GDPR: Tips and Tools

Last Modified on 06/29/2018 12:37 pm EDT

The European Union's General Data Protection Regulation (GDPR), which comes into effect on May 25, 2018, is pushing organizations (private, public, and non-profit) to reconsider the ways in which they collect, store, use, and disseminate personally identifiable information (PII). DevResults has been working hard to make sure our policies and practices are in line with the new rules, and we have put together a few resources to help you and your organization prepare.

> Note: DevResults offers information as a resource, but none of this should be read as legal advice. We recommend you contact your lawyers to find out how GDPR affects you.

GDPR has a few key concepts and tenets that everyone should be aware of: consent, better data protection, and better data management.

Consent

GDPR says that data must be freely given, with specific, informed, and unambiguous consent from stakeholders. There are a few resources out there that can help you frame how you request consent from anyone you collect personal information from. MailChimp has one of the **best examples** and hits all the necessary points (and you can use their language even if you don't use MailChimp!). This **Medium post** also goes into granular detail on what you should and shouldn't include.

If you transfer and store PII on DevResults, you should be letting your beneficiaries know. Here's how you could describe DevResults in a consent form:

We use DevResults -- a software app -- as our monitoring and evaluation platform. We store your information on DevResults and use it to analyze and report on our program.

If you're considering updating your Privacy Policy to give stakeholders a better idea of the information you collect and how you use it, **GitHub's privacy policy** is a great place to start.

Data Protection

Making sure the data you are collecting from beneficiaries and stakeholders is protected is extremely important.

Pseudonymization: GDPR suggests that all personal data be "pseudonymized": encrypted in a way that assigns artificial identifiers (pseudonyms) to otherwise identifiable data. Pseudonymizing data allows you to apply an additional layer of security to protect the identity of your stakeholders.

You can pseudonymize data in Excel by creating a unique ID for each person in a separate file, password protecting that file, and saving it on a separate (also password protected) hard drive that only a few people have access to.

The University of Nottingham has also created a free pseudonymizer you could use.

Aggregation: While thinking about GDPR and how best to protect information, it's also worth having an organization-wide conversation about how much information you need to collect and store, and how granular that data needs to be. Do you need to collect information from each household, for example, or can you collect more aggregated information at the village level?

Password management: Never store unencrypted or plain text password on your computer or in a shared drive. If possible, also avoid reusing passwords for different sites. Using a password manager like LastPass (this is what DevResults uses) or 1password allows you to use shared passwords as a team and keep records of who accessed certain information and when they accessed it.

Harddrive encryption: If you're holding a lot of sensitive data on your harddrive, you may want to encrypt it. BitLocker is a good option for Windows users and Macs come with a built-in encryption tool called FileVault .

Personal security: Protecting your own data is as important as protecting that of your beneficiaries. You should enable multi-factor authentication everywhere you can, make sure you're downloading software updates regularly (most of them have security fixes and patches), and install browser extensions like HTTPS Everywhere and Privacy Badger .

If you work in fields or regions that require additional security, consider using the Signal app for communication, DuckDuckGo as your search engine, the TOR browser , and a VPN (note: do not use a VPN you don't trust.)

Data management

Making sure your organization has excellent data management practices is critical to GDPR compliance. You should conduct a full data audit and create a data map showing what data you have, where it's stored, and who has access to it. The Engine Room has an example of a simple data audit spreadsheet template .

Conducting a Data Protection Impact Assessment (DPIA) to help you identify and minimize any data protection risks at the project level is also good practice. The UK Information Commissioner's Office has a checklist you can follow , and the Commission Nationale de l'Informatique et des Libertés has developed a free DPIA tool you can use.

If you have any questions or comments about the tools listed here, or if you would like to talk to us about how we protect your data, please read our Privacy and Security statements or reach out to us at privacy@devresults.com

Didn't answer your question? Please email us at **help@devresults.com** .

Related Articles