DATA MINIMIZATION TOOLKIT

Credits: *This data minimization toolkit was developed in 2022 by the Apra Ethics and Compliance's subcommittee members Lauren Banovz, Megan Horton, Deb Michling, Laura Owen, Jennifer Schlager, and Gisela Simental. In June 2023, edits and updates were made by Apra Ethics and Compliance's committee members Elizabeth Goodman, Erin Osborn, Laura Hout, Katherine Kneebone, Deb Michling, Jennifer Schlager, Sierra Bulson, and Madhu Vishnu. Special thanks to the Apra Board of Directors for their guidance and thoughtful edits.*

INTRODUCTION

Organizations make decisions based on data every day. Demographic information helps us target specific groups of constituents for annual appeal mailings. Wealth screening data helps us prioritize prospects for major gift solicitations. Data helps us answer questions daily--but we also need to ask questions about the data that we use: What do we do with data that has been in our database for years with no updates or source information? How long do we store wealth data? What information should we keep in contact reports? These questions focus on data minimization. This toolkit will define data minimization and deliver best practices for maintaining important relevant information while respecting constituent privacy and preferences.

What is data minimization?

Data minimization refers to best practices that ***strategically delimit*** the storage, collection, and retention of personal data relevant and necessary to accomplish fundraising goals.

There are many benefits of minimizing data.

- To comply with legal requirements: in an era of an increasing number and variety of privacy laws, minimizing what is in our databases helps comply with regulations. The implementation of **GDPR** set a privacy standard that is likely to be repeated in future laws throughout the world, including the right to be forgotten and the right to own personal data.
- To minimize or decrease cost: data storage costs money and it can be expensive to store data indefinitely. Fewer records and digital files reduce the overall cost.
- To minimize data breaches and data loss: decreasing the amount of data that can be exposed lowers the risk to organizations.
- To maintain best practices: practicing good data hygiene will make your organization's fundraising more effective and efficient; it will be easier to find relevant and up-to-date information more quickly.
- To be respectful of constituents: data minimization shows our constituents that we take care of their personal information, following **The Donor Bill of Rights**.

Data Environment

Before beginning a data minimization process, it is important to review and evaluate your data's environment. The following aspects should be considered (this is also necessary when creating internal data processes).

- **Data Inventory:** What information is being collected in your database? This includes basic information, but also what is captured in contact reports, proposals, profile notes, etc. Consider what is currently captured vs. what needs to be recorded.
- **Data Access:** Review who has access to the data and who needs access to the data. Can permissions vary by role?

- **Track Where The Data Goes:** Review who has the right to export data. What is included in those reports? What Personally Identifiable Information (PII) is included in reports? How long are exported reports saved or stored?
- **Third Parties:** What third parties or vendors are you using to acquire data? What are their data policies? Have they had data breaches? If so, how have they been handled? Is the data acquired from third parties ethically sourced? What data of yours is kept by the third party?
- **Legal Basis:** Do you have a justification for collecting or having data? GDPR provides **six legal bases** for processing data: consent, contractual, a legitimate interest, a vital interest, a legal requirement, and public interest.

When might we want to minimize data?

Regardless of the data management tool or CRM used by your organization, it is likely to contain a massive number of alumni, existing donors, prospective donors, patients, members, and other constituents. Data minimization also plays a role in managing an organization's risk profile: the less information that is stored, the less information there is to leak, or breach, therefore there is a lower chance of reputational damage.

Here are some best practices for data minimization of constituent records:

Age of Donor

- Inactivate records or add "no contact" markers as needed (check your organization's policies).
- Mark individuals over a certain age (e.g., 110+) as deceased/inactive.

Age of Record

- When was the donor's most recent gift?
- What was the last date of contact with the organization (excluding event invitations, attendances, etc.)?
- There are no set industry rules that prevent the deletion of constituent information. Determine whether your organization already has procedures in place; if not, a potential deletion policy could be removal of a record after 18 months of no contact.

Marriage Status/Divorce

- If both spouses are alumni, keep records.
- If one spouse is not an alumnus and has no giving recognition/credit, remove or inactivate the record. The record can be kept if recent interactions indicate the non-alum spouse is interested in giving.

Engagement of Prospect/Donor

- If an individual has specifically requested no engagement, mark their record as no contact and for exclusion from audit updates.
  - If a constituent in a GDPR-protected region wants their data deleted, organization must comply. GDPR also requires that organizations provide all data stored about them upon request by the data subject.
- If a constituent has not interacted with the organization in a certain number of years (e.g., 10 years), they could be marked as inactive.

