PERSONAL INFORMATION PROTECTION PROCEDURES – eZmax Solutions Inc.

Version 1.0

September 1, 2023

Version history		
Version	**Date**	**Prepared by**
Version 1.0	2023-09-01	Caroline Charbonneau

Privacy Officer Contact Information:

Caroline Charbonneau

privacy@ezmax.ca

eZmax, Solutions Inc.

2500 Daniel-Johnson Blvd., Suite 800 Laval, Quebec H7T 2P6

SECTION 1: Inventory of personal information files

1. Definition of personal information

As defined by the Commission d'accès à l'information du Québec, *personal information* is any information that relates to a natural person and directly or indirectly allows that person to be identified.

Personal information is confidential. This confidentiality is based on the right to privacy, which allows all individuals to exercise control over how their information is used or distributed.

2. Definition of public information

As defined by the Commission d'accès à l'information du Québec, certain information that allows for a person to be directly identified is public.

For example, the following information about a person's position within a company or government body is considered public information:

- Name
- Title
- Position
- Email address, work address and telephone number

3. Personal information – eZmax employees

The following information is collected and stored in eZmax employee files:

- First and last name
- Personal email
- Personal address
- Personal telephone numbers (home, cell)
- Date of birth
- Social insurance number
- Bank account information

Documents containing personal information are digitally generated and stored in the eZmax employee's Electronic Document Management ("EDM") folder. When a paper document is generated, it is scanned, added to the employee's EDM folder, and stored digitally. The paper document is then shredded. No paper documents are retained.

4. Personal information – contractors

For independent contractors, the following information is collected and stored in eZmax's supplier files:

- First and last name
- Email
- Address
- Telephone numbers (home, cell)
- Social insurance number
- Bank account information

Documents containing personal information are digitally generated and stored in the independent contractor's EDM folder. When a paper document is generated, it is scanned, added to the contractor's EDM folder, and stored digitally. The paper document is then shredded. No paper documents are retained.

5. Personal information – corporate eZmax and eZsign customers

eZmax software products are sold to businesses, so the customer information retained by eZmax is not considered personal information. However, eZmax and eZsign customers may potentially collect personal information that is stored in eZmax applications and databases. Please refer to clauses 8 and 9 for more information.

6. Personal information – individual eZsign customers

The eZsign solution is sold directly to customers via individual accounts. During this process, the following personal information is collected and stored in eZmax customer files:

- First and last name
- Email
- Address
- Telephone numbers (home, cell)

When electronic signature files are created with individual accounts, personal information is collected by individuals (not private companies) and stored in eZmax databases.

7. Personal information – free eZsign trial accounts

The eZsign solution allows individuals to create trial accounts. During this process, the following personal information is collected and stored in the trial account record of the eZmax application:

- First and last name
- Email
- Telephone number

8. Personal information retained by eZmax customers in the eZsign application

When electronic signature files are created by customers with the eZsign application, personal information is collected and stored in eZmax databases.

8.1 eZsign directories

Signer information:

- First and last name
- Email
- Telephone numbers (home, cell)
- Security question

8.2 Documents added to the application and signed

- All documents added to the eZsign solution, whether signed or unsigned, may contain personal information.
- It is impossible for eZmax to know the contents of these documents. It is therefore the responsibility of eZmax customers to have a procedure for the retention and destruction of these documents.

9. Personal information retained by eZmax customers in the eZmax application

9.1 Transaction records

For any type of transaction, including but not limited to listings, temporary listings, sales, buyer-broker agreements, other income, refused promises to purchase, disclosure notices, etc., the following information could be collected and stored:

For buyers and/or owners:

- First and last name
- Address
- Email
- Telephone numbers (home, cell)
- Date of birth
- Employer
- Profession

All documents added to the transaction record in the EDM may contain personal information. It is impossible for eZmax to know the contents of these documents. It is therefore the responsibility of eZmax customers to have a procedure for the retention and destruction of these documents.

9.2 eZsign electronic signature records

The following information about signers may be collected and stored in eZsign electronic signature records:

- First and last name
- Email
- Telephone numbers (home, cell)
- Security question

All documents added to electronic signature records, whether signed or unsigned, may contain personal information. It is impossible for eZmax to

know the contents of these documents. It is therefore the responsibility of eZmax customers to have a procedure for the retention and destruction of these documents.

