Toluna

GENERAL DATA PROTECTION REGULATION

GDPR EXPLAINED

MAY 2018

TOLUNA STATEMENT ON ITS COMMITMENT TO DATA PROTECTION

Toluna is a member of the ITWP group of companies. We are a leading provider of real-time digital consumer insights and empowers companies to brainstorm ideas, uncover new business opportunities and answer their questions in real time. We are transforming the way marketing decisions are made by bringing consumers and brands together via the world's largest social voting community. This real-time access to consumers is coupled with its state-of-the-art, market research survey and analytics platform. Toluna has 21 offices in Europe, North America, and Asia Pacific.

No organisation can ignore a critical area: i.e. risk from vendors/suppliers or and other third parties i.e. contractors, partners, and service providers when those third parties process personal data on behalf of the data controller, or when those vendors/suppliers are otherwise required to process personal data in order to perform the requisite services. In order to comply with the principle of accountability under the GDPR, organisations should properly identify, track and protect the personal data they control, especially when third parties are processing those personal data on their behalf.

When data controllers appoint data processors to process personal data on their behalf, they should ensure such processors implement appropriate technical and organisational measures to ensure the rights of the data subjects are protected and that the data controller must enter into written contracts with the data processor requiring them to process the personal data in a certain way (Art 28).

In addition, organisations need to have peace of mind from their suppliers to ensure the services being performed for them will not be interrupted or negatively impacted from any change in the law.

In light of the above, we have prepared the following document, and FAQ with the aim of providing you with information to aid your due diligence and assessment of Toluna's GDPR compliance levels post 25th May 2018, when selecting us to process your customer personal data in the course of providing market research services to you.

WE ADHERE TO ALL MARKET RESEARCH STANDARDS FOR DATA PROTECTION

Being a market research industry leader, keeping our client's information confidential and secure is of the utmost importance to us. We comply with the ICC/ESOMAR International Code on Market, Opinion and Social Research and Data Analytics and other applicable guidelines and codes of conduct on market research. See links below:

https://www.esomar.org/uploads/public/knowledge-and-standards/codes-and-guidelines/ICCESOMAR_Code_English_.pdf

We provide our services using market research industry standards, techniques and methodologies to ensure that respondents to market research studies are kept anonymous and the results are provided on an aggregated basis.

THE GENERAL DATA PROTECTION REQUIREMENT (GDPR) EXPLAINED

The General Data Protection Regulation 2016/679 (GDPR); a regulation in EU law on data protection and privacy for all individuals within the European Union and/or citizens/residents of the EU comes into force on 25 May 2018. This regulation replaces the EC Directive 95/46 on Data Protection. The purpose of the framework is to strengthen data protection rights for individuals, giving citizens more control over their personal data and to simplify the regulatory environment for international businesses by unifying the regulation across the EU and the EFTA countries. This should make it easier for individuals in the EU to understand how their data is being used and how and when to raise complaints if they believe their data is not being treated lawfully or fairly (even if the organisations processing their personal data are not located in the same country in which the EU citizen is resident).

The GDPR is intended to strengthen individuals rights:

The right to be informed: Being transparent on the use of individuals' data, including e.g. providing fair processing information through our privacy notices to our panellists.

The right of access: Confirmation that we are processing individual personal data, allowing them access to the personal data we process about them and providing them with additional relevant information they may ask us in relation to such processing.

The right to rectification: Having their personal data rectified if it is inaccurate or incomplete, and third-party processors should also be made to rectify their data if inaccurate or incomplete.

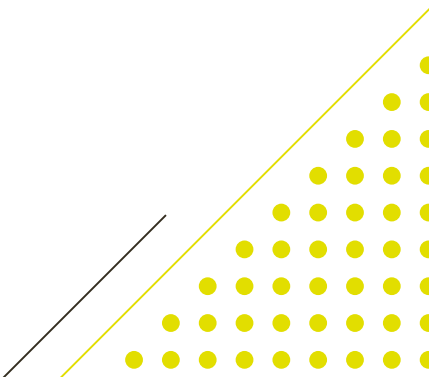
The right to erasure: Delete or remove his/her personal data where there is no compelling reason for its continued processing.

The right to restrict processing: In certain circumstances, blocking or supressing the processing of their personal data if requested and where so restricted, storing minimal personal data, and ceasing to otherwise process their personal data.

The right to data portability: Moving, copying or transferring personal data easily from one IT environment to another in a safe and secure way and in an easily readable format.