Sensitive Data (healthcare or patient records)

- Record the least amount of information possible (e.g., date of visit, doctor visited, inpatient/outpatient).
  - If a customer is in a GDPR-protected region, sensitive data can only be recorded with consent from the individual
- Use the most generic practice or specialty area possible (i.e., Cardiovascular Department, Pediatrics Team, etc.).
- Do not include any information regarding the patient's diagnosis or treatment plan To the greatest extent possible, ensure that this data is never loaded into your database.

Legal Reasons/Criminal Record

- Ask your legal counsel if the organization has policies that disqualify a donor based on a criminal conviction and inactivate or delete these records accordingly.
- Minimize the amount of detail you put in the record. A note could include vague language and a link to the details if it is available (e.g., "Research recommends disqualification based on legal issues. See link provided.")

- Bankruptcies or active liens may prevent a donor from giving in the short term, but it may not permanently disqualify a donor. It is best to convey this information to a gift officer without adding it as a data point. The gift officer may wish to make an appropriately vague note in a contact report (i.e., do not solicit this donor for X period of time).

Financial Regulatory Requirements

- If your organization collects U.S. income tax records and underlying data, that information should be maintained for seven years, along with records of any securities transactions. Records of any businesses that file foreign tax returns should be kept for at least ten years.
- Consult with your financial or legal teams to determine how these requirements might impact data minimization.

Identity Data Points

- Consider data such as race, ethnicity, and gender identity. Check for invalid or outdated data points (e.g., previously not having a gender-neutral option) or if the source of the data points is unknown.
- Reach out to your organization's legal counsel and/or data privacy team to conduct a risk assessment about including this information. Inclusion could breach HIPAA, FERPA, or other privacy laws.
- Compile and maintain these points only if they have been ethically sourced; do not record this information based on inference (i.e., social media photos or event attendances).
- See Apra's **DEI Data Guide** for more information on identity data collection and storage.

When might we want to keep data?

The principle of "data minimization" means that an organization should only keep data on an individual when it is necessary for a particular purpose. We may wish to keep data to help enhance and deepen our relationship with a prospect or donor. It is important to keep a record of meeting notes and milestones, but we must remember to record this information with discretion and sensitivity.

An employee should keep in mind the Donor Bill of Rights and **subject access requests** (under GDPR), which allow an individual to view the information the organization holds about them. A prospect or donor should be able to view their record and find it **truthful, respectful, and relevant** to the values and mission.

The table below provides examples of the types of things you should and should not include about a person when recording information in your database or on your computer:

INCLUDE	DO NOT INCLUDE
Meeting attendees, date, and location	Racial or ethnic origin, religion, sexual orientation (guidelines for ethical storage found in the **DEI Data Guide**)
Visit purpose	Political views and/or trade union membership
Summary of interaction and details of any solicitation	Criminal conviction
Career history	Any HIPAA or FERPA protected information
Next steps	Sensitive or embarrassing information about the prospect
Recommendations	Personal opinions and value-based judgements (e.g., prospect going through a "bitter" divorce)
Personal and family affiliations and background	Names or specific details about minor children (**children's rights are protected under GDPR**)
Philanthropic interests	Inconsequential information (contact reports do not need to be verbatim accounts of conversations)
Relationships with faculty, staff, classmates, donors, and volunteers	
Indicators of wealth (art collections, vacations, second homes, children in private school, etc.)	

What are some of the circumstances in which you should keep data?

- Legacy data: it is often necessary to keep records of deceased donors for tax and legal purposes.
- Due diligence: it is useful to keep records of decision making and the decision itself when it comes to due diligence, so an organization can manage its risk profile effectively.
- Skeletal records of former major donors and prospects: recording the reason why a donor is no longer part of the organization's major donor program is important as it prevents unnecessary contact with the individual and causing harm to the relationship.
- Deleting data might make the records less accurate or useless for processing purposes particularly where legal, medical, or criminal purposes are concerned.

WHO HAS ACCESS TO THE DATA?

Along with minimizing the data itself, it is important to consider what policies your organization currently has in place regarding access to donor and prospect records in your CRM. Who has permission to edit, decease, or delete a record? What precautions have been taken to limit access to potentially sensitive personal or medical information? It is especially important for employees with these editing capabilities to receive appropriate training, in addition to conducting regular database audits to ensure that any data minimization activity adheres to your organization's guidelines.

