# 23NTC Collaborative notes

# The ABCs of Data Privacy

**Session feedback**

**Link to session slides:**
The_ABCs_of_Data_Privacy_NTEN_2023_Allison_Jai_ODell.pdf

**Speakers and The_ABCs_of_Data_Privacy_NTEN_2023_Allison_Jai_ODell.pdfcontact info:**
Allison Jai O'Dell
Director, Data and Information Technologies
The Funders Network
allison@fundersnetwork.org
ajodell@gmail.com
https://linkedin.com/in/allisonjai/

**Speaker provided session material and resources:**
See slide-deck for hyperlinks

---

## Attendee collaborative Notes

*Attendees are invited to make notes and share resources related to this session.*

Experience with GDPR coming out in 2018, legal teams interpreting: Allison as Database Manager and Data manager to figure out the implementation side of things. Background is not a lawyer, but as a technologist, so focus is on implementation today

Contextualizing importance of data privacy - though it may not medical data, the combination of data can pose risks.

- "We kill people based on metadata" - Michael Hayden, former director of NSA and CIA.
    - *Quotation from linked article: … metadata alone can provide an extremely detailed picture of a person's most intimate associations and interests, and it's actually much easier as a technological matter to search huge amounts of metadata than to listen to millions of phone calls.*

Employees are the biggest data security risk

- Scenario: Planning a donor event, sending a spreadsheet with constituents. Loaded up into foundation CRM. Communications lead exports from CRM to upload to Facebook for retargeting. However, constituents that opted in were for specific outreach and some may

have signed up from California, which has stricter privacy protections.

More likely to encounter hacking activity in a coffee shop or a charging station than at home, or encounter something like a hack to your website.

CAN-SPAM:

- Sending through personal address doesn't exempt - only matters that you're sharing marketing content
- Offer unsubscribe options and do so in a timely manner

State privacy regulations are arising and they're CPRA-esque (California Consumer Privacy Act), e.g. Virginia, Colorado, Utah

GDPR

If you have more than 1 constituent in your database in Europe then GDPR applies

1. Lawfulness, fairness and transparency - don't do anything sneaky and tell folks how you plan on using their personal data
2. Purpose limitation: only process data for the reasons that you specified when you collected it and when your goals shift, give people the opportunity to opt out
3. Data minimization: only collect and maintain the data that you need. E.g. if you aren't doing text-banking campaigns, stop collecting cell phone numbers
4. Accuracy: You have a duty to keep personal data accurate and up to date, e.g. check national change of address registry, giving folks an opportunity to update, if you're not using the addresses, do you need to keep it?
5. Storage limitation: only store personally identifiable information for as long as necessary.
6. Integrity and confidentiality: You must ensure that you have appropriate security measures in place to protect the personal data you hold.
7. Accountability: Data controllers are responsible for demonstrating that they are in compliance

It lays out what organizations are expected to do in addition to rights.

1) Right to be informed - providing individuals with clear and concise information about what you do with their personal data
2) RIght of access - to be able to reach out and ask what data do you have on me?
3) Right to rectification: self-serve, to be able to update and notify
4) Right to erasure : right to remove information
5) Right to restrict processing : right to indicate, hey, do this, not that with my data
6) Right to data portability: receive an export of data, take to another platform
7) Right to object: to file an appeal or complaint to say organization is not honouring

PIPEDA - Canada's Personal Information Protection and Electronic Documents Act

PIPL - China's Personal Information Protection Law

Core components of a Data Privacy Policy

- Transparency
- Contact information - set up a separate email address to ensure that it can be monitored and managed
- Opt Out / In Instructions - can be during sign up of programs, explicit consent

- Children under 13 years of age

Implementation of a Data Privacy Policy

Inspiring Trust

Starting with a data security audit
- Sketch out what personal data organization has, where it's kept, where it comes from, where it goes, etc.
- Sample Data Security Audit Example

| | |
|---|---|
| Data Group | Donation Records |
| Who Uses It | Development Team; Marketing Team |
| How It's Used | Thank donors; Cultivate future gifts; Determine success of giving campaigns and plan future strategies; Generate IRS Form 990 |
| Where It's Stored | GiveLively; Salesforce CRM |
| How It's Protected | Only Development Managers and System Admins have access to GiveLively and Salesforce Opportunity records; Both platforms require Multi-Factor Authentication for login |

# Questions from the Chat

### Question: It seems like website cookie popups are not truly achieving our goals of getting real informed consent. Is there an alternative? Do we just have to do it for compliance purposes even though they are so annoying?

### Question: How secure is Google Drive? My staff seem to loooove using Google Drive. I'm trying to steer them toward using SharePoint, because it is monitored by our IT consultant, while Google Drive is not, and I think it is more secure. How worried should I be about folks relying on Google Drive?

- Generally, 50% can be automated and controlled, and 50% will require more “hand holding” and working with individuals
- Different platforms allow different levels of control, such as preventing certain users from downloading items
- Monitor usage reports. Engage individuals one-on-one and talk about the issue.
- Even if you can’t manage everything, you can still have an impact.

## Question: There are so many regulations by so many governing bodies and governments. Some claim to apply to anyone who may have info about someone who submitted it while in their country. How in the world could any of these regulations be enforced?