9.3 Employee records

The following information about employees may be collected and stored in employee records:

- First and last name
- Personal email
- Personal address
- Personal telephone numbers (home, cell)
- Date of birth
- Social insurance number
- Bank account information

All documents added to employee records in the EDM may contain personal information. It is impossible for eZmax to know the contents of these documents. It is therefore the responsibility of eZmax customers to have a procedure for the retention and destruction of these documents.

9.4 Broker records

The following information about brokers may be collected and stored in broker records:

- First and last name
- Personal email
- Personal address

- Personal telephone numbers (home, cell)
- Date of birth
- Social insurance number
- Bank account information

All documents added to broker records in the EDM may contain personal information. It is impossible for eZmax to know the contents of these documents. It is therefore the responsibility of eZmax customers to have a procedure for the retention and destruction of these documents.

SECTION 2: Retention, destruction, and personal information anonymization procedure

1. Overview

Implementing a retention, destruction, and personal information anonymization procedure is important to ensure that we protect individuals' privacy, comply with privacy laws, prevent privacy incidents involving personal information and security breaches, maintain customer trust, and protect our reputation.

2. Objectives

The purpose of this procedure is to protect individuals' privacy and to comply with our legal obligations regarding the protection of personal information.

3. Scope

The scope of this procedure covers the entire personal information lifecycle from collection to destruction. It concerns all employees and stakeholders involved in the collection, processing, retention, destruction, and anonymization of personal information in accordance with legal requirements and data privacy best practices.

4. Definitions

Personal information: Any information that directly or indirectly identifies a natural person.

Retention: Secure storage of personal information for a required duration.

Destruction: Deletion, disposal, or permanent erasure of personal information.

Anonymization: The process of irreversibly and permanently modifying personal information to ensure that no individual can be identified from the information, whether directly or indirectly, by any means.

5. Procedure

5.1 Retention period

5.1.1 Personal information has been categorized as follows:

- eZmax employee information
- Subcontractor information
- eZsign customer information
- Free eZsign trial account information

Personal information retained by eZmax customers and stored in the eZmax and eZsign applications is covered in the Procedure for requesting de-indexation and deletion of personal information.

For more information, please refer to the complete list of personal information files we retain.

5.1.2 The retention period for each of these categories has been established as follows:

- eZmax employees: 7 years after employment ends

- Contractors: 7 years after the contract ends
- Individual eZsign customers: 7 years after the last bill
- Free eZsign trial accounts: 60 days

5.2 Secure storage methods

5.2.1 The personal information eZmax retains is hosted in the ca-central-1 region by AWS (Amazon Web Services) unless the agreement between the customer and eZmax specifies another region.

5.2.2 More information regarding data security can be found in the Trust Centre section of the eZmax website.

5.3 Destruction of personal information

5.3.1 When personal information has been collected on paper, it must be completely shredded after being digitized. No paper version will be retained.

5.3.2 Digital personal information must be completely deleted from devices (computers, phones, tablets, external hard drives), servers, and the cloud.

5.3.3 The destruction schedule, based on the retention period for each personal information category, will be carried out and reviewed annually by management. It is imperative that planned destruction dates be documented.

5.3.4 Destruction will be carried out in such a way that personal information cannot be recovered or reconstituted.

5.4 Anonymization of personal information

Personal information should only be anonymized if the company wishes to retain and use said information for serious and legitimate purposes or if destroying it is not possible.

5.5 Employee training and awareness

5.5.1 Employees must receive regular training on the retention, destruction, and personal information anonymization procedure, as well as on the risks associated with privacy breaches.

5.5.2 This also includes making employees aware of data security best practices and the importance of complying with established procedures.

SECTION 3: Procedure for requesting de-indexation and deletion of personal information

1. Overview

This procedure addresses the privacy and confidentiality concerns of eZmax customers and provides a means for customers who retain personal information in eZmax applications to destroy and/or anonymize it.

2. Objectives

The purpose of this procedure is to provide a structured mechanism for managing requests to de-index and delete the personal information of eZmax customers.

3. Scope

This procedure applies to the internal team responsible for managing requests to de-index and delete personal information. It covers all information published on online platforms, including the website, applications, or any other digital medium used by our customers.

4. Definitions

Deletion of personal information: The act of completely erasing data, making it unavailable and irrecoverable.

De-indexing of personal information: The removal of information from search engines, making it less visible, but still directly accessible.

Deletion permanently removes the data, while de-indexing limits how visible it is online.

Anonymization of personal information: The process of irreversibly and permanently modifying personal information to ensure that no individual can be identified from the information, whether directly or indirectly, by any means.

