

Policy on the protection of personal data

1. Who is the data controller and who is the data protection officer?

The notary office Jadoul, Kestelyn, Genicot & Dierckx processes personal data as part of its activities.

Jadoul, Kestelyn, Genicot & Dierckx, located at Broekstraat 25/1 te 3080 Tervuren, with company number 0740.800.777, acts as the data controller for the processing of personal data carried out within the Office (hereinafter: "the notary office"). The data controller is the natural or legal person who determines the purpose and means of processing personal data.

The notary office values privacy protection. It is committed to safeguarding personal data with special care and processing it transparently in strict compliance with data protection laws, particularly the General Data Protection Regulation (EU) 2016/679 (hereinafter: "GDPR") and the Code of Conduct of the National Chamber of Notaries dated January 28, 2021, which specifies certain application conditions of the GDPR for notaries (hereinafter "Code of Conduct").

In accordance with the GDPR and the Code of Conduct, the notary office has appointed a Data Protection Officer, namely Privanot vzw. The Data Protection Officer can be reached at the following email address: info@privanot.be, or by mail at the following address: Privanot vzw, Bergstraat 30, 1000 Brussels.

Through this data protection policy, we aim to provide further clarification on how we handle personal data. This policy answers the following questions:

- Who is the data controller and who is the data protection officer?
- Why is your personal data processed?
- What is the legal basis for processing your personal data?
- What personal data does the notary office process?
- What are the sources of information?
- To whom can your personal data be disclosed?
- Who are the data processors of the notary office?
- Is your personal data transferred outside the European Economic Area (EEA)?
- How long is your personal data retained?
- How is the security and confidentiality of your personal data guaranteed?
- What are your rights?

It should be noted that information regarding the processing of personal data of internal employees for Human Resources purposes is found in the notary office's employment regulations. Information on the processing of personal data of external employees for personnel matters is included in specific documents such as service agreements or general policy documents.

2. Why is your personal data processed?

Purposes – The notary office collects and processes personal data primarily to ensure the legal certainty of transactions for which the notary guarantees authenticity, as well as for managing cases entrusted to the notary.

Additionally, processing is required to fulfill other important tasks and objectives, namely:

- the management of the notary office's files, including processing carried out before and after the execution of an authentic deed, such as conducting searches and checks necessary for the execution of a deed, as well as any other processing required for the fulfillment of the notary's duties as a public official and the tasks entrusted to them by citizens;
- The administrative management and follow-up of citizens' files, including invoicing and accounting;
- Conducting verifications and checks within the framework of AML legislation;
- Ensuring the security of buildings, goods, personnel, and visitors through video surveillance;
- Optimizing website navigation through the use of cookies;
- Improving customer-friendliness and the quality of services by utilizing citizen feedback and statistical analyses of the notary office's operations and services with the help of software;

3. What is the legal basis for processing your personal data?

Lawfulness – The processing of personal data by a notary is considered lawful when, in most cases, it is necessary to comply with a legal obligation to which the notary is subject or required for the performance of a task in the public interest entrusted to the notary handling the case within the firm.

The processing of personal data by the firm is based on, but not limited to, the following legislation:

- The Law of 25 Ventôse An XI concerning the organization of the notarial profession;
- The Act of 18 September 2017 on the prevention of money laundering and terrorist financing, as well as the limitation of cash usage.

Additionally, the lawfulness of processing may also be based on the legitimate interest of the data controller, such as improving customer satisfaction or securing the firm through surveillance cameras.

Finally, personal data processing may be based on the consent of the data subject, for example, when non-functional cookies are used on the firm's website.

4. What personal data is processed by the study?

Depending on the services requested, the notary office may process the following personal data:

- identification data (surname, first name, civil status, national register number, place and date of birth, etc.);
- contact details (postal address, e-mail address, telephone number, etc.);
- economic and financial data (bank account number, etc.);
- data relating to legal capacity;
- data relating to professional activity;
- data relating to deeds executed at the notary office;
- data relating the family, social, tax or other circumstances that the notary is required to collect from official sources and administrations concerning you;
- video surveillance footage;
- data relating to the quality/satisfaction of the services provided.

5. What are the sources of information?

As a public officer, the notary must collect and use personal data for professional purposes. These data originate from:

- yourself or your legal representative ;
- authentic data sources strictly regulated by specific legislation, such as the National Register, the Crossroads Bank of Social Security, the Central Inheritance Register, the Central Register of Cohabitation and Marriage Contracts, etc. ;
- official bodies authorised to provide data to notaries in the context of their public interest duties;
- images captured by surveillance camera(s).

6. To whom can your personal data be disclosed?

Depending on the processing context, the personal data processed by the notary office may be shared with third parties ("recipients"), in particular:

- to legally authorised partners, such as federal government services and notarial institutions, for the storage of transcripts of deeds and their metadata in the context of electronic registration and for the registration of your data in the central registers of the notarial profession (e.g. the Central Register of Marriage Contracts, the Central Register of Power of Attorney Agreements, the Central Register of Declarations relating to the appointment of an administrator or a person of trust, etc.);
- to the Royal Federation of Belgian Notaries, regarding data relating to real estate assets, to include them in a notarial database aimed at generating statistics and assisting notaries in estimating property values during their duties;
- the Provincial Chamber of Notaries and/or the National Chamber of Notaries (e.g. in the context of their duties related to accounting control or the prevention and combating of money laundering);

- other notaries involved in your case (e.g. in the case of a deed of sale of real estate);
- the National Archives for the conservation of files, minutes and wills;
- Banks involved in your case;
- The expert accountant/tax consultant responsible for the bookkeeping of the notary office;
- Subcontractors for the management and continuity of the notary office, such as software suppliers for the preparation of documents.

