

Privacy Policy

How we protect and process personal data and how the data can be modified.

We trade as VSL-SYSTEM sp. z o.o., KRS No: 0000764453, REGON No: 382150077, VAT No (NIP): 5252775513, the amount of share capital: 5.000,00 ZŁ, registered office: 11 Mazowiecka St. Office no. 49, 00-052 Warsaw, Poland.

Our activity is commonly known as a virtual bureau and in legal terms it is defined as “providing a registered office, business address or correspondence address and other related services to a legal person or an unincorporated association. The company is a controller of personal data given by you at the time of signing the agreement and collected from other sources.

The company is also an “obligated institution” within the meaning of the Act on Counteracting Money Laundry and Terrorism Financing of 1 March 2018.

This document describes data storage methods, data recipients and rules for data modification or erasure.

Purpose and basis of the use of personal data and data storage period

1) Personal data was obtained at the time of agreement signing from a signatory/signatories and collected from generally available sources (National Court Register/Central Record of Business Activities) and is used to perform our agreement and make financial settlements thereunder.

2) We use the personal data to fulfil our accounting and legal obligations, including invoicing income under the agreement, sending invoices via the Internet.

3) We also use the personal data when issuing and delivering other accounting documents at your requests, e.g. KP (cash received), duplicate invoice.

4) We will use the personal data:

a) till the expiry of our agreement to the extent necessary to perform such an agreement;

b) for the lawfully necessary period of data storage, for example for tax purposes or for the purpose of administrative or court proceedings, etc.;

c) for the period during which it is possible to make claims under unpaid invoices;

d) for time set out in the Act on Counteracting Money Laundry and Terrorism Financing of 1 March 2018, which means that the following issues must be taken into account:

- personal data contained in the virtual bureau agreement and attachments thereto will be processed to meet the regulations of the aforementioned Act, including the evaluation of risks connected with money laundry and terrorism financing, as well as the use of defined financial security measures set out by the Act;

- to apply the financial security measures, our company may process and copy information coming from the identification documents of the tenant (as a party to the agreement) and a person authorised to act on the tenant's behalf;

- our company as an “obliged institution” stores copies of documents and the tenant's data specified in the agreement for 5 years, counting from the first day of the year following the year of expiry of the virtual bureau agreement.

Data collected by us to enter into the agreement

1) To enter into the agreement, we need the data specified in the Act on Counteracting Money Laundry and Terrorism Financing of 1 March 2018.

Such data include:

a) the data of a natural person:

- first name and surname,

- citizenships,

- PESEL or date of birth, if no PESEL was assigned,

- the state of birth
- series and number of an identification document (passport for persons from outside Poland),
- place of residence,
- name of business, in the case of natural persons carrying out their business activity,
- unique taxpayer reference (NIP),
- address (as at the agreement date) of the main place of business, in the case of natural persons carrying out their business activity,

b) data of a natural person or an unincorporated association:

- business name,
- form of organisation,
- address (as at the agreement date) of a registered office or business place,
- unique taxpayer reference (NIP) or, if not available, the state of registration, name of a commercial register and number and date of registration in the register,
- full name of a natural person (or several natural persons if the entity is represented by more persons, e.g. two Directors) that represents the legal person or unincorporated association,
- PESEL and state of birth or date of birth, if no PESEL was assigned, of a natural person (or several natural persons if the entity is represented by more persons, e.g. two Directors) that represents the legal person or unincorporated association.

c) The data of a person acting as a proxy for the purpose of the lease agreement:

- first name and surname,
- citizenships,
- PESEL or date of birth, if no PESEL was assigned,
- the state of birth
- series and number of an identification document (passport for persons from outside Poland),

d) Data of beneficial owners:

- first name, surname and citizenship.

e) Data of persons signing a distance lease agreement outside our company's offices:

- a scan of an ID card or passport or an extract of data from the ID card certified as a true copy by a local Notary Public.

f) Data of persons signing a lease agreement if such persons are from outside Poland, the European Union, Norway, Lichtenstein, Switzerland, the USA, Canada, Australia, New Zealand:

- a scan or copy of a passport.

g) To enter into the agreement, we also need the tenant's statement that the beneficial owner is/is not a politically exposed person or a member of the family of or a person known as a close associate of a politically exposed person.

2) Such data include generally available information recorded in the generally accessible Central Record of Business Activities or National Court Register or we need an extract from a foreign register of companies.

3) In addition to Appendix 6 to the agreement, the company's representative gives personal data of persons who will come to the personal data controller's office on the company's behalf to collect the company's correspondence. The data can be generally available data from the National Court Register or Central Record of Business Activities, e.g. first names, surnames, PESELs of directors, proxies, attorneys of the company or the data may concern another person. If the data of a person that is not disclosed in the National Court Register or Central Record of Business Activities is given, the consent of such a person must be presented.

All data of third parties in relation to the parties to the agreement must be given provided that regulations on the personal rights of third parties are not violated.

4) In addition to Appendix 8 to the agreement, the company's representative must give the company's e-mail and/or telephone number.

During the term of the agreement, if the agreement covers scanning company correspondence, we obtain correspondence scans. Correspondence scans appear at our company as a result of the service you have chosen. The scans are not analysed. Although, given their nature, they are in a digital form

(hereinafter referred to as electronic files).

Storage time: identical to the term of the agreement, however storage divides into two steps.

Stage 1 - correspondence scan is in the form of an unencrypted, regular PDF file and it is sent to an e-mail address and removed as soon as possible, usually within 7 days.

Stage 2 - correspondence scan is in the form of an encrypted PDF file and only such a file is stored according to the above-mentioned storage period.

During the term of the agreement, we obtain information about correspondence incoming to your company. The information is not analysed, but is stored in a digital form.

