PERSONAL DATA FLOW MAPPING

A practical guide for ensuring compliance with privacy legislation

OPEN NORTH

CONTENTS

WHAT IS PERSONAL DATA FLOW MAPPING?

Organizations that collect and use personal data as part of their business have a strict obligation to protect that information from inappropriate use and disclosure. However, for many small non-profits and social enterprises, this is a challenge. You may not have a dedicated IT department, and your data likely lives in many different places—from secure cloud servers to stacks of paper on a coordinator's desk.

You cannot protect what you cannot find.

At its core, personal information mapping is the process of creating a visual or descriptive representation of the lifecycle of personal information within your organization. It is more than just a list of files; it is a narrative of how data travels. It involves answering these key questions:

› What personal data do we collect?
› From whom and from where do we collect the data?
› Why do we collect it (the purpose)?
› Where is it stored, both internally and with third parties?
› Who has access to it internally?
› With whom is it shared externally (such as vendors, funders, or partners)?
› How does it move between systems (for example, via email, automated API, or manual entry)?
› How long do we keep it?

Benefits of personal data flow mapping

Data flow mapping helps your organization understand several critical aspects of your data management practices:

› **Custody:** It helps you identify what personal data you *actually* hold versus what you *think* you hold.
› **Location:** It helps you locate where data is stored, including physical filing cabinets, personal laptops, and digital servers.
› **Access:** It allows you to see who can view or use the data, and whether that access is necessary.
› **Transit:** It illustrates how data moves between your internal systems and external partners.

By visualizing the paths that data takes, you can identify points of vulnerability—such as emailing sensitive health data without encryption - and take proactive measures to reduce risks. It also allows you to assign data management responsibilities clearly, which ensures that specific stakeholders are held accountable.

Can you use this process for non-personal data?

Yes. While this guide focuses on personal information for legal compliance, these techniques apply to any type of data. You can use this process to migrate software, identify business bottlenecks (like redundant data entry), or remove cluttered storage.

Is data flow mapping a legal obligation?

Quebec's Law 25

In Quebec, all private-sector organizations, including non-profits and charities, must comply with Law 25. While the law does not explicitly state that "you must have a map," it does require a Privacy Impact Assessment (PIA for many activities. A data map is the prerequisite for a PIA. You cannot assess the risk of a project if you do not know how data flows through it.

You generally need to assess privacy risks in the following situations:

› **Sharing data for research or statistics:** This applies when you disclose data to third parties (like university researchers) without individual consent.
› **Updating or acquiring systems:** This applies when you set up a new Client Relationship Management (CRM) tool, move to the cloud (such as Microsoft 365 or Google Workspace), or launch a new app.
› **Transferring data outside Quebec:** This applies when you use a service provider that stores your data outside the province, which is a very likely scenario in the case of cloud-based services.

A note on federal privacy law (PIPEDA)

Mapping your data flows is also a best practice for compliance with Canada's federal privacy law, the Personal Information Protection and Electronic Documents Act (PIPEDA). The key takeaway is this: You cannot comply with requests to delete or correct user data (which is a right under both laws) if you do not know where all copies of that data are stored.

> Note 💡
>
> Following the steps outlined in this guide does not replace the requirement to conduct a full privacy impact assessment (PIA) when one is legally required. For detailed guidance on PIAs, consult the *Commission d'accès à l'information (CAI)*.

HOW TO IMPLEMENT EFFECTIVE DATA FLOW MAPPING?

Understanding how personal information flows within your organization is one of the best ways to strengthen privacy practices and improve daily operations. Whether you're a community service provider, a local government partner, or a social enterprise, data flow mapping helps you see the full picture of what information you collect, why you collect it, where it goes, and who has access along the way.

Think of it as creating a "map" of your data journey, from the moment your organization collects or generates information to when that data is stored, shared, or ultimately deleted.

Step 1: Plan your mapping exercise

Mapping personal information is easiest if you plan the process first. This stage involves defining the scope, identifying the team, and gathering existing documentation.

Instructions

1. **Create a data flow mapping plan document:** Open Template 1: Data flow mapping plan that accompanies this guide and use it to document the decisions you will make in the subsequent steps.
2. **Determine the scope:** Choose a specific process to map first (for example, "volunteer recruitment," "donor management," or "client intake"). Do not try to map the entire organization at once.
3. **Identify the team:** Appoint a coordinator to lead the work (this might be the Executive Director or Office Manager) and identify the "data users" (staff members) who will provide the detailed knowledge.
4. **Gather documents:** Collect existing policies, forms, and contracts to see what rules are already in place.

Example: Planning a data flow mapping exercise

The Montreal Fruit Share Co-op is a small not-for-profit organization that connects residents who have fruit trees on their property with volunteers who pick the fruit which is then donated to local food banks.

› **The plan:** The organization identifies two main sets of personal information: volunteers and residents (tree owners). They decide to focus first on volunteers' personal information to keep the project manageable.
› **The team:** The executive director leads the project to ensure accountability. However, they involve the volunteer coordinator, who manages the day-to-day schedules, to ensure they capture the reality on the ground rather than just the theory.

