

INFORMATION CLAUSE ON PROCESSING OF PERSONAL DATA

VECTOR SYNERGY SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ (hereinafter also referred to as the "Company") is particularly committed to confidentiality and the protection of personal data, therefore we set out below the principles governing the processing of your personal data provided to the Company.

1. Personal Data Controller

The controller of personal data (the "Controller") is VECTOR SYNERGY SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ seated in Poznań, entered into register of entrepreneurs of the National Court Register under KRS number 0000369575; registration court which keeps the Company's documents: District Court Poznań – Nowe Miasto and Wilda in Poznań, VIII Wydział Krajowego Rejestru Sądowego; share capital: 73.500,00 PLN, having registered office and correspondence address: ul. Marcelińska 90, 60-324 Poznań, NIP: 7811857270, REGON: 30157574.

You may contact the Controller as follows:

- by mail: ul. Marcelińska 90, 60-324 Poznań;
- by e-mail: info@vectorsynergy.com;
- by phone: +48 61 667 07 44.

2. Data Protection Officer

We have appointed a data protection officer – Mr Arnold Paszta. It is a person with whom you can contact in all matters relating to the processing of personal data and the exercise of rights related to data processing.

You may contact the data protection officer as follows:

- by mail: ul. Marcelińska 90, 60-324 Poznań;
- by e-mail: arnold.paszta@vectorsynergy.com.

3. Purpose of personal data processing

Purpose of processing your personal data	Basis of processing personal data
Conclusion and execution of all type of contracts	Article 6 sec. 1 lit. b GDPR
Customers and co-workers service	Article 6 sec. 1 lit. a GDPR, article. 6 sec. 1 lit. f GDPR
Monitoring - TV, business mail	Article 6 sec. 1 lit. c GDPR; article 6 sec. 1 lit f GDPR
Statistic on the use of services	Aritcle 6 sec. 1 lit. f GDPR
Recruitment processes for internal vacancies, traineeships and internships	Aritcle 6 sec. 1 lit. b GDPR, article 6 sec. 1 lit. c GDPR

Recruitment of employees	Article 6 sec. 1 lit. a GDPR, article. 6 sec. 1 lit. c, article. 9 sec. 2 lit. b GDPR
Recovery of claims	Article 6 sec. 1 lit. f GDPR
Archiving documents	Article sec. 1 lit. c GDPR
Other own and commissioned objectives and tasks	Article sec. 1 lit. c GDPR
Marketing and PR activities of the Controller	Article sec. 1 lit. f GDPR
Marketing of other products or services	Article sec. 1 lit. f GDPR

Your personal data will not be processed for automated decision-making, including profiling.

4. Legal basis for processing

In case of processing personal data where we obtain the consent of the data subjects, the legal basis is art. 6 sec. 1 lit. a of the GDPR.

In case of processing of the personal data necessary for the performance of the contract in which the data subject is a party, the legal basis is art. 6 sec. 1 lit. b of the GDPR.

If the processing of personal data is necessary to fulfil a legal obligation to which the Controller is subject, the legal basis is art. 6 sec. 1 lit. c of the GDPR.

If the processing of personal data is necessary to protect vital interests of the data subject then the processing is based on art. 6 sec. 1 lit. a of the GDPR.

5. Data recipients

The recipients of the data may be:

- entities and persons, whose access to the data results from the provisions of the law,
- banks – in order to process the carried-out transactions,
- postal and courier service providers,
- service providers who supply the Company with technical and IT solutions to enable it to conduct its business. Such recipients of data will process your data only on the basis of an agreement concluded with the Company as Controller and in accordance with our instructions.
- Controller shall transfer data only when it has them and when it is necessary for the fulfilment of the given purpose of the processing of the personal data and only to the extent necessary for its fulfilment.

6. Collecting data from sources other than directly from you

In some situations, we can collect your data from other sources than directly from you. In such case, the source of data can be other public administration bodies or third parties. In such case, Controller shall inform you about source of data acquisition unless a specific provision exempts him from this obligation.

7. Information concerning the requirement or the voluntariness of the provision of personal data

Providing the personal data is (depending on the type of the data processing operation):

- statutory requirement, where processing is carried out in order to fulfil a legal obligation,
- contractual requirement or condition of concluding a contract, if the data are collected for the purpose of taking steps prior to and entering into a contract,
- voluntary, in case of providing data is based on data subject's consent.

8. Period of storing personal data

We will retain your personal data until the matter for which it was collected has been dealt with, and then in accordance with the uniform material list of files and the provisions of the Act of 14 July 1983 on the national archival resource and archives.

Once the contract has been fulfilled, your personal data will be stored in accordance with the provisions of generally applicable law. For accounting and tax purposes, we process the data for a period of 5 years, calculated from the end of the calendar year in which the tax obligation arose.

If the data were processed by us for the purpose of establishing, asserting or defending against claims, we will process the data for this purpose for the duration of the period of limitation of claims resulting from the relevant legal regulations. If there is a dispute, litigation or other proceedings in progress, the archiving period will be calculated from the date of the final conclusion of the dispute or, in the case of multiple proceedings, the final conclusion of the last one, regardless of how it was concluded, unless the law provides for a longer data retention period or a longer period of limitation for the claim/right to which the proceedings relate.

If the data was collected on the basis of your previously given consent - we will process this data until you revoke it.

