GDPR Is Here: Are You Compliant?

Bonnie Yeomans
Special Privacy Counsel
June 12, 2019
General Data Protection Regulation (GDPR)
What is the GDPR?

• A regulation agreed upon by the European Parliament and Council in April 2016.
• Came into effect May 25, 2018.
• Harmonizes privacy laws across the EU.
• Replaces Data Protection Directive 95/46/EC as primary law regulating how companies protect EU residents' personal data.
• Companies had 2 years to put processes and procedures in place to comply.
GDPR and Charitable Organizations

- The GDPR applies to organizations (including charitable ones) that process “personal data,” regardless of their size.
  - *The most commonly owned personal data by charitable organizations is the data concerning*
    - donors or potential donors,
    - beneficiaries of the charity’s programs,
    - volunteers, and
    - more generally, any individual who interacts with the charity (employees, consultants, external service providers, etc.).
The definition of personal data is so broad that all charitable organizations necessarily process personal data.

If your organization is located in the European Union (EU), the GDPR applies.

For organizations not located in the EU, the GDPR will also apply to them if they

- offer goods and/or provide services to EU-based individuals, or
- monitor the behaviors of EU-based individuals.
• It is irrelevant that payment is/is not required for the goods or services.
  
  – Example: U.S. charitable organization which, as part of its activities, helps Syrian refugees based in France would need to comply with the GDPR, as it provides services to individuals based in the EU.
Penalties under the GDPR

• Penalties are technically the same for all organizations
• For the most serious instances of non compliance, organizations may be fined up to 4% of the organization’s annual revenue or €20 million, whichever is greater.
  – *It seems unlikely that the regulatory authorities would sanction charitable organizations with such high amounts.*
• Non-compliance with the GDPR will have a reputational impact on a charitable organization and risk losing the trust of supporters and donors.
Risk-based Approach to Compliance?

- Many companies were not 100% compliant by May 2018, and are not still.
- Partial compliance better than no compliance.
- Factors to consider:
  - Burden/cost of particular GDPR requirement.
  - Likelihood of enforcement of particular requirement in this circumstance.
  - Applicable fines associated with non-compliance.
  - Customer facing elements.
Top 10 GDPR Compliance Challenges
Data Mapping – A Good Place to Start

• The first step towards compliance is to identify the type of personal data handled by your organization (data mapping).

• As questions such as:
  – *What categories of data is my organization handling?*
    – human resources-related data, personal data with respect to donors, volunteers, and the beneficiaries of the organization’s programs, etc.
  – *For each category of data, what kind of data does my organization have?*
    – name, phone number, personal address, email address, photo, etc.
Data Mapping – A Good Place to Start (cont’d)

- When and how is the data collected and used, and for how long is that data retained?
- Does my organization handle any sensitive data?
  - Sensitive data includes health data, data regarding sexual orientation, data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs and trade union membership, as well as any genetic and biometric data.
- For what purpose is the data collected and used (human resources related obligations, fundraising, organization of events, volunteer management, etc.)?
Is that data shared with any third party?
- If so, where is that third party located?
- Is the data hosted in that country?
- Is the third party under an agreement to protect the data?
  - Data breach notification
  - Data retention
  - Data subject requests
Top 10 GDPR Compliance Challenges

• (1) Data Retention
  – Must keep personal data only for as long as necessary to fulfill the original basis for collecting and processing it
    – Unless additional consent is obtained
  – Prolonged storage permitted if personal data is anonymized
  – Data mapping and inventory efforts must be prioritized
  – Prioritize personal data that will present the greatest risk to the data subject if kept beyond permitted time period
  – Keeping too much data can lead to problems
Top 10 GDPR Compliance Challenges (cont’d)

• (2) Direct Marketing
  – Electronic marketing is regulated by both GDPR and EU’s ePrivacy Directive (soon to be a Regulation)
    – GDPR provides several ways to legally use data
    – Direct marketing under the ePrivacy Directive is allowed only if the individuals receiving the communication have given their prior consent.
  – Do not need consent if the services or products advertised in the communication are similar to those that the individual has purchased in the past.
    – This rarely applies to charitable organizations, as they typically are not in the business of selling products or services
Top 10 GDPR Compliance Challenges (cont’d)

- Company may have legacy databases of contact information, but Company has not obtained consent since GDPR implementation
  - Consent has to be specific, informed, freely given, and must be an unambiguous indication of the individual’s agreement to the processing of his or her personal data.
  - Assess whether consent obtained pre-GDPR implementation was given in line with the standards of the GDPR
    - If it was not, GDPR-standard consents must be obtained
    - Unless “legitimate interest” (GDPR) and existing business relationship, and offer of product or service that was purchased in past (ePrivacy)
Top 10 GDPR Compliance Challenges (cont’d)

• (3) Compliance for a Global Group: EU Rights to EU Data Subjects, or EU Rights to All?
  – *Does GDPR require rights to be extended to natural persons all over the world?*
  – *Assess whether it is operationally feasible to treat EU and non-EU data subjects differently*
Top 10 GDPR Compliance Challenges (cont’d)