Step 2: Inventory your data locations

Before you can map the data, you must identify every "container" where data might live. You must be thorough and include the "shadow IT" (unofficial or unapproved tools) that staff might be using to make their jobs easier.

Instructions

1. **Brainstorm locations:** List every digital and physical place where your organization stores information.
2. **Check for "shadow IT":** Ask your staff if they use personal devices, WhatsApp groups, or unsanctioned apps to do their work.
3. **List common sources:** Ensure you check shared drives (Google Drive/SharePoint), SaaS tools (CRMs, email marketing), communication platforms (Slack/Teams), and physical storage (filing cabinets).

Example: Creating an inventory of data locations

The team from Montreal Fruit Share Co-op meets to brainstorm where volunteer data might be stored. They identify four specific "buckets":

› Paper registration forms: Collected at community fairs.
› Google spreadsheet: A master list used by the office admin.
› FruitPick app: A mobile app that connects volunteers to specific fruit picks.
› Mailchimp: Used to send the monthly newsletter.

They note each of these data locations to include in their data flow map.

Note

For a more comprehensive look at this specific step, Open North's "Getting to Know Your Data" guide provides detailed advice on conducting a data inventory. The outputs from a full data inventory exercise can complement this step perfectly.

Step 3: Classify the types of personal data

Once you know *where* the data is, you must look inside those containers to determine what the data is. This step is critical because Quebec's Law 25 imposes different requirements depending on the sensitivity of the information.

You should categorize your data into three levels:

› **Personal data:** This is any information that relates to a person and allows them to be identified (e.g., name, address, email).
› **Sensitive personal data:** This is a special category that requires a high level of protection. If this data is leaked, it could cause significant harm (e.g., medical info, financial data, sexual orientation, union membership).
› **Business contact information:** This is a person's contact info at their place of employment. It is generally subject to fewer restrictions.

Instructions

1. **Review the inventory:** Go through the list of locations you created in Step 2.
2. **Tag the data:** For each location, determine if the data inside is "personal," "sensitive," or just "business contact info."
3. **Verify with staff:** Ask the people who use the files daily whether there are any hidden columns or notes that might contain sensitive information (such as health notes in a "comments" field).

Example: Classifying types of personal data

The Montreal Fruit Share Co-op team reviews the "buckets" they found in Step 2 to see exactly what details are inside. Here's what they discover:

› They see that the Google Sheet contains names and emails (personal data).
› They review the paper registration form and realize it asks about "physical limitations" or allergies to ensure volunteer safety. They flag this as sensitive health data.

They now know that the paper forms in the filing cabinet require much higher security than the email list in Mailchimp.

Step 4: Map the data flow

Now that you have your inventory and your classification, you must organize it into a structured table. This helps you visualize the lifecycle: from collection to storage to usage and, eventually, deletion.

The most important pieces of information to capture include:

› **Activity or process** – What happens and in what order (for example, "Volunteer signs up," "Staff reviews application," "Information entered into CRM").
› **Source of personal information** – Where the data comes from (e.g., web form, paper intake form, partner referral).
› **Type of personal information** – Such as name, contact information, date of birth, or demographic details.
› **Where it's stored** – For electronic data, this could be a folder or database. For paper-based records, this could be a filing cabinet or binder.
› **Who has access** – Which staff, teams, or external partners can see or edit it.
› **How long it is retained for and how is it deleted or destroyed** when it is no longer needed.

You can adjust the structure and level of detail depending on your organization's size and complexity.

A smaller organization may only need a high-level summary showing systems and key flows, while larger or more data-intensive organizations may prefer a more detailed breakdown by file, database, or activity.

The important thing is that your table provides a clear and accurate picture of how personal information moves through your operations.

Instructions

1. **Create a spreadsheet:** Open Template 2: Data flow mapping table that accompanies this guide.
2. **Populate the rows:** For every activity identified in your scope, fill in a row in the template.
3. **Trace the journey:** Ensure you capture where the data comes from (source), its destination (storage), who has access to it, and the length of time it is kept (retention).

Example: Mapping the data flow

The Montreal Fruit Share Co-op decides to organize their findings into a structured table (using Template 2) to see the flow clearly.

#	activity	type of personal information	format	storage	access	retention
1	Volunteer completes registration form	Name, email, phone, availability	Online form	Google Sheets	Admin staff	indefinite
2	Admin enters data into scheduling app	Name, phone, email	Manual entry	Fruit Pick App database	Admin and coordinators	indefinite
3	Volunteer receives schedule notification	Name, assignment details	Automated email	Fruit Pick App database	Admin	indefinite

Tips for visualizing your data flow

If you choose to draw a diagram (using a whiteboard, paper, or software like draw.io), using standard shapes makes your map easier for others to read. You do not need to be an artist; clear labels are more important than perfect drawings.