5. Procedure

5.1 Receipt of requests

5.1.1 Requests for de-indexation and deletion of personal information must be received by the Support team.

5.1.2 Customers can submit their requests via:

- By mail:

  The Privacy Officer, Caroline Charbonneau
  eZmax Solutions Inc.
  2500, boul. Daniel-Johnson, bureau 800 Laval, Québec H7T 2P6
- By email to privacy@ezmax.ca

5.2 Identity verification

When the request comes from an individual:

5.2.1 Before processing a request, a reasonable effort must be made to verify the individual's identity.

5.2.2 This can be done by requesting additional information or by verifying the individual's identity by video call.

5.2.3 If the individual's identity cannot be satisfactorily verified, eZmax may refuse to process the request.

When the request comes from a company:

5.2.4 For customers using the eZmax application: a detailed request will be sent to the company's authorized signatory. The form must be completed and signed by an authorized signatory of the company. Company details will be verified in the appropriate business registry.

5.2.5 For customers using the eZsign application: eZsign customers can set up the deletion of their personal information themselves, so the procedure will be shared with them. If the request requires eZmax

intervention, a request must be completed and signed by an authorized signatory of the company. Company details will be verified in the appropriate business registry.

5.2.6 If the authorized signatory's identity cannot be satisfactorily verified, eZmax may refuse to process the request.

5.3 Evaluation of requests

5.3.1 The team will carefully review the request and the personal information concerned to determine whether it is eligible for de-indexation or deletion.

5.3.2 Requests will be handled in a confidential and timely manner.

5.4 Reasons for refusal

There are valid reasons why eZmax may refuse to delete or de-index personal information:

- To continue providing goods and services to the customer
- To comply with labour law
- For legal reasons in the event of a dispute

5.5 De-indexing or deletion of personal information

The team will take the necessary steps to de-index or delete the personal information in accordance with eligible requests.

5.6 Follow-up communications

5.6.1 The team is responsible for communicating with requesters throughout the process by acknowledging receipt and providing regular updates on the status of their request.

5.6.2 Any delays or problems in processing requests must be clearly communicated to requesters.

5.7 Monitoring and documentation

5.7.1 All requests to de-index or delete personal information and subsequent actions taken in response will be recorded in a dedicated tracking system.

5.7.2 Recorded information will include details about the requests, actions taken, and the dates and results of these actions.

SECTION 4: Procedure for requesting access to personal information and handling complaints

1. Overview

Since individuals may request to access the personal information that the company holds on them or file complaints, it is important to have predefined guidelines for responding to these types of requests.

2. Objectives

This procedure ensures that all requests for access are handled in a confidential, timely, and accurate manner while respecting the rights of the individuals concerned.

3. Scope

This procedure applies to the internal stakeholders responsible for handling requests for access and complaints, as well as individuals who wish to access their own personal information.

4. Data access request procedure

4.1 Submission of requests

4.1.1 Individuals who wish to access their personal information must submit a request in writing to the company's privacy officer.

- By mail:

  The Privacy Officer, Caroline Charbonneau
  eZmax Solutions Inc.
  2500, boul. Daniel-Johnson, bureau 800 Laval, Québec H7T 2P6
- By email to privacy@ezmax.ca

4.1.2 The request must clearly indicate that it is a request for access to personal information and provide sufficient information to identify the individual and the information sought.

4.1.3 This information may include name, address, or any other relevant information for reliably identifying the individual making the request.

4.2 Receipt of requests

4.2.1 Once the request has been received, an acknowledgement of receipt will be sent to the individual to confirm that the request is being processed.

4.2.2 The request must be processed within thirty (30) days of receipt.

4.3 Identity verification

4.3.1 Before processing a request, a reasonable effort must be made to verify the individual's identity. This can be done by requesting additional information or by verifying the individual's identity by video call.

4.3.2 If the individual's identity cannot be satisfactorily verified, eZmax may refuse to disclose the personal information that has been requested.

4.4 Responding to incomplete or excessive requests

4.4.1 If a request for access to personal information is incomplete or excessive, the privacy officer will contact the individual to request additional information or clarification.

4.4.2 The company reserves the right to refuse a request if it is clearly unreasonable, excessive, or unjustified.

4.5 Processing requests

4.5.1 Once the requester's identity has been verified, the privacy officer in charge of processing requests for access to personal information will proceed with gathering the requested information.

4.5.2 The privacy officer will check the relevant directories to gather the personal information requested, taking care to comply with any legal restrictions.

4.6 Reviewing the information

4.6.1 Before disclosing the personal information to the individual requester, the privacy officer will carefully examine the information to ensure that it does not contain any third-party information that could be confidential or violate any other rights.

