LEMIEUX & ASSOCIATES

a NATIONAL leader in investigative services

Data Privacy Policy

Table of Contents

1. Purpose

Lemieux & Associates ("Company") is committed to protecting the privacy and confidentiality of the personal information that is collected and processed during our investigative activities. The Data Privacy Policy establishes practices and procedures regarding the collection, use, disclosure, and retention of personal data. This policy ensures the Company:

- Complies with federal and state privacy laws.
- Protects the rights of staff, customers, and partners.
- Is open about how it stores and processes individuals' data.
- Protects itself from the risks of a data breach.

2. Scope

The Data Privacy Policy applies to all personal data collected, processed, and stored by Lemieux & Associates as part of our investigative activities, whether offline or online. It also applies to all staff, volunteers, contractors, suppliers, and other people working on behalf of Lemieux & Associates.

3. Responsibilities

Everyone who works for or with Lemieux & Associates has some responsibility for ensuring data is collected, stored, and handled appropriately. Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

The **Executive management team** is ultimately responsible for ensuring that Lemieux & Associates meets its legal obligations.

The **Data Protection Officer** is responsible for:

- Keeping management updated about data protection responsibilities, risks, and issues.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the data Lemieux & Associates holds about them (also called "Subject Access Requests").
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

The **IT Manager** is responsible for:

- Ensuring all systems, services, and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services used to store or process data (for instance, cloud computing services).

The **Marketing Manager** is responsible for:

- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets like newspapers.
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

4. General Guidelines

Employees should keep all data secure, by taking sensible precautions and following the guidelines below.

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- The Company will provide training to all employees to help them understand their responsibilities when handling data.
- Strong passwords and multi-factor authentication must be used, and they should never be shared.
- Personal data should not be disclosed to unauthorized individuals, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their line manager or the Data Protection Office if they are unsure about any aspect of data protection.

5. Data Collection

The Company may collect personal information from various sources, including but not limited to:

- Individuals who voluntarily provide information during inquiries or investigations.
- Clients that voluntarily provide information during the case intake process.
- Third-party sources such as public records, government agencies, or other authorized entities.
- Electronic sources, including websites, social media platforms, or other publicly available information.

The types of personal data collected may include, but are not limited to:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Dates of birth
- Social security numbers
- Employment details
- Financial information
- Personal health information*
- Social media information

*In compliance with the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191 as amended) ("HIPAA"), Lemieux & Associates has adopted a supplemental Health Insurance Portability and Accountability Act Compliance Policy to ensure reasonable protection of Protected Health Information ("PHI"), as defined by the Code of Federal Regulations 45 C.F.R. 160.103.

6. Data Use

Lemieux & Associates only uses personal data for legitimate purposes directly related to its investigative services and to fulfill contractual obligations or legal requirements, specifically for the purposes of:

- Conducting investigations in accordance with applicable laws and regulations.
- Verifying identities, backgrounds, and credibility of individuals involved in our investigations.
- Gathering evidence and information necessary for clients' legal or regulatory needs.
- Maintaining records, reporting, and communication related to our investigative activities.

The following guidelines should be adhered to when working with personal data:

- Employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. It should never be sent by email, as this form of communication is not secure.
- Data must be encrypted before being transferred electronically. The IT Manager can explain how to send data to authorized external contacts.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data in the Lemieux & Associates case management system.

7. Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT Manager.

Generally, personal data should not be stored on paper. However, when necessary, it should be kept in a secure place where unauthorized access and viewing are not permitted.

- When not in use, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorized people can see them, such as on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

When stored electronically:

- Data should only be stored within the Lemieux & Associates case management system, where it can be protected from unauthorized access, accidental deletion or alteration, and malicious cyber security attacks.

- Data should be protected by strong passwords and multi-factor authentication and never shared between employees.
- If data is stored on removable media (like a CD or DVD), these devices should be encrypted and kept locked away securely when not being used.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the Company's standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.

8. Data Accuracy

Lemieux & Associates takes reasonable steps to ensure data is kept accurate and up to date. It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be noted and removed from the database.
- Marketing databases should be checked against industry suppression files periodically.

9. Data Disclosure

In certain circumstances, personal data may be disclosed:

- To authorized employees, agents, or contractors who need access to the information for the purposes of conducting investigations.
- To relevant third parties, such as law enforcement agencies, legal authorities, or regulatory bodies, as required or permitted by law.
- To the Company's clients or their authorized representatives who have engaged its services and have a legitimate interest in the information.

Lemieux & Associates does not sell or rent personal data to third parties for marketing or any other purposes.

10. Data Retention

As noted in the Record Retention Policy, personally identifiable information (PII) or case information is maintained for a minimum of 7 years or indefinitely, unless otherwise required by applicable laws and regulations. Non-personally identifiable information is retained indefinitely. Reasonable and appropriate measures are taken to protect personal data from unauthorized access, loss, or alteration.

11. International Data Access

In limited instances, personal data may be securely accessed from an international location outside of the jurisdiction where the data was originally collected. In doing so, the Company will ensure that appropriate safeguards are in place to protect the data, in accordance with applicable data protection laws.

12. Individual Rights

Data protection regulations such as the European Union's General Data Protection Regulation (GDPR) and other countries' privacy laws provide certain rights for data subjects. Data subject rights under such privacy laws often include the following:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right of data portability
- Right to object

If you wish to confirm that Lemieux & Associates is processing your personal data, or to have access to the personal data Lemieux & Associates may have about you, please contact privacy@lemieuxassociates.com.

13. Contact Information

For any questions or concerns regarding this Data Privacy Policy or Lemieux & Associates' practices, please contact:

Lemieux & Associates
110 Washington Avenue, 2nd Floor
North Haven, CT 06473
203-780-8021
privacy@lemieuxassociates.com