Virtual Water Cooler Chats

Marianne Pelletier, Marianne@Staupell.com

Gregory Duke, Greg@Staupell.com

Patti Patel, Patti@Staupell.com

August 12, 2020

Staupell Analytics Group

GDPR: What you need to know

What is GDPR?

- Regarding data held either *within* or *about citizens/residents* of the European Economic Area

- Each country (whether it's still in the EEA or not) has its own version of GDPR
  - Administered by each country's ICO (Information Commissioner's Office)

What is GDPR?

- General Data Protection Regulation

Why does each of these words have an important meaning?

What does GDPR decree?

- GDPR requires nations, businesses, and organizations to **process** the data of EU citizens and residents only when there is a **lawful basis** to do so

- “Process” in this context really means any use of data up to and including simply holding the data in a database

What does GDPR decree?

- For most nonprofits, the most common lawful basis for data processing requires that the EU citizen or resident **opt in** by providing an **affirmative consent**

- "Opt in" - The citizen or resident must agree to the processing in writing or by other method (for example, by checking a box on a website)
  - Not responding to the question/request is not considered affirmative consent

What does GDPR decree?

- Some other examples of “lawful basis”

- To process a gift or for tax concerns
- To process a purchase or event attendance
- To prove education or professional credentials

What happens if GDPR rules are breached?

- There is a “process” of escalating punishment for personal data breaches, beginning with written warnings and ending with fines

- For the eight months from May 2018 to January 2019, 59,000 GDPR breaches were reported to various ICOs, but only 91 fines were levied (and none of those were paid by nonprofits)

- Having said that—there is nothing stopping an ICO from going directly to a fine for an egregious breach

What happens if GDPR rules are breached?

- "Up to and including a heavy fine": maximum fine of €20 million *or* 4% of an organization's annual worldwide revenues, whichever is higher

- Note that each country in which a breach occurs can levy its own fines; so if rule are breached in France, Germany, and Italy each country can levy the maximum fines (so up to €60 million and 12% of the organization's annual worldwide revenues)

Question 1: “Are we going to be fined?”

- A lot of organizations in the US and Canada were scared of this when GDPR went into practice!

- At the time the EU hadn’t emphasized the “sliding scale of punishment”

Question 1: “Are we going to be fined?”

- Based on previous ICO actions in various countries, the answer is probably going to be “no”
  - Although some countries seem quicker to levy fines than others; the UK has been most proactive
- ICOs appear to be looking at how large and how egregious a breach is before even considering fines

Question 1: "Are we going to be fined?"

- That's not to say that you should ignore GDPR
- If you put more effort into following the regulations, ICOs will treat your case more fairly
- On the other hand—as in the case of the Austrian sidewalk—a country's ICO might consider making an example of you if you blatantly ignore the rules

Question 2: “How do we ask people if they want to be contacted if we can’t process their data?”

“That’s one heck of a catch!”

Question 2: “How do we ask people if they want to be contacted if we can’t process their data?”

- The answer to this hinges on the difference between a *law* and a *regulation*

- *Law*: “You can’t do X and if you do, you’ll get punishment Y.”

- *Regulation*: “We want situation A to occur, so you need to do actions B, C, and D. If situation A isn’t occurring, we’ll look at what actions you have been doing and consider punishments E, F, G.”

Question 2: “How do we ask people if they want to be contacted if we can’t process their data?”

- In short: you can perform an action to conform with the regulation

- So you can use data and contact someone to request permission to process data, but ONLY to do so—you can’t use that contact to try to fundraise or suggest that opting in will confer “special benefits” (you can only explain what information the constituent will expect to receive)

- You also must be respectful of the constituent’s time and privacy—i.e. don’t send follow-up correspondence every few weeks [this is spelled out in Recital 32]

Question 3: “What do we do if there’s a data breach?”

- You may have heard about a company whose name sounds like a bird, whose product sounds like something you might find on a bathroom sink, that had a breach lately

Question 3: “What do we do if there’s a data breach?”

- In their case, it appears that the ICO (at least in the UK) knew about the breach before either the company’s customers or the persons whose data was exposed.
  - Whether this was right to do from a PR standpoint…it’s probably right to contact the ICO first
- Under GDPR rules, any data breaches must be reported to the relevant country’s (countries’) ICO within 72 hours
- That might mean you have to report a data breach before you’re absolutely sure whose data was breached

Question 3: “What do we do if there’s a data breach?”

- Under GDPR regulations, data breaches aren’t just caused by criminal organizations or hacks—they can be the result of:
  - Accidentally sending personal information to the wrong person
  - Accessing files that aren’t relevant to their job function
  - Sharing information with someone outside the organization
  - Losing a device, such as a laptop, that contains personal information
  - Failing to secure information online, making it publicly available

Question 3: “What do we do if there’s a data breach?”

- GDPR does remind us that:
  - Every organization must have a plan in place for a data breach
  - When there is a data breach, it’s often best to step back and consider the situation before informing affected customers. It’s important to inform them quickly, but it’s more important to provide them with the right information

Question 4: “How can we find good information about GDPR?”

- First of all, it’s worth the time to go directly to the source: https://www.gdpreu.org/
  - The two pages you’ll really want to read are “Overview” and “Key Concepts” (the second is where we find that “process” of data under GDPR is the same as “hold” or “use”
- If you really want to dive into GDPR itself, there are two document repositories you’ll want to review:
  - The text of the regulation itself (“Articles”: https://gdpr-info.eu/)
  - Discussions of how the articles are used in practice (“Recitals”: https://gdpr-info.eu/recitals/)

Question 4: “How can we find good information about GDPR?”

- For US and Canadian organizations: this is a third-party website but it does seem to contain correct, easy-to-understand information: https://www.websitepolicies.com/blog/gdpr-canada-usa

What Are Your Questions?

Keeping in Touch with Us

- Marianne

  marianne@staupell.com
  @mpellet771

- Greg

  greg@staupell.com
  @GregEDuke

- Patti

  patti@staupell.com
  @pattiatstaupell