System-wide Permissions

If a department or employee has access to your organization's entire database, it may feel like they wield complete control over donor data. Granting access to the system could theoretically grant access to unauthorized or inappropriate users to edit or delete whatever an individual employee wants. What protocols can be established to prevent this?

- Review your organization's training practices. What are the qualifications of the employees allowed to modify addresses, mark an individual as deceased, or completely delete records? Most organizations require multiple educational sessions before these permissions are granted within the system. Consider limiting the number of individuals with complete access, while limiting what everyone who has access to the database can see.
- If an employee has complete access to the organization's records, how can you ensure they do not go on a sudden deletion spree? Or what if their computer is stolen and an unauthorized person gains access to your database?
  - Check to see if the work of these employees is supervised or reviewed. Is it possible to tell when record changes are made and by whom?
  - Additionally, and possibly most importantly, does your organization conduct regular database audits to check for abnormal or potentially fraudulent activity?

Access to Patient Information

- Prior to getting a patient's approval to be engaged as a donor, place restrictions around who in your organization can access their records. For example, only allow employees within the medical development team to view records that contain solely patient information.
  - If a patient doesn't make a donation, this ensures their record will remain private and not be pulled into the organization's greater constituent pool.
- Create a different constituent type or category for these records, such as Hospital Friend.
  - Instead of directly naming the patient, use the identifier Hospital Friend 12345 rather than John Snow 12345.
  - The patient's name, address, and contact information can be included on a secondary tab within the record.
- Medical-specific information should be very limited and adhere to HIPAA policies.
- All records of this type should be searchable only by approved personnel.

Access to Student Information

Post-secondary education institutions:

- Work in accordance with the Admissions/ Records/Registrar/Compliance & Policy offices regarding compliance with FERPA guidelines for faculty and staff. Depending on organization structure you may be required to take compliance training on FERPA.
- If a record was created for a student and their parents and they end up not attending the institution (and they have no other affiliation to the organization), then an effort to inactivate or remove those records from the database should be made. Consult with your Data Governance team as appropriate regarding the policy/ procedure for these removed records as it may have impact outside of prospect development.

Contact Reports and Proposals/ Opportunities

Contact reports serve as institutional memory about the interaction between your organization and its constituents to help fundraising and other development staff stay up to date on engagement efforts. Opportunities or Proposals in your database are to record solicitations (planned or actual) so there is an accurate pipeline and for planning purposes. Recording these, even if they are not successful, is helpful for future solicitations.

The timely recording of both contact reports/ interactions and opportunities are important for having accurate data for fundraising staff and reports. These records do not need to be verbatim accounts of what occurred, but simply reflect the purpose, strategy, outcomes, and next steps of interactions or proposals.

See the table on page 3 for recommendations on what information to include and exclude in contact reports, proposals, and other interaction records.

Metadata: What is it, and why is it important?

For any point of information or resource, there is a second level of data that provides more detail than what meets the eye. According to **Britannica**, Metadata is "**data** about informational aspects of other data." For example:

- The date of creation/modification
- The author/person who input the data
- The source of information (e.g., LexisNexis, DonorSearch, Alumni Survey, Direct from Constituent, etc.)

These data points are all essential metadata that give the user greater context for the relevant data at hand. In terms of prospect research and donor data, metadata is especially key, as it gives us important background to identify how old information is, how that information has changed, and where that information came from in the first place.

Metadata can even flag for us how accurate information may be based on provenance. Did the datapoint come from a first-hand conversation with a donor, or from internal prospect research? Metadata tells us how strong the information really is, allowing the user to make more informed decisions on how to retain and appropriately use the data in question. For the same reason, metadata is an inherent part of data minimization: how do we know information is still relevant? How could we determine whether it is worth retaining if we didn't have the background metadata provides? Without metadata, any data minimization effort is incomplete. We need the metadata to help us determine, in the end, if information stays or goes.

Inactivating or Removing Records

To ensure that erroneous data is not continuously stored in our databases, inactivating, or removing records (or parts of records) is a good practice when certain criteria are met. These criteria include, but are not limited to:

- The constituent is deceased
- Records that do not have any valid contact information
- Records that have not had any interactions in a certain period of time (e.g., 10 years), and do not have: relationships to other records, an active membership, endowment or legacy gift stewardship activity, or other organization-related attributes

Audits are helpful to review information to ensure that the data should be inactivated or removed. Your database may contain duplicate records of active constituents but with inactive data. Audits are helpful in managing duplicate records as well.