• (4) Responding to Data Subject Access Requests (SARs)
  – How expansively should companies respond to SARs?
  – How to verify identity of requestor
  – How to vet legal backing of request
  – Timeliness of response
  – Doesn’t matter if the request comes from a “good place” or is someone just trying to make trouble or to do discovery in preparation for litigation
Top 10 GDPR Compliance Challenges (cont’d)

• (5) Heightened Requirements for Certain Categories of Personal Data
  - Race, ethnicity information is “sensitive information” subject to heightened GDPR requirements
  - Ensure all employees and vendors trained on cybersecurity awareness
  - Do not retain this data if not needed
Top 10 GDPR Compliance Challenges (cont’d)

• (6) Data transfers outside the EEA
  – Transfer of personal data to recipients outside the EEA is generally prohibited unless:
    – The jurisdiction in which recipient located is deemed to provide adequate level of data protection
    – The data exporter puts in place appropriate safeguards
    – A derogation or exemption applies (e.g., Privacy Shield, model contract, binding corporate rules)
  – Review existing circumstances in which personal data is transferred outside of EEA and ensure data transfer mechanism complies with GDPR requirements
Top 10 GDPR Compliance Challenges (cont’d)

• (7) Data Breach Notification
  – Notice required to regulators if there is a “risk to the rights and freedoms of the individual; notice to individual if there is a “high risk to the rights and freedoms”
  – GDPR notification obligations require notifying data protection authorities within 72 hours of becoming aware of a data breach
  – “Becoming aware” means having a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised
  – Emphasize prompt action to investigate the incident
  – Plan ahead with a security incident response plan/ Table tops
Top 10 GDPR Compliance Challenges (cont’d)

• (8) Vendor Management Protocol
  – Companies are responsible for third parties to whom they entrust EU employee data and customer data.
  – Controllers must monitor vendors to require that they process data in accordance with applicable requirements.
  – Vendor must secure data and notify company in the event of a breach.
California Consumer Privacy Act of 2018
EU’s GDPR and CA’s CCPA

- Two similar, but different, laws
- GDPR enforcement began May 2018; CCPA: 2020
- Substantively overlapping, but only partially
- Overlapping substance is still different in detail
- Each law requires things that are not required by the other
Comparison to GDPR

**GDPR**
- Record retention policy
- Information security policy
- Incident response plan
- Direct marketing compliance
- Data protection officer
- EU local rep
- Data protection impact assessments
- Data exports

**Both**
- Data mapping
- Documentation of data processing
- Privacy policy updates
- Data subject request procedures
- Addendum to service provider agreements
- Personnel training

**CCPA**
- Back-end compliance (e.g. de-identify PII)
- Review consumer contracts (e.g. website terms)
- Pay for privacy
CCPA Overview

• Becomes effective January 1, 2020; enforcement begins: July, 2020
• Territorial reach: for-profit businesses that collect and control California residents’ personal information, and:
  – (a) have annual gross revenues in excess of $25 million; or
  – (b) receive or disclose the personal information of 50,000 or more California residents, households or devices on an annual basis; or
  – (c) derive 50 percent or more of their annual revenues from selling California residents’ personal information.
• “Doing business in California” = red herring
CCPA Overview (cont’d)

• The Act also draws in corporate affiliates of such businesses that share their branding.

• CCPA gives consumers 4 basic rights:
  – 1) right to know what personal information a business has collected about them, where it was sourced from, what it is being used for, whether it is being disclosed or sold, and to whom it is being disclosed or sold;
  – 2) right to “opt out” of allowing a business to sell their personal information to 3rd parties;
CCPA Overview (cont’d)

– 3) the right to have a business delete their personal information (with some exceptions); and
– 4) right to receive equal service and pricing from a business, even if they exercise their privacy rights under the CCPA.
Key GDPR Principles for Charitable Organizations
Key GDPR Principles

• (1) Limit personal data processing
  
  - The GDPR provides that personal data needs to be obtained only for specified and lawful purposes.
  
  - For example, in order for a charitable organization to manage the payment of its members’ contributions, the organization is justified in collecting the names and contact information of its members, and in keeping such data for the duration of the membership.
Key GDPR Principles (cont’d)

• (2) Inform
  - **GDPR emphasizes transparency**
    - Organizations must inform the individuals what data they have in a concise and intelligible way, and in plain language.
    - *For instance, a privacy policy should be short and explanatory, and a link to it should be included in all of the organization’s communications.*
Key GDPR Principles (cont’d)

• (3) Ensure that data subjects’ rights are respected
  - Under the GDPR, individuals have the right to ask confirmation as to whether or not personal data concerning them is being processed, and where and for what purpose.
  - They are also entitled to object to the processing of their data, have personal data rectified if it is inaccurate or incomplete, and to request the deletion or removal of personal data.
  - Organizations should designate a reference person who will answer all potential requests.
Key GDPR Principles (cont’d)

• (4) Ensure the security of personal data
  – The GDPR requires personal data to be processed in a way ensuring its security.
  – Charitable organizations have to ensure that appropriate technical or organizational measures are being used to protect personal data against unauthorized or unlawful processing and against accidental loss, destruction or damage.