feeding the minds that feed the world

Enhanced Data Protections & Regulations: Impact on IFT & Sections

Thomas G. Foley, CAE
VP, Membership & Customer Development

Terrence L. Merkley, MBA
VP, Information Technology

Today's Agenda

- What is GDPR?
- What is IFT Doing to Comply?
- How Does It Impact Sections?
- How Is Our Section at Risk?
- What should Sections Focus On?
- Questions

What is GDPR?

- Developed by the European Commission starting in 2012 to strengthen and unify data privacy protection across the EU.
- Approved in 2016; Enforceable (worldwide) as of May 25, 2018.
- Includes specific provisions for the handling of personal data of EU data subjects that is exported outside the EU.
- Imposes mandatory reporting for data breaches, duty to respond to EU citizens privacy rights, increased sanctions for noncompliance, revised consent criteria, and much more.
- Subjects all organizations that maintain and use European member or customer data to these regulations.

Common GDPR Questions

- **Who does the GDPR affect?**
- **What are the penalties for non-compliance?**
- **How does the GDPR affect policy surrounding data breaches?**
- **What are my responsibilities?**
- **What is the difference between a data processor and a data controller?**

Source: https://upload.wikimedia.org/wikipedia/commons/7/73/Global_European_Union.svg

Who is Affected by GDPR?

- GDPR applies not only to organizations located within the EU but it also applies to organizations located outside of the EU if they offer/provide goods or services to EU data subjects.
- It applies to all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company's location.

Source: https://upload.wikimedia.org/wikipedia/commons/7/73/Global_European_Union.svg

Key Definitions

The regulation covers the processing of “personal data” (e.g. name, phone number, member ID) that relates to “data subjects” (e.g. members) by or on behalf of a “data controller” (e.g. IFT or a Section).

- **Data Subject - An identifiable person is anyone who can be identified, either directly or indirectly, by things like a name, identification number, location data, online identifier, or data that relates to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.**

- **Data Controller - A controller determines the purposes and means of processing personal data.**

Key Definitions (more)

- **Data Processor - A processor is responsible for processing personal data on behalf of a controller.**

- **Personal Data - Personal data is any information that relates to an identified or identifiable natural person (the "data subject"). As a result, "personal data" would apply to much of the data that organizations like IFT holds on our members, prospects, former members, sponsors, donors, meeting attendees, etc.**

- **Special Data - Some personal data is categorized as special data by GDPR. This data is subject to greater restrictions, and includes data about religious or philosophical beliefs, health, racial or ethnic origin, trade union membership, political beliefs, and sex life or sexual orientation.**

Key Definitions (more)

- **Lawful Basis - GDPR defines six lawful bases for processing of personal data:**
  - To meet contractual obligations entered into by the data subject.
  - To comply with the data controller's legal obligations.
  - To protect the data subject's vital interests.
  - For tasks carried out in the public interest or exercise of authority vested in the data controller.
  - For the purposes of legitimate interests pursued by the data controller.
  - Consent
- **Consent - GDPR defines "consent" as: 'any freely given, specific, informed and unambiguous indication of the data subjects wishes". It is important to note that silence (i.e. pre-checked boxes or inactivity) does not establish consent.**

Key Principles of GDPR

- Data subjects own their personal data
- Organizations should keep only the personal data they need, only for as long as they need it, and only for the purposes indicated in their lawful basis.
- Data subjects have the right to request changes to the way an organization uses their personal data
- Organizations must respond to such requests in a timely way

Additional Principles of GDPR

- **GDPR also enforces a number of related principles regarding the handling of personal data:**
  - Lawfulness, fairness and transparency: Personal data must be processed lawfully, fairly and in a transparent manner.
  - Purpose limitation: Personal data must be collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
  - Data minimization: Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
  - Accuracy: Personal data must be accurate and, where necessary, kept up to date. Personal data that is known to be inaccurate is to be erased or rectified without delay.
  - Storage limitation: Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary.
  - Integrity and confidentiality: Personal data must be processed in an appropriately secure manner including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, by the use of appropriate technical or organizational measures.
  - Accountability: The data controller is responsible for, and has to be able to demonstrate compliance with, the principles stated above.

Major Requirements for Organizations

- Effective information security controls
- Rapid breach notification plan
- Maintain record of personal data processing activity
- Maintain record of requests from data subjects to alter or remove their personal data
- Conduct data privacy assessments for new initiatives
- More…

Penalties for Non-Compliance

- GDPR imposes stiff fines on data controllers and processors for non-compliance.
- Fines vary based on the severity of non-compliance. The most significant penalties are up to €20 million, or 4% of the organization's annual revenue, whichever is higher.

Data Subject Rights

- The GDPR provides the following rights for individuals:
  - The right to be informed
  - The right of access
  - The right to rectification
  - The right to erasure
  - The right to restrict processing
  - The right to data portability
  - The right to object
  - Rights in relation to automated decision making and profiling.

Source: Information Commissioner's Office
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

Top 5 Things for Sections To Do…..

1. Remain Calm! Exposure for IFT sections will be minimal

2. Understand who has access to your data

3. Understand your data!
    - What is being collected?
    - How is it being processed?
    - Is it necessary to business functions?

Top 5 Things for Sections To Do…..

4. Talk to your vendors - Understand how they use your data

5. Follow-up immediately with members who request to be forgotten or have specific questions on GDPR

We Don't Have Members In The EU….Does This Apply?

- **Regardless of GDPR requirements, many of the items we are discussing today involve best practices when handling member data!**
- **We also anticipate more regulations could be put in place domestically with restrictions similar to GDPR.**

  - *June 28, 2018: New York Times:*
    California Passes Sweeping Law to Protect Online Privacy

    "California has passed a digital privacy law granting consumers more control over and insight into the spread of their personal information online, creating one of the most significant regulations overseeing the data-collection practices of technology companies in the United States……The legislation, which goes into effect in January 2020, makes it easier for consumers to sue companies after a data breach. And it gives the state's attorney general more authority to fine companies that don't adhere to the new regulations."

Additional Resources

Here are some additional resources where you can learn more about IFT's Privacy Policy & GDPR:

- IFT Privacy Policy
  http://www.ift.org/About-Us/Privacy-Policy.aspx
- Forbes - *Three strategic realities for CIOS as the GDPR Deadline Draws Near*
  https://www.forbes.com/sites/forbestechcouncil/2018/01/24/three-strategic-realities-for-cios-as-the-gdpr-deadline-draws-near/#1e32ccbbb806
- ASAE/Associations Now: 4 Data Issues TO Act On Now, As GDPR Looms
  https://associationsnow.com/2018/03/4-data-issues-to-act-on-now-as-gdpr-looms/
- EU GDPR Informational Portal
  https://www.eugdpr.org/
- IHasco GDPR Essential Online Training:
  https://www.ihasco.co.uk/courses/detail/gdpr-training

Questions