Depending on a person's constituency, a record can be made inactive, which helps minimize the data seen and used at your organization. Some general guidelines follow.

Alumni Records

- Keep all records even if they have not made any gifts to the institution. Alumni count impacts reporting. If you work for an educational institution, this is the main constituency within the database.
- Former spouse of an alum: if the only reason a person is in your database is that they used to be married to an alum, and has never donated, they could be marked inactive.

Donor Records

- Giving threshold: if a donor has given over a certain amount (e.g., $25K), the donor record will not be inactivated

Membership Records

- If a constituent is a donor (or paid annual member) and not a member of any additional constituency, the donor records could/should be kept for historical reference. However, if the individual has opted out of further mailings/ solicitations/etc., and a significant amount of time has passed since the last gift (e.g., 20+ years), the record could be marked inactive.

Patient Records

- If a patient is not a donor to your institution, the constituent can be marked inactive or deleted from the database after a certain period (e.g., 5+ years).
- Patient data importation policies are designed to transfer minimal information from hospital visit records and can only be viewed by development employees with special permissions. Additionally, patient records often remain separate from the organization's greater constituent pool until they make a gift or commit to a gift. Due to these policies, patient data may not require as much minimization as active donor data.

Data Retention: how long should we keep data?

The storing of information is vitally important to comply with government and industry regulations and internal administration requirements. To help with this, it is recommended that organizations write a data retention policy, a set of guidelines that helps organizations keep track of how long information must be kept and how to dispose of the information when it is no longer needed.

A data retention policy should seek to answer the following:

- **What types of information do we need/want to store?** Different types of data (e.g., personal, and sensitive) will be subject to different rules and regulations – you need to check relevant state/ federal laws and international laws such as GDPR to determine what information you can store.
- **Do you need the data?** You should determine whether you need the data to accomplish some goal, or whether you are retaining certain data that has no associated defined purpose or use. For example, do you need to store a supporter's date of birth or pet's name? Do you still need information on that lapsed donor from 10 years ago?
- **Do you have a plan to use the data you are collecting?** Why are you collecting this data and how are you going to use it? Best practice is to store only that amount of data your organization needs to provide regular reports, drive useful dashboards, and make critical operational decisions around fundraising.
- **How long are you entitled to keep the information?** The length of time you should hold on to data is often subjective and dependent on your reasons for processing the data. An organization should outline how long they intend to keep data, which might vary from 30 days to 3 years and beyond! Speak to your internal partners, including legal and compliance teams and information security, to get advice on this.
- **What should you do with data when it is no longer needed?** Many data management regulations state that you can only keep data for a specific purpose or time period; all donors will become inactive at some point (through relocation, age, death, lack of interest etc.) and it is good practice to delete such data on a regular basis. Data should be deleted from your database, as well as any mirrored copies of the database or a backup copy of the database from your vendor.

- **What is your process for subject access requests and data opt-out?** Organizations are required to communicate and explain how prospects and donors can opt-out of communications with your organization, suppress their personal data, or access personal information you may hold about them. You should have a clear and simple process to enable individuals to do this if they wish to – this is normally outlined in an organization's privacy policy.
- **What is your process for deleting data?** Will you seek to archive or anonymize certain data or remove it from the database immediately? How regularly will you monitor and manage this deletion process?

Overall, it is considered best practice to develop a data retention statement that defines an "Active supporter," which may include characteristics such as:

- They have donated to your organization in the last 3 years
- They volunteered in the last year
- They have responded to a campaign, letter, or communication positively

How you define the parameters of data retention policy is ultimately up to your organization; there are some legal and administrative restrictions, but it is also dependent on your organization's aims, objectives, and ambitions for the future.

Opt-out of Data Retention

Our constituents have the option of requesting that their personal data be removed from the database and that their records be deactivated. Opt-out and general fundraising privacy language, should be available and clear for your constituents. See resources below for opt-out language examples.

If a constituent opts-out include:

- Verify the identity of the constituent making the request.
- Deactivate all but the most essential information (e.g., name/record type/degree) to ensure that the individual is not contacted in the future, or re-added to the database, and for archival purposes.
- Add "no contact" coding so the constituent is not contacted in the future.
- Add alerts on the record (e.g., "Record inactivated on MM/DD/YYYY per the constituent's request to opt-out. Do not contact…").
- Retain donation information for legal purposes, including for tax purposes.
- Retain information in case of a potential or actual legal claim.

