Are you ready for GDPR? Key things to know:

Consent - Whenever a data subject is about to submit their personal information, the data Controller (usually a company) must make sure that he/she has given their consent, that it is “freely given, specific, informed and unambiguous,” with Controllers using “clear and plain” language. Controllers must provide evidence that their processes are compliant in each case.

New Rights for Individuals - Data subjects have a "right to be forgotten" that requires Controllers to alert downstream recipients of deletion requests. Data subjects also have a "right to data portability" that allows them to demand a copy of their data in a common format. The GDPR also affirms their rights to request access to their data and those requests must be processed in a timely manner.

Privacy by Design and DPIA - The GDPR requires that data privacy be built in "by design" when new systems are developed. It also requires that a Data Privacy Impact Assessment (DPIA) be performed which systematically considers the potential impact that a project or initiative might have on the privacy of individuals. If potential privacy issues arise, the organization must mitigate them before the project is underway.

Data Privacy Officer - Organizations that regularly perform large-scale monitoring of data subjects must have a Data Privacy Officer (DPO) to oversee compliance efforts, i.e. a Controller’s relationships with vendors who process and store personal data, vendors’ security practices, and notification of data subject requests. The GDPR’s new "one stop shop" provision allows organizations with offices in multiple EU countries to have a "lead supervisory authority" acting as a central point of enforcement to avoid inconsistent directions from multiple supervisory authorities.

Contracts & Privacy Documentation - Controllers and Processors must review their Privacy Notices, Privacy Statements, and any internal data policies to ensure they meet the requirements under the GDPR. If a Controller engages third party vendors to process the personal data under their control, they will need to ensure their contracts with those Processors are updated to include the new, mandatory Processor provisions set out in Article 28 of the Regulation. Similarly, Processors should consider what changes they’ll need to make to their customer contracts to be GDPR-ready by May 2018.

Scope - While the current 1995 EU Data Protection Directive governs entities within the EU, the territorial scope of the GDPR is far wider, in that it will also apply to non-EU businesses who market their products to people in the EU or who monitor the behavior of people in the EU. In other words, even if you’re based outside of the EU but you control or process the data of EU citizens, the GDPR will apply to you.

Accountability and Penalties - Controllers and Processors must be able to demonstrate their compliance with the GDPR to their local supervisory authority. In the case of a violation, Controllers and Processors who mishandle personal data or otherwise violate data subjects’ rights could incur fines of up to €20 million or 4% of their global annual revenue (whichever is greater).

Reporting Breaches - Controllers must notify their country’s supervisory authority of a personal data breach within 72 hours of learning it, unless the data was anonymized or encrypted. Breaches that are likely to bring harm to an individual – such as identity theft or breach of confidentiality – must also be reported to the individuals concerned.

SurveyCTO
Powered by Dobility

What GDPR means for our users and the data they collect:

Current business practice

- A data-collection platform that allows users to encrypt their data with their own 2048-bit encryption keys. Nobody from Dobility can read that encrypted data, and in the event of a data breach on the Dobility server, that data would be effectively unreadable.
- Convenient tools to review and export encrypted data with your encryption keys, without requiring that we or any of our servers ever see those keys.
- An EU-based hosting option for all premium and enterprise subscribers. For those users, all SurveyCTO service, databases, and backups reside only in the EU.
- Software, server architecture, and internal processes for every subscription that maximizes data protection, far beyond industry standards, such as dedicating a separate memory and execution space and a separate back-end database.

As of May 25, 2018

- Collection of private or sensitive data on EU citizens without a signed GDPR-compliant Data Processing Agreement (DPA) will not be allowed.
  - A standard DPA will be available for premium and enterprise subscribers only, no option for free or lower-cost subscription plans. We will require that all subscriptions covered by a DPA be hosted on our EU infrastructure.
- Encryption keys must be configured for all data collection forms.
  - Form fields excepted from encryption coverage (those explicitly flagged as “publishable” for the purposes of server-side quality checks or easy publishing to outside systems) must never contain personally-identifiable or sensitive data.
- We will update our privacy policy, assign a Data Protection Officer (DPO), and implement other internal steps necessary to maintain compliance with GDPR requirements.

For more info, go to: http://blog.surveycto.com/surveycto_gdpr/