Toluna™
In touch with people

General Data Protection Regulation (GDPR) Explained

Toluna Provides an In Depth Look at the GDPR and what it Means for Survey Research

Introduction

Over 100 countries, jurisdictions and territories across the globe now have privacy laws in place to protect personal data held by private and public bodies and over 40 countries and jurisdictions have pending bills or initiatives on privacy laws.

The EU and EFTA member States have agreed to adopt a new legal framework on the treatment of personal data (the General Data Protection Regulation (GDPR)). This paper is designed to share some of our learnings, and help explain the protocols we've implemented to comply with the GDPR.

October 2017

The GDPR Explained

The GDPR replaces the EC Directive 95/46 on Data Protection and will come into force on 25 May 2018. 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 EU citizens 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).

Some of the Requirements of the GDPR are set out over the following pages.

Individuals' Rights are Strengthened Under the New GDPR Framework and Include:

- **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.

Accountability and Governance

The new legislation creates an onus on companies to understand the risks that they create for others, and to mitigate those risks. Corporations are now having to demonstrate their compliance with the GDPR, so comprehensive, but proportionate governance measures must be put in place. Where it was advisable in the past to use good practice tools such as; privacy impact assessments and privacy by design, these are now legallyrequired for corporations that process a lot of personal data. All policies and procedures and employee training programmes will need to be reviewed and updated if necessary, as well introducing some new ones to comply with the GDPR. Each transfer of personal data will need to be recorded as Corporations will also need to appoint a Data Protection Officer, who will be first point of contact for supervisory authorities and individuals.

Breach Notification

A duty on all organisations to report certain types of data breach to the relevant supervisory authority within 72 hours, and in some cases to the individuals affected.

Fines/Risks of Non-Compliance

The risk of non-compliance is significant - An organisation, wherever located may be fined up to a maximum level of €20 million or up to 4% of its total worldwide annual turnover, whichever is higher. In addition to monetary fines, the damage to corporate reputation is negatively impacted.

What Specific Challenges does a Company Conducting Market Research have in Relation to Data Protection?

Every company has a duty to ensure they comply with all local laws in all the countries in which they operate, however as market researchers, we may be required to abide by a higher threshold, e.g. ICC/ESOMAR Guidelines and Codes of Conduct. New technologies have increased the volume and types of data available that need to be protected e.g. IP addresses, tracking technologies used to store data e.g. by the use of cookies or pixel tags, so personal data is collected by passive means as well as directly.

What are the ITWP Group of Companies Doing to Ensure 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. A team has been formed with the backing of ITWP Executive and Senior Management teams.

The business has already undertaken a data retention and data analysis exercise to understand:

- What data is flowing and mapping out the lifecycle of the flow of such data.
- Who has access to the Personal Data and why, including understanding the legal basis for any such processing, in conjunction with reviewing our privacy policies.

We are conducting a gap analysis to understand if there are any gaps in our knowledge, processes, measures and/or procedures. This includes reviewing all our policies, procedures and programmes for:

- Security: Toluna is accredited with ISO 27001 for its IT applications and all supporting infrastructures are designed to adhere to ISO 27001 standards.
- Processing outside the EU: Toluna USA Inc., who provide all our hosting and backup services elected to self-certify to the EU-US Privacy Shield Framework administered by the US Dept. of Commerce.
- Individuals' rights
- Data retention
- Employee privacy policies
- Panellist privacy policies

Renewing and/or undertaking:

- Employee training programmes
- Suppliers
  - Supplier onboarding process (questionnaires, contract templates, quality etc)
  - Understanding our supplier's obligations under existing contracts.
  - Understanding what measures and processes they are undertaking to comply with the GDPR and what timescales they have on expecting to achieve compliance with the GDPR.
  - Discussing with suppliers the impact of GDPR on the services being performed.
- Clients - Reviewing existing and template client agreements.
- The appointment of a Data Protection Officer.

A Privacy and Business Impact Assessment, based on the principle of Privacy by Design is also underway. The ITWP Group is committed to the GDPR program, and is on track to be fully compliant for May 2018.

This document is intended to outline to the recipient challenges the ITWP business have identified regarding compliance with the GDPR and the steps taken by ITWP to comply with the regulations. It is not intended that the recipient should rely on this document for legal advice. Instead recipients should seek their own legal advice in relation to the matters referred to in this document.


Toluna
In touch with people