RESOURCES

CAN-SPAM Rule. (Mary 21, 2008). Code of Federal Regulations. **https://www.ftc.gov/business-guidance/resources/can-spam-act-compliance-guide-business**

The Donor Bill of Rights (n.d.). Association of Fundraising Professionals. **https://afpglobal.org/donor-bill-rights**

Fundraising Opt-Out. (n.d.) McLaren Health Care. **https://www.mclaren.org/main/fundraising-opt-out**

Fundraising Policy Guidelines. (n.d.). Stanford University. **https://privacy.stanford.edu/guidelines/fundraising-privacy-guidelines**

Getting GDPR Consent & Opt-in. (n.d.) Zettasphere. **https://www.zettasphere.com/gdpr-consent-opt-in-examples/**

Hinely, Mark. (2018, August 23). GDPR Fundamentals: Legal Basis for Processing Data. *KirkpatrickPrice.* **https://kirkpatrickprice.com/video/gdpr-fundamentals-legal-basis-for-processing/**

Klosowski, Thorin. (2021, September 6). The State of Consumer Data Privacy Laws in the US (And Why It Matters). *The New York Times.* **https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/**

Privacy Law Comparison Matrix (n.d.). WireWheel. **https://wirewheel.io/resource/privacy-laws/**

Richner, Cedric A., III. and Penate, Jill Schrems. (2015, September 11). The HIPAA Privacy Rule: What Fundraisers Need to Know. *The Giving Institute.* **https://www.givinginstitute.org/news/250351/The-HIPAA-Privacy-Rule-What-Fundraisers-Need-to-Know.htm**

Terms, Privacy & Notices. (n.d.). March of Dimes. **https://www.marchofdimes.org/policy.aspx**

What is Data Minimization? (n.d.). Trend Micro Incorporated. **https://www.trendmicro.com/vinfo/us/security/definition/Data-Minimization**

Zetoony, David A. (2020, October 26). Does the CCPA require data minimization with regard to the collection and use of information? *Greenberg Taurig, LLP*. **https://www.gtlaw-dataprivacydish.com/2020/10/does-the-ccpa-require-data-minimization-with-regard-to-the-collection-and-use-of-information/**

GLOSSARY OF TERMS

Anonymize: The process of removing identifying information from a data point.

Audit: An examination of the processes, contents, and personnel related to an organization's philanthropic database.

Data hygiene: Involves the data management practices organizations deploy when regularly reviewing their databases to ensure all information is relevant, current, and of high quality. It's a set of processes that ensures the removal of irrelevant and outdated data. The end result of data hygiene is information that is complete, correct, and consistent. (source: **https://www.lytics.com/blog/what-is-data-hygiene/**)

Data minimization: Delimiting the storage, collection, and retention of personal data relevant and necessary to accomplish fundraising goals.

Data retention: Possessing, utilizing, and storing data.

Family Educational Rights and Privacy Act (FERPA): A federal law that affords parents the right to have access to their children's education records, the right to seek to have the records amended, and the right to have some control over the disclosure of personally identifiable information from the education records. When a student turns 18 years old, or enters a postsecondary institution at any age, the rights under FERPA transfer from the parents to the student (source: U.S. Department of Education, **https://studentprivacy.ed.gov/faq/what-ferpa**)

Freedom of Information Act (FOIA): Provided the public the right to request access to records from any federal agency. It is often described as the law that keeps citizens in the know about their government. Federal agencies are required to disclose any information requested under the FOIA unless it falls under one of nine exemptions which protect interests such as personal privacy, national security, and law enforcement. (source: United States Department of Justice, Freedom of Information Act, **https://www.foia.gov/about.html**)

General Data Protection Regulation (GDPR): This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data. (source: **https://gdpr-info.eu/art-1-gdpr/**)

Health Insurance Portability and Accountability Act (HIPAA): An act that protects individuals' medical records and other personal health information. (source: U.S. Department of Health and Human Services, **https://www.hhs.gov/hipaa/for-individuals/faq/187/what-does-the-hipaa-privacy-rule-do/index.html**)

Metadata: A second level of data that provides more information on the original data set.

Personally Identifiable Information (PII): Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. (source: U.S. Department of Labor. **https://www.dol.gov/general/ppii#:~:text=Personal%20Identifiable%20Information%20(PII)%20is,either%20direct%20or%20indirect%20means**)