- › **Use consistent shapes:**
  - › **Rectangles:** Use these for activities or processes (e.g., "Staff reviews application" or "Data entry").
  - › **Cylinders (or stacks of coins):** Use these for data storage (e.g., databases, filing cabinets, or cloud servers).
  - › **Arrows:** Use these to show the direction of the flow.
- › **Label the arrows:** Do not just draw a line from the "Web Form" to the "Database." Write text *on the arrow itself* to describe exactly what data is moving (e.g., "Name & Email").
- › **Use "swimlanes":** To show who is responsible for what, divide your diagram into horizontal rows (swimlanes). Label each row with a role (e.g., "Volunteer," "HR Manager," "IT System"). Place the shape in the row of the person or system performing the action.
- › **Colour code for risk:** Consider using a specific colour (like red or orange) for lines or shapes that involve sensitive personal information. This makes high-risk areas pop out immediately.

Step 5: Use your map to inform decisions

Your completed data flow map is not just a compliance document to file away; it is a diagnostic tool. Now that you can see the flow, you must look for "leaks" or "blockages."

Instructions

1. **Analyze for risks:** Look at your completed Template 2. Are there places where sensitive data is stored insecurely? Are there duplicates?
2. **Check retention periods:** Look at the "Retention" column. If it says "Indefinite" or is blank, you need to create a rule to delete old data.
3. **Update policies:** If you find new third-party vendors (such as a new cloud app), update your privacy policy to disclose them.
4. **Plan the next review:** Decide when you will update this map again (e.g., in one year).

Note

For more information on identifying and mitigating cybersecurity risks, see Open North's guide:
opennorth.ca/resources/cybersecurity-for-small-and-medium-sized-organizations

Example: Using the map to inform decisions

The Montreal Fruit Share Co-op looked at their spreadsheet from Step 4 and identified a few risks – as well as actions they could take to address those risks:

› **Duplication:** They noticed that volunteer data was being manually re-entered from Google Sheets into the app, causing errors. They committed to exploring integration options to sync the two systems automatically and reduce the need for manual data entry.
› **Physical data security:** They realized the paper waivers (containing sensitive health info) were in a filing cabinet accessible to anyone in the office. To address this risk, they decided to move these files to a locked drawer and restricted key access to authorized staff only.
› **Retaining data for longer than necessary:** They found records dating back 5 years for volunteers who had not helped in years. To address the risks associated with retaining unnecessary personal data, they implemented a policy requiring the deletion of volunteer data 2 years after a volunteer becomes inactive.

CONCLUSION

Personal data flow mapping is a practical, accessible way to better understand how personal information moves through your operations. By taking the time to document what data is collected, why it is needed, where it is stored, and who can access it, organizations gain clearer visibility into their actual practices - not just what policies say should happen.

Importantly, data flow mapping is not a one-time exercise. It is a **living document**. As programs evolve, new tools are introduced, and partnerships change, information flows shift as well. Maintaining an up-to-date map helps organizations respond more effectively to privacy obligations and build trust with the people whose information they hold.

Get started today

To begin creating your first data flow map, you can use and adapt the templates below. If you require support to implement data flow mapping in your specific context, Open North offers a targeted support service. Contact us at info@opennorth.ca.

About Open North

Building trust in data, for the common good

Open North is a not-for-profit organization dedicated to advancing the common good. Working alongside governments and civic-minded organizations of all sizes, we provide data expertise to enhance decision making, drive innovation, improve public and civic services, and address society's most pressing challenges.

Our work focuses on building the capacity of organizations to make better decisions about managing their data so that it is useful, actionable, secure, and trustworthy throughout its entire lifecycle. At Open North, we combine deep expertise in data with a multidisciplinary approach. Our team includes urban planners, software engineers, community organizers, data scientists, cybersecurity and IT audit specialists, sociologists, geographers, and technology lawyers, bringing diverse perspectives to every project.

Open North is part of Montréal in Common, a project led by the City of Montréal as part of the Smart Cities Challenge, carried out with the financial support of the Government of Canada.

opennorth.ca

About the Smart Cities Challenge and Montréal in Common

Montréal in Common is an innovation community led by the City of Montréal whose partners are experimenting with solutions regarding access to food, mobility, and municipal bylaws, with a view to rethink the city. Montréal in Common projects are made possible thanks to the prize awarded to the City of Montréal by the Government of Canada as part of the Smart Cities Challenge.

Authors: Steven Coutts and John Griffin

TEMPLATE 1: DATA FLOW MAPPING PLAN

Objective(s) What do we want to achieve with this personal data flow mapping project?	
Scope Which business process or activity will the data flow map focus on? Which data types, formats and systems should be included? What should be excluded?	
Roles and responsibilities Who will be responsible for coordinating the project? Who else needs to be involved in the project to ensure it is successful?	
Tools What tools will we use to create the data flow map?	
Governance How often will you conduct a major review or update of the personal data flow map? What processes will you put in place to ensure the information stays up-to-date in between major updates/reviews?	

TEMPLATE 2: DATA FLOW MAPPING TABLE

#	activity or process	type of personal information	format	location	access	retention
1						
2						
3						
4						
5						
6						
7						

Personal data flow mapping