Storage time: identical to the term of the agreement.

5) Please, note that whether your business correspondence is scanned or not, we also obtain the data of senders of such correspondence, e.g. a sender may be a business partner or an employee.

Therefore, when you provide your business correspondence to us, you actually provide personal data of your business partners or employees. For that purpose, you have to sign the personal data processing agreement.

Recipients of your data

Your data are delivered to the following extent:

1) All data and electronic files: to the supplier of a hosting server where the database is kept, files are hosted and electronic mail is operated. We have entered into a data processing agreement with the supplier.

2) Only telephone number: if a subscription fee is not paid within the period set out in our agreement, the telephone number is transferred to the “paid text message gate” supplier to send a text message with a request for payment. We have entered into a personal data processing agreement with the supplier of the “paid text message gate” services.

3) All data and electronic files: our employees who have signed relevant confidentiality and personal data protection statements and have knowledge of personal data processing.

4) All data of your company: debt collectors or buyers, if you do not pay our invoices.

5) Only generally available data of the company (name, address, VAT No, as simply visible on the invoice): entities providing book-keeping, accounting, tax, legal services to our company (at present there is only one entity of this type, which is our book-keeping bureau).

6) All data and electronic files: tax authorities, the police, special services, etc. at their request for the purpose of their proceedings, including all competent state authorities.

7) Telephone number, information about the sender and sender's city of mail received for your company - it is transferred to the service provider of the “paid text message gate” services to send an SMS, if you have purchased a package for sending this information via SMS, in addition to the standard package with information via e-mail.

Transmission of your data to our subcontractors

1) Personal data are processed by the aforementioned subcontractors solely on the basis of a written agreement which complies with applicable regulations.

2) The personal data will not be disclosed to any other persons or institutions, unless this is required by governing law or necessary to process the personal data subject to a relevant agreement which provides for the protection of rights, confidentiality and privacy.

Other sources of your data

1) Your data are acquired from the Central Record of Business Activities and National Court Register.

2) If you pay our invoices via banks or other financial institutions, we obtain information about persons making the payment and numbers of bank accounts used for payment purposes. The data are only processed in order to refund an overpayment, if any, or at a request of state services, e.g. bailiffs, tax offices, the police, etc.

Countries where your data are transmitted

At present, all our subcontractors come from Poland and we do not plan to transmit your data outside Poland and the European Union.

Data used for decision-making

During the performance of our agreement, we process the data concerning your payment or non-payment of fees stemming from the agreement. On this basis, it is possible that we will terminate the agreement and stop providing our services. However, the final decision is made by a representative of our company.

Your rights to personal data and rules for rights exercising

1) Right to rectify or erase the data:

a) electronically by logging in the website panel:

<https://www.biurowirtualnewarszawa.pl/panelklienta/>

moving to the tag Other > Contact and writing information about data you want to correct and new data in the text field;

b) electronically: by writing the information about data you want to correct and new data to any e-mail of our company on the website <https://www.biurowirtualnewarszawa.pl/> from your e-mail given in the agreement;

c) by mail: by writing the information about data you want to correct and new data to the address given on the website <https://www.biurowirtualnewarszawa.pl/>. The letter must be legibly signed by persons authorised to represent your business entity;

2) erasure of data that are illegitimately processed: procedures described in Section 1 above;

3) restriction to data processing: procedures described in Section 1 above;

4) access to data: information about the data we have and making copies of data - procedures described in Section 1 above;

5) object to data processing to be reviewed by us: procedures described in Section 1 above;

6) lodging a complaint with the Chairman of the Personal Data Protection Office.

If you exercise the right to be forgotten or the right to restriction of processing because you object to reasons connected with your

special circumstances, please attach a description of such unusual circumstances or a statement set out by law.

Data protection

1) We use technical and organisational measures which ensure the protection of data processing adequately to the risks.

2) In the case of data kept in a physical form, these are an anti-theft door, an alarm and monitoring by a security company.

3) In the case of data kept electronically in the server, these are a login and a password, as well as data transmission encrypting with SSL certificates. We make backup data of copies on a regular basis.

4) PDF files with correspondence scans are encrypted with a recognized secure cryptographic algorithm, passwords to open files are selected individually for files, randomly, without repetitions greater than the same password up to a maximum of 5 files, with random characters, letters and numbers. PDF files without a password are periodically deleted.

5) In the case of data stored electronically on a desktop computer or laptop, this computer is secured with a login and password, a firewall and anti-virus software with a theft tracking system. Regularly a copy of the data is created to an encrypted backup cloud that meets TIER III and TIER IV, with ISO 9001 and ISO 27001 certificates, encrypted with the AES-256 algorithm, however these computers do not store correspondence scans at all, which are deleted

from them on an ongoing basis after sending it to e-mail.

6) All laptops are used as PCs and are never taken out of our company's premises.

Cookies on <https://www.biurowirtualnewarszawa.pl/>

A document available at

<https://www.biurowirtualnewarszawa.pl/english/formularze/cookies-spzoo.pdf>

constitutes an integral part of this Privacy Policy.

Amendments to the Privacy Policy

We reserve the right to amend this document, provided that your rights hereunder will not be restricted without your consent.

Contact data

Contact data of our company are available on <https://www.biurowirtualnewarszawa.pl/> and in the commonly available Central Record of KRS under the number 0000764453.

As on August, 13th 2021, the data are as follows:

VSL-SYSTEM sp. z o.o.

Al. Jerozolimskie 85 suite 21

02-001 Warsaw

E-mail: info@vsl-system.pl

ul. Mazowiecka 11 suite 49

00-052 Warszawa

E-mail: mazowiecka@vsl-system.pl

Direct contact with the Data Controller:

administratordanychosobowych@vsl-system.pl