MCNAUL EBEL
NAWROT & HELGREN PLLC

GDPR FAQs

Alex Hecker
ahecker@mcnaul.com

Quick refresher

- GDPR - EU data privacy law effective May 25, 2018
- Imposes obligations on certain controllers and processors of personal data
- Obligations include:
  - Disclose privacy practices
  - Honor data subject rights
  - Report data breaches
  - Mandatory contractual provisions with processors

- Draconian fines: higher of up to 20m€ or 4% annual global turnover

GDPR FAQs since May 25th

Does GDPR apply to my business?

If you do either of the following to EU data subjects, then yes:

- offer goods or services
  - Example: Sales of products in euros
  - Example: Advertise your product in a language spoken in EU
- monitor their behavior
  - Monitoring ≈ tracking personal data (usually associated with profiling and behavioral advertising)

How are GDPR and US privacy laws different?

- Definition of a child is older under GDPR (<16) than under COPPA (<13)
- GDPR requires breach notification more often than US federal and state data privacy laws
- Definition of "personal data" much broader than similar protectable categories of information under US federal and state laws
- Companies must honor "data subject rights" (*e.g.*, rights of access, rectification, erasure, etc.)

Does X constitute personal data?

- If you're asking, it probably is
- "Personal data" defined broadly as "any information relating to an identified or identifiable natural person"
- Can include:
  - IP addresses
  - Email addresses
  - Name
  - Location

A security incident has occurred. Do we need to take action?

- If an exploitable security vulnerability was present—but no breach occurred—disclosure may not be necessary
- However, even if there was no "breach":
  - thoroughly document the incident; and
  - fix the vulnerability ASAP
- Three types of breaches that require notification:
  - "Confidentiality breach" - unauthorized or accidental disclosure of, or access to, personal data
  - "Availability breach" - accidental or unauthorized loss of access to, or destruction of, personal data
  - "Integrity breach" - unauthorized or accidental alteration of personal data

There was a breach. Do I need to notify our users?

- If a personal data breach occurred—and there's a risk to individuals' rights and freedoms—notify authorities
- Affected subjects should be notified "When the personal data breach is likely to result in a *high* risk to the rights and freedoms of natural persons"
  - Example: A direct marketing e-mail is sent to recipients in "to:" or "cc:" field, thereby enabling each recipient to see the email address of other recipients
- Notification should occur within 72 hours of becoming aware of breach

A banned player wants us to erase their data. Do we have to comply?

- GDPR gives data subjects the right to require controllers to delete their personal data
- However, there's likely an exception to this right where a company needs to retain personal data to enforce certain bans
- Companies are allowed to retain information that's the subject of a request for erasure in order to establish, exercise, or defend legal claims *(e.g.*, violation of terms of service)

McNaul Ebel

NAWROT & HELGREN PLLC