7. Who are the data processors of the notary office?

A data processor is a natural or legal person, a government authority, a service or another entity that processes personal data on behalf of the notary office.

The notary office relies, among others, on the following categories of processors:

- Hardware supplier;
- Software suppliers, for example, for case management and accounting administration;
- Backup provider;
- Supplier for the destruction of paper documents;
- Supplier of surveillance cameras;
- Consultant or external employee.

8. Are your personal data transferred outside the European Economic Area (EEA)?

In principle, your personal data will not be transferred outside the European Economic Area (hereinafter "EEA").

If your personal data are transferred to countries outside the EEA and the European Commission determines that the destination country does not provide an adequate level of protection, the notary office will take all necessary measures to safeguard your personal data by providing additional guarantees (for example, by implementing standard contractual clauses approved by the European Commission, signing binding corporate rules, etc.).

9. How long will your personal data be kept?

In accordance with the principle of limited data retention, the aforementioned data may only be retained for as long as necessary to fulfill the stated purpose, taking into account the specific applicable laws and the statutory limitation periods for property and personal claims. The retention periods below correspond to those specified in the notary office's processing register.

The retention periods vary depending on the nature of the documents in question:

- Citizen records are retained as long as the citizen has not chosen to change notaries and may be kept for the entire lifetime of the citizen to facilitate legal advice (in accordance with Article 9 of the Notary Act);
- Case files are retained for 50 years after closure for evidentiary purposes (in accordance with Article 62 of the Notary Act);

- Notarial deeds (minutes) are retained for 50 years after their execution and are then transferred to the National Archives (in accordance with Article 62 of the Notary Act);
- Books (accounting records) are retained for 10 years after the end of the financial year (in accordance with Article 33 of the Notary Act);
- Bank statements are retained for 10 years after the end of the relevant financial year (in accordance with Article 33 of the Notary Act);
- Personal data processed under AML legislation are deleted after the 10-year retention period (in accordance with Articles 60 and 62§1 of the AML Act);
- Surveillance camera footage is retained for a maximum of 1 month (in accordance with Article 6 of the amended law of March 21, 2007, on the installation and use of surveillance cameras);
- Personal data processed for website management are retained as long as necessary to achieve the intended purpose;

10. How are the security and confidentiality of your personal data ensured?

The notary office implements appropriate technical and organizational measures to ensure a security level tailored to the risk and adopts security measures for personal data processing as established in the Code of Conduct of the National Chamber of Notaries dated January 28, 2021.

These security measures are designed to prevent the destruction, loss, alteration, modification, unauthorized access, or misrepresentation of collected personal data to third parties, as well as any other unauthorized processing of such data.

The notary office ensures, among other things, that:

- Access to premises containing data carriers is restricted to authorized persons only;
- The server environment is adequately secured;
- Personal data are securely stored and destroyed;
- Employees and processors securely access only the data necessary to achieve the intended purpose;
- A procedure for reporting data breaches is available to members of the notary office;
- A policy regarding the rights of data subjects is available to members of the notary office;
- An information security policy is available to members of the notary office;
- A GDPR awareness policy is available to members of the notary office;
- Technical security measures, such as firewalls, antivirus software, and regular security updates, are applied.

These measures are regularly reviewed and assessed by the aforementioned DPO as part of routine check-ups.

The notary office has concluded a data processing agreement with its processors, in accordance with Article 28 of the GDPR and Article 2 of the Code of Conduct of the National Chamber of Notaries dated January 28, 2021.

The firm shall take appropriate technical and organisational measures to ensure a level of security appropriate to the risk. In addition, the firm shall ensure that it adopts the security measures for the

processing of personal data set out in the Code of Conduct of the Chambre nationale des notaires of 28 January 2021.

11. What are your rights?

Under the GDPR, as a data subject whose personal data is processed by the notary office, you have various rights concerning your personal data, provided they do not conflict with the legal obligations to which the notary office is subject.

Under certain circumstances, you have the following rights:

- Right to information: You have the right to access which personal data the notary office processes about you, as well as to be informed about the purposes of this processing and the data retention period.
- Right of access: You have the right to view and obtain a copy of the personal data that the notary office holds and processes about you.
- Right to rectification: You have the right to have inaccurate or incomplete personal data concerning you corrected.
- Right to erasure ("right to be forgotten"): You have the right to request the deletion of your personal data processed by the notary office.
- Right to restriction of processing: You have the right to restrict the processing of your personal data, for example, when you dispute the accuracy of the data.
- Right to data portability: You have the right to receive your personal data in a structured, commonly used, and machine-readable format and to transfer it to a third party.
- Right to object: You have the right to object to the processing of your personal data by the notary office.

You can exercise your rights directly with the notary office via email (info@notarissen-tervuren.be) or by letter [Broekstraat 25/1 3080 Tervuren] or by contacting the Data Protection Officer via email at info@privanot.be.

Finally, if you believe that your rights are not being respected in accordance with the GDPR, you can file a complaint with the Data Protection Authority (Persstraat 35, 1000 Brussels or via their website www.gegevensbeschermingsautoriteit.be).