The right to object: If an individual objects to processing their data for certain purposes (including for scientific or historical research and statistics) on grounds relating to his or her particular situation, ceasing to process their data unless there are legitimate grounds for the continued processing.

Rights in relation to automated decision-making and profiling: Individuals should not have decisions made about them if such decision-making was based on automated processing; and such decision has legal or other serious consequences for the individual.



ENSURING OUR COMPLIANCE WITH THE GDPR

For the many years we have been in business, we have always had clear terms with our panellists on how we process their Personal Data and to whom in what circumstances we may disclose their Personal Data. In order to address how the GDPR affects our business, we have undertaken a global program to review and address key areas on where we may need to change our policies, processes and procedures and have outlined the following.

Data Security

Our clients can expect that we will treat their data with the same high level of security and privacy as Toluna does its own data.

We will only accept client provided personal data via secure encrypted transfer protocols such as FTP sites. Similarly, any client provided data required to be forwarded to a third-party supplier for processing will only ever be transferred via secure encrypted transfer protocols.

Client data will only be processed for the purposes for which they were provided and for no other reason. Access to the data is restricted to pre-defined and tightly controlled groups of employees on a 'need to know' basis only.

Data Hosting

All our hosting and backup services are managed by its USA company; Toluna USA Inc., ("Toluna USA") from the Toluna data centre in Wilton Connecticut. Toluna USA recognises that the EU has established strict protections regarding the handling of EU personal data, including requirements to provide adequate protection for EU personal data transferred outside of the EU. Toluna USA has elected to self-certify to the EU-US Privacy Shield Framework administered by the US Department of Commerce ("Privacy Shield") so that it can provide adequate protection for all EU personal data. Toluna USA is responsible for the processing of personal information it receives, under the Privacy Shield and subsequently transfers to a third party acting as an agent on its behalf. Toluna USA adheres to the Privacy Shield Principles of Notice, Choice, Accountability for Onward Transfer, Security, personal data Integrity and Purpose Limitation, Access, and Recourse, Enforcement, and Liability. You can find details of our self-certification via the link below:

https://www.privacyshield.gov/participant?id=a2zt0000000TP1YAAW&status=Active

Training Staff to Work With Data

Toluna has launched a worldwide mandatory training program for all its' staff who process personal data to ensure staff there is a high level of awareness and compliance with requirements of the GDPR and local data protection laws.

What We Expect of our Suppliers

We also work closely in partnership with carefully selected third-party suppliers and we enforce stringent terms on processing data and the performance of the services, ensuring they meet our standards. Part of the onboarding process means that our suppliers or potential suppliers are required to complete detailed data security and GDPR compliance questionnaires, as well as providing information on their quality standards and other key information. The questionnaires are then vetted by the Toluna management to ensure our standards on quality, data security and data processing, including those of our clients are met. Additionally, we do not allow our suppliers to subcontract any portion of the services without our prior consent.

Data Transfers

We will only transfer EEA personal data outside the EEA with our clients' prior consent and/or knowledge and put in place the EU standard contractual clauses to ensure that the necessary standards and requirements of the GDPR are adhered to.

Data Retention Policies

Client provided data is retained for a period between 6 and
12 months after survey completion in case a client requires clarification of the survey after it has taken place; unless otherwise requested by the client; after which it will be deleted.

Data Protection Officer

In preparation for the GDPR, we have appointed a Data Protection Officer (DPO). The DPO has appointed data privacy champions in all the major offices across the EU. The DPO is responsible for leading the ITWP group compliance program on privacy matters and the privacy champions ensure our processes and policies we have put in place to comply with the GDPR are complied with.

FAQ

Q: Please describe your organization's approach to privacy, including how privacy risks are assessed by your organization, reviewed and addressed by your leadership teams and the internal stakeholders involved in the development and implementation of your privacy program?

A: Our GDPR Steering Committee includes key individuals from our Legal, IT Security, Operations, HR, Client Services, Data Processing and Procurement teams to facilitate and maintain our GDPR program. The team is headed up by the Group General Counsel, who reports directly to the group CEO.

We have appointed a DPO and data privacy champions in every European country where we are operating. The DPO is responsible for leading the ITWP group compliance program on privacy matters and the privacy champions ensure adherence to the processes and policies we have put in place to comply with the GDPR.

We have conducted an Article 30 Data inventory questionnaire and report. This is reviewed and refreshed as needed or every 6 months, or every time there is a new processing of personal data.

