ClickDimensions

Preparing for GDPR Compliance

Data privacy, and the protection of it, is a growing concern among individuals, businesses and governments worldwide. When it goes into effect on May 25, 2018, the European Union's (EU) General Data Protection Regulation (GDPR) will be the latest legislation to address that concern. The GDPR is also expected to bring about significant changes in the way organizations process, store and protect the personal data of their customers.

What is the GDPR?

The GDPR replaces the 1995 EU Data Protection Directive, and significantly broadens the scope of data privacy in the European Union. In the wake of countless data breaches, the new law aims to greatly strengthen the rights of EU residents when it comes to the privacy of their personal information. It establishes a wide range of new regulations on organizations who collect or process the personal data of EU residents. It also imposes harsh penalties for violations or non-compliance.

Article 5 of the GDPR outlines the six key principles of the legislation:

1. There should be transparency into how collected data will be used.
2. Data should only be used in the manner specified when it is collected.
3. The data collected should align with why it is collected.
4. Collected data must be kept up-to-date and accurate.
5. Data should only be stored as long as necessary for its specified purpose.
6. Data should be processed in a way that ensures security of that data.

Does the GDPR apply to my organization?

While the GDPR is European Union legislation, given the global nature of business today, the GDPR reaches far beyond just organizations operating in the EU. The GDPR applies to any organization who collects or processes the personal data of EU residents regardless of where that organization is located or where the data is stored. In short, if you have even a single contact in your database who resides in the EU, your organization must comply with the GDPR.

Information contained in this document should not be considered legal advice; it is for informational purposes only. Consult your compliance department or legal counsel for specific guidance.

What kinds of data are protected under the GDPR?

The GDPR has a broad scope when it comes to the types of personal data protected, which includes:

- Basic identifying information such as name, mailing address and email address
- Web data such as location, IP address and cookie data
- Health and genetic data
- Racial, ethnic and cultural data

What are the penalties for violating the GDPR?

The GDPR enacts steep penalties for misusing or mishandling personal data. Violations can ultimately cost businesses up to €20 million or 4 percent of global annual turnover, whichever is higher.

How can my business prepare for GDPR compliance?

With the GDPR set to take effect on May 25, 2018, impacted businesses are scrambling to ensure that they comply with the new regulation. Here are steps your business can take now to prepare:

1. **Create a sense of urgency from the top down.** To emphasize its importance, company leadership should drive GDPR awareness and preparedness. While there are still months to go before the legislation takes effect, a sense of urgency driven by company leadership now can help ensure that your organization is ready when it's time to comply.
2. **Establish a task force.** In addition to leadership involvement, many different departments within an organization will need to help prepare for and comply with the GDPR. To that end, create an interdepartmental task force that is made up of members from IT, marketing, sales, operations, accounting and any other business function that collects or handles customers' personal data.
3. **Perform a data audit.** What personal information do your currently hold in your database? Where did it come from? Who do you share it with? These are all questions you should ask when looking at the current state of personal data within your organization, and will be required knowledge for GDPR compliance. Age is also an important consideration in a data audit. The GDPR requires special protection for children's personal information, so it is important to be aware of whether those requirements apply to your business.
4. **Review privacy policies.** Take the time to review existing privacy policies and determine if changes are necessary in order to be in compliance with the GDPR. While some organizations may find that their privacy policies already comply, the GDPR does include new requirements about how

privacy policies are worded and stating why your organization is collecting certain information, among other provisions. You can review information about privacy policy requirements under the GDPR here.

5. **Consider incident response.** Preparedness for data breaches becomes even more urgent with passage of the GDPR. Once in effect, the new regulation will give organizations 72 hours to report data breaches. Ensure that you have procedures in place to detect, report and investigate such incidents.
6. **Form a plan and timeline.** Once you have surveyed the current data collection and protection landscape within your organization, it's time to create a concrete and comprehensive plan for GDPR compliance. Focus on who will do what and by when. Be sure that your plan also includes milestones that will ensure compliance by the May 25, 2018 deadline.
7. **Create a process for ongoing compliance.** While initial preparations for the GDPR going into effect will require most of the heavy lifting in terms of compliance, it won't be a set-it-and-forget-it initiative for organizations. Put policies and processes in place to ensure ongoing compliance and be sure to consider how new business structures or initiatives may be impacted by GDPR.

What is ClickDimensions' role in its customers' GDPR compliance?

For purposes of providing our services to our customers, ClickDimensions is a data processor under the GDPR and will be required to meet all requirements imposed on data processors under the regulation. Our customers are considered data controllers and are responsible for their compliance with the law. And, finally, we are also considered to be a data controller when we market to our own customers and prospects, and we will ensure our own marketing practices meet the requirements.

What are ClickDimensions' responsibilities under the GDPR?

Our primary responsibilities as a data processor are to ensure that our operating policies and practices, and our product and platform adhere to GDPR requirements. Also, we are working hard to offer our customers features that help them in their efforts to be GDPR compliant. While this isn't a requirement of the GDPR and the technology itself can't ensure your compliance, we are committed to providing the best marketing platform for Microsoft Dynamics 365. Part of that commitment is providing tools that make it easier and more efficient for our customers to manage their compliance with privacy directives and legislation such as the GDPR.

What is ClickDimensions doing to ensure its compliance with the GDPR?

We have spent months working with our general and external counsel to prepare a plan for our own compliance with GDPR requirements. In short summary,

ClickDimensions will be making the following changes to our products, processes and policies in preparation for the GDPR:

- **Disclosures.** Updates to our privacy policy and other terms on clickdimensions.com.
- **Data subject rights.** Creating a process where ClickDimensions customers can request details for a data subject (an EU resident) and then execute a range of actions including deleting all records of that data subject from our systems.
- **Security.** While our systems already have a high standard of security and benefit from the Microsoft Azure platform, we are completing a rigorous audit of our security practices, processes and platform. We are continuously enhancing these practices to account for new technologies and to address new threats.
- **Communication.** We will update our breach notification process to ensure full compliance with the GDPR's requirements to enable our customers (as data controllers) to notify the appropriate authorities and data subjects concerning any data breach in events where notification is required by the GDPR.
- **Cross-border data sharing.** In addition to our existing certifications under the EU-US and Swiss-US Privacy Shield, and our commitments to comply with the EU Model Clauses, we are creating a new Standard Data Processing Agreement for more direct compliance with the GDPR.

Where can I learn more about the GDPR?

You can access the full text of the GDPR here. The Justice section of the European Commission's website also offers many GDPR resources including FAQs, fact sheets, press releases, public opinion surveys and more.

If you are a current ClickDimensions customer and you have a question about ClickDimensions' compliance with GDPR or other privacy regulations, you can reach out to your account manager or contact us at security@clickdimensions.com.