4.6.2 If third-party information is present, the privacy officer will assess whether it can be unbundled or whether it should be excluded from the disclosure.

4.7 Communicating the information

4.7.1 Once these verifications have been completed, the personal information will be sent to the individual within a reasonable period of time in accordance with applicable legal requirements.

4.7.2 The personal information will be sent to the individual electronically or by secure mail, depending on the individual's preference and appropriate security measures.

4.8 Monitoring and documentation

4.8.1 All steps in the process of handling requests for access to personal information must be recorded accurately and completely.

4.8.2 The details of the request, actions taken, decisions made, and the corresponding dates must be recorded in an access request tracking register.

- Date request received
- Date of acknowledgement of receipt
- Date of identity verification
- Identity verification method
- Decision – access request granted or refused
- Date of disclosure (if applicable)

4.9 Confidentiality

Everyone involved in processing requests for access to personal information must maintain confidentiality and privacy.

4.10 Handling complaints and appeals

4.10.1 If an individual is dissatisfied with the response to his or her request for access to personal information, he or she will be informed of the complaint procedures and remedies available from the Commission d'accès à l'information.

4.10.2 Complaints must be handled in accordance with internal complaint management policies and procedures (next section).

5. Complaint handling procedure

5.1 Receipt of complaints

5.1.1 Complaints may be filed by contacting the privacy officer:

- By mail to the attention of:
  The Privacy Officer, Caroline Charbonneau
  eZmax Solutions Inc.
  2500, boul. Daniel-Johnson, bureau 800 Laval, Québec H7T 2P6
- By email to privacy@ezmax.ca

Complaints are required to be recorded in a centralized register that is only accessible by designated eZmax personnel.

5.1.2 Employees must immediately inform the department that handles complaints.

5.2 Preliminary assessment

5.2.1 The designated person reviews the complaint to assess its validity and severity.

5.2.2 Frivolous, defamatory, or obviously baseless complaints may be rejected. However, in such cases, a justification must be provided to the person who filed the complaint.

5.3 Investivation and analysis

5.3.1 The person in charge of the complaint will conduct a thorough investigation, gathering evidence, interviewing the parties concerned, and collecting all relevant documents.

5.3.2 The person in charge of the complaint must be impartial and have the necessary authority to resolve the complaint.

5.3.3 The person in charge of the complaint must keep all information about the complaint confidential and ensure that all parties involved are treated equitably.

5.4 Resolution of complaints

5.4.1 The person in charge of the complaint will propose appropriate solutions to resolve the complaint in a timely manner.

5.4.2 Solutions may include corrective action, financial compensation, or any other action necessary to satisfactorily resolve the complaint.

5.5 Communication with the person who filed the complaint

5.5.1 The person responsible for the complaint will communicate regularly with the person who filed the complaint to keep the

person informed of the progress of the investigation and resolution of the complaint.

5.5.2 All communications must be professional, empathetic, and respectful.

5.6 Closing of complaints

5.6.1 Once the complaint has been resolved, the person in charge of the complaint must provide a written response to the person who filed the complaint summarizing the measures taken and the proposed solutions.

5.6.2 All information and documents about the complaint must be kept in a confidential folder.

SECTION 5: Security incident and personal information breach response procedure

eZmax strives to maintain the security of our IT infrastructure and our customers' data, with the understanding that no company can be entirely insulated from potential security incidents. For this reason, we've drawn up a detailed incident response plan in the event of a security breach in our business or IT assets. This full plan is available upon request.

eZmax is determined to act as soon as possible to mitigate the risk of ongoing data leaks, to conduct investigations to identify vulnerabilities, and to take necessary corrective action to prevent further incidents. Incident management team members will work together to assess and manage the situation to reduce risk and identify the appropriate stakeholders based on the level of risk.

Incidents may take the form of malicious code attacks, unauthorized access to eZmax systems, unauthorized use of eZmax services in attacks, general misuse of systems, or hoaxes.

The goal of the incident response plan is to protect customer data and meet all legal and regulatory requirements.

Privacy breaches – Special intervention

If a security incident related to a privacy breach has occurred, eZmax undertakes to take the following actions:

- To fill in the privacy incident log to document the incident
- To investigate the privacy breach to determine whether personal information has been lost due to unauthorized access or use,

unauthorized disclosure, or any other privacy breach and whether there is a risk of serious harm to the individuals concerned

- In such cases, to report them to the Commission de l'accès à l'information du Québec, and report them to anyone whose personal information was involved in the incident