Q: How does Toluna conduct privacy risk assessments of its products and services?

A: From the data inventory report, every processing is risk assessed to ensure that the processing serves a legitimate interest and is executed in accordance with our privacy notices and that the processing is necessary for the exercise of those legitimate interests. We ensure that any particular high risk processing e.g. children's personal data, special categories of personal data and client sample personal data are recorded and processes put in place to reduce the risk of causing harm to the data subjects involved.

Q: How does Toluna educate and train its personnel about data protection and data privacy policies and procedures?

A: We are conducting a training program for all our staff worldwide who process personal data. This is tailored and targeted to ensure the attendees have training that makes sense for the purposes for which they process personal data. These include:

- Data Privacy champions – and other key individuals, mainly member of Toluna's GDPR Steering Committee
- Human Resources
- Data Processing and Operations
- Sales and Researchers

Our training and policies on processing personal data also cover policies and provisions to ensure no data leakage and execution of EU contractual model clauses in the event that a transaction requires transfer or processing of GDPR citizens' personal data outside of GDPR jurisdiction.

FAQ (CONT.)

Q: What considerations and actions do Toluna take into account when processing personal data is required for the performance of market research services?

A: We consider the following when transferring/processing personal data:

- We use a secure transfer method and that whilst in transit, such personal data is encrypted;
- We ensure that the data subjects whose personal data is being processed have given their informed consent for the processing of such personal data;
- We ensure that we or third parties only process personal data that are necessary for the legitimate purposes for which such personal data were collected – so not excessive;
- We enter into appropriate data processing agreements for the receipt and/or transfer of such personal data with the relevant third parties;
- We assess the risks of the processing of such personal data to ensure that such processing does not negatively impact the rights and freedoms of the data subjects concerned;
- We vet all our supplier data processors and only transfer client personal data to them with the client prior consent.
- We enter into EU contractual model clauses if the processing is to be done outside the EEA, or the data is being transferred to a country that does not have adequate laws in place to protect the rights and freedoms of the data subjects concerned.

Q: If Toluna is required to transfer PII, what method is used for such a transfer and is any encryption used?

A: Toluna typically uses an SFTP site for transfers, as well as provision to encrypt the data during the transfer. PGP two-way encryption is the most commonly applied encryption technique, but we occasionally apply one-way encryption so that neither we nor the party on the other end of the PII transfer are given a legible rendering of members' PII data.

Q: Please provide details of Toluna's recruitment/registration process, specifically the details provided to panel members to verify that the required level of information has been provided to them to register their informed consent;

A: Panellist recruitment to a programme are subject to Toluna's standard privacy policy, as available on our website. In the event of specific project requirements, we will also obtain the requisite informed consent of the panellist.

Please note that in the light of GDPR we are currently reviewing all our privacy notices and will be making them available on the website by 25th May 2018.

Q: How is personal data kept secure? Please note any certifications you hold and provide certificate copies;

A: We are ISO 27001:2013 certified in relation to hosting customer data for our DIY online solutions

Q: What is the process for deleting personal data on request? What is the timeline for deleting personal data from receipt of request?

A: We will delete Customer sample data within 60 days of the request.

FAQ (CONT.)

Q: Where is Toluna panel data physically housed/stored?

A: All our hosting and backup services are managed by our sister company; Toluna USA Inc., ("Toluna USA") from the Toluna data centre in Wilton Connecticut. Toluna USA recognises that the EU has established strict protections regarding the handling of EU personal data, including requirements to provide adequate protection for EU personal data transferred outside of the EU. Toluna USA has elected to self-certify to the EU-US Privacy Shield Framework administered by the US Department of Commerce ("Privacy Shield") so that it can provide adequate protection for all EU personal data. Toluna USA is responsible for the processing of personal information it receives, under the Privacy Shield and subsequently transfers to a third party acting as an agent on its behalf. Toluna USA adheres to the Privacy Shield Principles of Notice, Choice, Accountability for Onward Transfer, Security, personal data Integrity and Purpose Limitation, Access, and Recourse, Enforcement, and Liability. You can find details of our self-certification via the link below:

https://www.privacyshield.gov/participant?id=a2zt0000000TP1YAAW&status=Active

Q: What security protections & safeguards does Toluna have in place?

A: Toluna follows defence in depth approach for security; all our business applications are hosted out of Toluna's own data centre which has multi-layer security. Application and Infrastructure is protected via WAF, IPS, Firewalls and hardened routers and servers.