As an employer, we are obliged to keep employee records. Records of employees hired before 1 January 1999. - 50 years, records of employees hired for the first time between January 1999 and December 2018. - 50 years, unless we provide ZUS OSW statement and ZUS RIA information report to ZUS - then the retention period is 10 years, records of employees newly hired from 1 January 2019. - 10 years from the end of the calendar year in which the employment relationship ceased.

9. Your rights

- **Right to information (Article 15 GDPR)** You have the right to be informed at any time about which categories of personal data and what information we process about you, the purpose of the processing, how long and according to which criteria the data is stored and whether profiling is used in connection with this. You have the right to request a free copy of your personal data from the Controller. For all other copies which you request or which go beyond the person's right to information, we are entitled to charge an appropriate administrative fee.
- **Right of rectification (Article 16 GDPR)** You have the right to request the immediate rectification of the personal data processed and, taking into account the purposes of the processing, the right to request the completion of incomplete personal data. If you would like to exercise your right to rectification, you can contact the Controller at any time to make the necessary correction.

- **The right to erasure (Art. 17 GDPR)** you have the right to request the erasure of your data ("right to be forgotten") when data collection is no longer necessary, when you have revoked your consent to data processing, when data are unlawfully processed or have been unlawfully collected and there is a legal obligation to erase the data under EU or national law. However, the right to be forgotten does not apply when there is an overriding right to freedom of expression or freedom of information, data collection is necessary to comply with a legal obligation, erasure is not possible due to archiving obligations incumbent on the Controller or data collection serves the assertion, exercise or defence of legal claims.
- **Right to restriction of processing (Article 18 GDPR)** You have the right to request the restriction of the processing of your data when you contest the accuracy of the data, the processing is unlawful, you refuse to erase your personal data and request the restriction of the processing instead, when the necessary purpose of the processing ceases to exist or you have objected to the processing in accordance with Article 21(1) as long as it has not yet been established that the legitimate interests on our part outweigh your interests.
- **Right to data portability (Article 20 GDPR)** you have the right to transfer your personal data, in a commonly used form, in order to transmit it without prejudice to another responsible entity, if, for example, there is consent on your part and the processing is carried out by automated procedure.
- **Right to object (Article 21 GDPR)** You have the right to object to the processing of your personal data at any time, unless we can provide convincing and compelling evidence regarding the processing which outweighs your interests, rights and freedoms. Furthermore, you cannot exercise your right to object when a legal provision stipulates the collection, processing and use of data or obliges you to collect, process or use such data.
- **Right to lodge a complaint with a supervisory authority (Article 77 GDPR)** You have the right to lodge a complaint with the competent supervisory authority if you believe that a breach has occurred in the processing of your personal data.
- **Right to withdraw consent in connection with the right to data protection (Art. 7. 3 GDPR)** The consent you have given for the processing of your personal data can be revoked at any time without stating a reason. This also applies to the revocation of declarations of consent that were given to us before the EU Data Protection Regulation (GDPR) came into force.

10. Sensitive data

Controller will not process your sensitive data, e.g. health data, unless you have given your additional consent.

11. Transfers of personal data to third countries

Your personal data may be transferred to a third country (i.e. a country outside the European Economic Area) or an international organisation. In such a case, such transfer shall only be carried out if the Controller and the processor fulfil the conditions set out in Chapter V of the GDPR. These conditions will be met in the following situations:

- where the European Commission has issued a decision finding an adequate level of protection as referred to in Article 45 sec. 3 of the GDPR provided by the third country, territory or specific sector or sectors within that third country or by the international organisation concerned (hereinafter also referred to as the "Decision") and where the data transfer falls within the scope

of the Decision (a list of Decisions can be found on the following website: https://ec.europa.eu/info/law/lawtopic/data-protection/international-dimension-data-protection/adequacy-decisions_pl);

- in the absence of a Decision or if the data transfer falls outside the scope of the Decision, where appropriate safeguards as set out in Article 46 GDPR (hereinafter also as "**Safeguards**") are provided, including inter alia by means of the standard contractual clauses adopted by the European Commission pursuant to Article 46 sec. 2 GDPR ("Standard Contractual Clauses"), provided that the conditions for the use of the Standard Contractual Clauses are met,
- in the absence of a Decision or the impossibility of providing Safeguards, in specific situations and under the relevant conditions described in Article 49 of the GDPR.

In particular, the Controller uses modern technological solutions and some of its suppliers have servers located in the United States. At the moment, the European Commission has not approved an adequate level of protection for such transfer by issuing a Decision. The US law does not guarantee such a high level of protection of your personal data as the EU regulations. The transfer of data to servers located in the United States may increase the risk that you will not be able to exercise your right to protect your personal data, e.g. to stop its unlawful use or disclosure. US law does not provide any legal way for individuals to access, rectify or erase personal data concerning them. The necessary restrictions and safeguards against data interference by US intelligence authorities have also not been implemented in the US. Therefore, the level of data protection in the US is not equivalent to EU law.

Accordingly, when your data is transferred to the United States, appropriate safeguards will be in place - in particular, the transfer will take place on the basis of an agreement with the data importer containing Standard Contractual Clauses. However, if it is not possible to apply the Standard Contractual Clauses or to provide other Safeguards, the transfer of your personal data to servers located in the United States will only take place on the basis of your consent or if another of the prerequisites of Article 49 of the GDPR.

In order to obtain detailed information on the possible transfer of your data to a third country or international organisation and on the grounds and conditions for such transfer, please contact the Controller or the Data Protection Officer (see points 1 and 2 this information clause for contact details).