The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks, GDPR (EU) and ISO. At Industry level, we follow the guidelines of Insight Association, ESOMAR and MRSI.

IRB's privacy practices are being scrutinized and certified by TRUSTe every year since 2013

Privacy by Design

IRB's panel recruitment, data collection, data handling and data sharing model is designed, ensuring the application of privacy and data protection principles at all stages of corporate functions, IT system, network infrastructure and business practices, as a complete solution to meet the purpose. IRB has adopted the framework that ensures privacy and data protection for all it's current & future products/ services.

All employees of IRB are trained and updated in timely manner to follow the framework of privacy & data protection throughout day-to-day business activities and developing new processes, products & procedures.

Database Security

All possible measures are implemented to ensure the data security (hosting, security checks, network firewalls, application firewalls, anti-virus, restricted access on public internet, userbase password protected access, anti-cyber threat software etc.). IRB's database is secured through SSL encryption by Symantec (now known as Digicert).

IRB has implemented a strong security system and able to identify the breaches timely and quickly. A process is already in place to deal with the clients/partners in case the PII is demanded (Legal, Documentations). They are expected to comply with data protection guidelines and have a strong security program in place, to avoid any kind of threat against data protection and must be able to identify the breaches and inform us in time. All other timeline adherences are expected in case of any breach from the third party (or Processor).

IRB has implemented an operation level structure to minimize the threat of data leak and misuse internally. Access to the database is limited to authorized team members only and there is a formal approval process in place to grant, update or remove accesses of the individuals based on the job roles.

Security Infrastructure

Server Management

- Our servers having any personal data collected from users are running with secured firewall/s and with OS patch updates.
- 3rd party applications like cPanel to manage hosting services are configured to be up to date with any critical released vulnerability patch/s.
- There are rules written for http to https redirection for front end web browser access to all public facing web applications.
- Remote shell access to servers is bound to known IPs that guarantees access of servers to only know & identified people.
- Default ports to access the servers remotely are changed in order to protect any bad attempts to reach the login window of servers.
- Remote Access of cPanel to manage hosting on server is also secured and limited to known and identified IPs only, ensuring a safe & identified access.
- Servers & cPanel are configured to protect the system from Brute Force attacks and make a self-decision of blocking, restricting all access to an IP or a range of IPs after a number of defined wrong attempts.
- Server firewall is configured to prevent DDOS attacks, and have some DDOS attack detection rules in place, which upon such identification takes self-initiated action and blocks all access to such source/s.
- FTP access to servers for the purpose of upload, download and making changes to files by developers is also restricted and limited to known IPs, which can be accessible only through identified users over company VPN.
- We are not exchanging any personal data of users over any 3rd parties applications, like Skype, or and other 3rd party method to send & receive files.
- Information exchange with server by internal office users is made mostly using SFTP over VPN (Secure File Transfer Protocol), in some cases where we need to share data from one user to another, we use own corporate Microsoft Exchange Email Server.

- We have Production databases on MySQL Platform. These databases are hosted on secured production servers only, which are also well secured in terms of their access.
- Our production database is designed to accept and allow access only to identified users with their protected passwords.
- Since servers hosting the databases are secured in terms of access & attack prevention, databases hosted on these servers also leverage the same level of securities.
- Communication channel to database from Application is encrypted with HTTPS/SSL encryption.
- We have a system in place that is dedicated to perform encryption of Personal Information Data and store data in encrypted form in database. Also, only encrypted packets of data are transmitted while performing send & receive request.

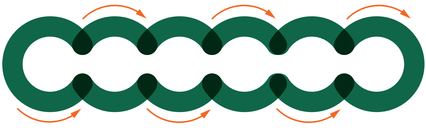
Applications & Processing

List of applications accessing & processing PII data submitted by users –

- Opinionbureau.com
- Onlinesurveybureau.com
- Surveys.irbureau.com
- The-capacity.com
- Capacitysurveys.com
- Pasmt.com

PII DATA FLOW & PROCESS DIAGRAM

Process Starts here



PII Submitted by en users/s	PII Travel over SSL	PII received at PKI-AES Encryption node at designated Server	PI Encypted and stored in Database	PII data is retrieved from server in encrypted mode over SSL/VPN to internal non public facing server using DB to DB or SFTP method	DB/Application developers decrypts the data on their system and use it for analysis purpose. Connection to the internal private server is closed after all analysis is peformed on PII

Privacy Policy and Update Notification

All the important information is being shared with the panelists in privacy policy statement explicitly. It very clearly answers "WHO, HOW and WHY the data is being gathered, how is it going to be used and who will it be shared with" and we also get consent from the panelists/survey participants before using it.

IRB's privacy policy link can be accessed at below link:
https://www.opinionbureau.com/requestedContent?pageId=privacy_policy

Whenever IRB updates privacy policy, it notifies all of the members about updated policy through email and dashboard notifications in their Opinion Bureau account. It's up to the individual to either agree or disagree with the new policy. In case of disagreement, one can immediately withdraw their consent and discontinue membership with the website (or panel). IRB follows the process to delete all personal and related information of a user from database on the withdrawal of membership.

Consent & Transparency Management

IRB explicitly informs the purpose of data collection and it's usage to the panelists and/or survey participants and seek their consent before allowing them to join survey panel and participate in online surveys/votes. IRB asks for the individuals' consent every time they participate in surveys that demands PII collection and sharing with third-party.

IRB collects personal information in relation to obtaining an individual's consent as a legal basis for processing personal data. IRB ensures that their consent indicates their agreement to participate in IRB's surveys by clearly understanding the purpose and usage of their personal information. For example, consent management process for panel recruitment can be viewed at below link on signup button click:

https://www.opinionbureau.com/RegistrationForm

An individual can withdraw the membership at any time by opting out from IRB's panel. And IRB ensures that all personal and related information is deleted from the database.

Right to Access, Rectify & be Forgotten

The individuals who join IRB panel are the primary owner of their personal identifiable information and related data. At IRB, we have given the panelists full ownership of their data and they can access, rectify, delete and unsubscribe with easy steps. The data is fully deleted once the panelist unsubscribes and we do not send any mails or make any contact to the person until they register and go through the signup procedure again.

IRB provides 24 * 7 help desk support to the panel members with 24 hours of request processing turnaround time.

We do not hold any data of unsubscribed panelists and is disposed with all possible safety measures.

Detection of Breach

- We follow a process of analyzing success and failure audit logs for every 12 hours that tells us how many attempts were made a successful login to a server or access provided through a service; and it also tells us if there are any bad attempts and also that the system blocked the bad attempt or allowed the access, however the latter one is very unlikely but in case found we start taking further action of finding and blocking such sessions/access.

- Except of the server level logs review, we have a firewall in place which automatically sends us an alert in case of any brute-force attack to direct or ftp bad login attempts with the source information, upon receiving such informative logs, we start our corrective action towards it.

Compliance Audit

IRB ensures the adherence of Privacy & Data Protection Policy without any breach by scrutinizing the practice through internal audits time to time. In addition to internal audits, IRB procures the audit services from TRUSTe to review it's Privacy & Data Protection practices and compliances by performing technical and manual scrutiny.

TRUSTe issues a certificate to IRB once audits and rectifications are completed.

IRB has appointed a Data Protection Officer (DPO) internally to ensure the order and compliance. IRB DPO is accessible @ dpo@irbureau.com.

Ashutosh
President
E: ashutosh@irbureau.com