We also conduct annual external security assessment by leading cyber security consulting companies; to identify any security gaps.

There is a 24/7 security monitoring team which looks at every incident and takes the appropriate action immediately.

Employees are also given annual cyber security awareness training and regularly briefed about latest threats.

Physical / Data Centre: Our datacentre is solely owned within a Toluna managed facility, with Physical Site Access controlled by card-key access system limited to Datacenter personnel.

Specifications:

- Location: Wilton, Connecticut, United States
- Owner: Toluna USA
- Power Architecture: N+1 (within Power Supply and batteries)
- Two 80KW Standby Generators
- AC Models:
  - 2 - 8 Ton DataAire A/C Units
  - 1 – 10 Ton APC A/C Unit
  - 2 – 4 Ton APC A/C Units (Standby)
- Halon 1301 Fire System

The following Network Services are completely redundant:

- Edge Routers
- Internet providers
- Core switches and routers
- Firewalls
- Content Delivery Services

The Perimeter consists of:

- Ingress and Egress filtering
- IPS inspection
- Application delivery via DMZ only
- Fail-Secure Design

FAQ (CONT.)

Q: What has Toluna done to update its breach response program as a result of GDPR?

A: We have updated our data breach response process ensure that responses for data breaches can be dealt with and, if necessary, reported to the appropriate supervisory authority within the required 72-hour period. We have a team of individuals across Legal, Security, Operations and IT that are assembled and notified quickly so we can comply with the data breach notification requirements of the GDPR.

Q: Does Toluna have any data centre certifications?

A: No.

Q: Does Toluna have any security certifications?

A: Yes, ISO 27001:2013 for our online diy solutions

Q: What is the disaster recovery/business continuity plan?

A: Disaster recovery plan:

- Activation of recovery operations would be implemented should services, from the Wilton, CT, data center location, be interrupted for a period beyond 24-hours. The VP of IT Operations, or designated alternate, will be responsible for making the activation decision. It is expected that business operations can resort to alternate processes ("work-arounds") during the 24-hour period.
- In the event of an outage to the Wilton, CT, data center, recovery will occur at the alternate data center, located in Dallas, TX, within the targeted 24-hour RTO (Recovery Time Objective), with a potential data loss of 24-hours (Recovery Point Objective). Applications will be recovered based upon criticality (Tiers).

Business continuity plan:

- Currently, the BCP process is informal
- We are actively working with outside consulting to create a well-defined global BCP plan

Q: Is it possible to enable multifactor authentication?

A: Yes, but this is not something that we currently provide.

Q: What is Toluna's password policy?

A: All Toluna members are required to register with a unique and valid email address and password. Members are prohibited from logging in with another account holder's password and from sharing their password with anyone else. When members forget their password, they are able to share their username to have a password reset URL sent to the email address associated with their member account.

Q: How does Toluna handle cookie consent?

A: Our Cookie Policy is prominently displayed within our Privacy Policy, and explains to members that use of our site constitutes acceptance of our use of cookies.

Our Cookie Policy also provides members with details about the types of cookies we use, the purposes for which they're used, the number of days a cookie remains active before expiration, and reference to resources members can use to block, control or delete cookies installed on their browser or hard drive.

FAQ (CONT.)

Q: What data is Toluna tracking on our clients' users or employees? Can they be identified by this data?

A: We do use cookies on visitors to our websites for promoting services that may be of interest to certain clients who have previously purchased certain services. The use of cookies is in accordance with our cookie policy.

Q: What practices and tools are Toluna using to bring itself in line with GDPR compliance?

A: We have put in place processes to ensure we know what data are being processed, by whom and where and for what purposes. We are also employing processes on logging and utilizing data leakage software to protect the loss and/or unauthorized processing of personal data.

Q: How long is the data stored?

A: Client sample data is stored for between 6 and 12 months in-line with ESOMAR guidelines, unless the client asks us to delete the data earlier. We keep the data for this period to assist our client in checking the validity of the market research, giving the client the opportunity of re-running the survey at a later date and other project related reasons.

Q: Is the organisation compliant with industry best practice standards such as ISO27001 or PCI-DSS?

A: We are ISO 27001 certified for our online diy tools e.g. Toluna QuickSurveys. Our processes and practices are by and large commensurate to the ISO27001 practices.

Toluna

E contact-uk@toluna.com T +44 (0)20 8832 1700 W corporate.toluna.com