NAFEM Member Webinar
What you need to know about the General Data Protection Regulation (GDPR)
May 15, 2018
Welcome

Presented by:
Barbara Dunn, Partner, Barnes & Thornburg LLP
The GDPR – Quick Recap

• Regulates “processing” of “personal data” of EU residents
• “Processing” includes the collection, use, transfer, monitoring, tracking – even viewing of “personal data”
• Rights follow EU residents around the world
• MAJOR differences compared to U.S. law
• Massive compliance challenge for U.S. businesses
• No “grandfathering” provisions
• Significant fines for non-compliance – up to 4% of global revenue
• Remember May 25, 2018
Does GDPR Apply to Me?

• The answer is likely yes:
  – Customers residing in the EU
  – Meetings and tradeshows in the EU
  – Office in EU
  – Open for business to anyone residing in EU
  – GDPR definitely applies
Lawful Basis of Processing (Art. 6)

• All processing of personal data must be “lawful”
• Processing lawful only if one of the following applies:
  – Data subject has given **consent**
  – Processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party
  – Processing is necessary for the **performance of a contract** to which the data subject is party
  – Processing is necessary for compliance with a **legal obligation**
  – Processing is necessary in order to protect the **vital interests** of the data subject or of another natural person
  – Processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of **official authority** vested in the controller
Legitimate Interests

• **2 Part Test:**
  – Identification of “legitimate interests”
  – Balancing test weighing interests vs. fundamental rights and freedoms of data subject

• **May include:**
  – Direct marketing
  – Unsolicited non-commercial messages
  – Research

• **Legitimate interest must be:**
  – Lawful (i.e., in accordance with applicable EU and national law)
  – Sufficiently clearly articulated to allow balancing test
  – Represent a real and present interest (i.e., not speculative)
Consent (Art. 7)

• *Can* include technical settings, or other “conduct”
• *Cannot* include “silence, pre-ticked boxes or inactivity”
• Service can’t be conditioned on consent
• Specific to each operation, can’t be “blanket”
• Sensitive data needs “explicit consent”
• Consent for children (under age 16) is different!
EXAMPLE OF A GDPR CONSENT REQUEST
Scenario: A website requests consent to share data with a brand for product offers

Details of recipients and categories of recipients:
Text links to contact details of the controller and their data protection officer:
Article 13, para 1, a, b, and e.

Duration:
Article 13, para 2, a.

Can say no.
Recital v2.

Pop-up Dialog
We would like to share your browsing habits on our site with **Brand Name and their analytics partners**, to understand what offers may be of interest to you.

These data will be deleted after 6 months. You can withdraw permission at any time in **My Data**.

Learn more?

No
OK

Purpose of processing, and notification of profiling:
Article 13, para 1, c, and para 2, f.

Text links to tool for withdrawing consent:
Article 3, paragraph 3.

Text links to tool to complain to supervisory authority, and to access, correct, and transfer data, etc.
Article 13, para 2, b, c, and d.

https://pagefair.com/blog/2017/gdpr-consent/
Assess Data and Determine Lawful Basis – Legitimate Interest (LI) or Consent (C)

- **Customers**: LI as to company; C as to third party use
- **Prospects**: LI as to company; C as to third party use
- **Former Customers – Recent Past**: LI as to company; C as to third party use
- **Former Customers – Long Past**: Purge data or obtain C
- **Vendors**: LI as to company; C as to third party use
Privacy Policy

• Detailed description of Company’s use of data
• Information as to Cookies and Use of Analytics
• Right to Be Erased/Forgotten
• Right to Data Transfer
• Data Storage
• Data Protection Officer
Vendor Contracts

Data Processing Agreements (DPA)

- Company as Controller
- Company as Processor
- Rights and Responsibilities
- Indemnification
- Sub processors
6 Things to Do Before May 25, 2018

1. Map Your Data and Divide into Categories (e.g., customer, prospect, former customer)
2. Determine Lawful Basis for Each Category (e.g., legitimate interest or consent)
3. Develop Consent Form and Process to Obtain Consent
4. Develop EU GDPR Compliant Privacy Policy for website
5. Develop and issue Data Processing Agreements
6. Check Cyber-liability Insurance
Ongoing Care and Feeding

• DPOs/Staffing: Determine whether DPO or new staff (e.g., CPO) needed. Hire, train, implement.
• Incident response plan for data breaches
• Document, document, document
• Ensure compliance with EU Resident request re their PD
• Make sure data coming in the door is “clean”
• Make sure data going out the door is “clean”
Questions

Your Questions
Resources

Company profile updates
Keep your Company and Personal Profiles up-to-date.
Read more »

Considering building or enhancing your company's government relations function?
Here's how doing so could help grow your business.
Read more »

SBA office of advocacy partnering with NAFEM
To stay abreast of regulatory changes and understand how they affect small businesses, the Office of Advocacy has teams of attorneys who cover specific government agencies and regularly engage with trade associations and companies nationwide. For example, Prianka Sharma, assistant chief counsel, joined NAFEM’s October 2017 Regulatory Roundtable.
Read more »
Additional Resources

- http://eugdpr.org
- https://easygdpr.eu/home/
- https://gdpr-info.eu/
Thank you!

Contact us:

dparker@nafem.org or +1.312.821.0205
info@nafem.org
www.nafem.org
+1.312.821.0201