PERSONAL DATA PROTECTION RULES
VERTIGO SERVICES OOD, EIK 202655266

VERTIGO SERVICES OOD is a trading company with limited liability, operating in the field of real property management and maintenance. The main activity of the company is the management and maintenance of Business Center Vertigo, locate on 109 Bulgaria Blvd. The company has signed management contracts with all tenants in the building and is constantly striving to improve the quality of the service offered. VERTIGO SERVICES OOD attaches great attention to the correct, conscientious and secure processing of the personal data of their employees and clients. Hereby VERTIGO SERVICES OOD undertakes to ensure an adequate level of data protection. The guideline shall be applied in compliance with the requirements of the General Data Protection Regulation (GDPR).

This guideline is intended to ensure the confidentiality, integrity, availability, and authenticity of personal data at each of the stages of the data processing in the interest of the data subjects. In addition to complying with the legal provisions on personal data protection, appropriate technical and organizational measures are necessary to achieve this goal. All employees must be aware of the risks associated with the technical systems and communication technologies and must take due care in the processing of data.

1. Importance, purpose, accessibility

1.1. This guideline is the mandatory basis on which lawful and sustainable protection of personal data is carried out in the company VERTIGO SERVICES OOD.

1.2. This guideline aims to ensure compliance and protection of rights of the personal data subjects.

1.3. VERTIGO SERVICES OOD has developed specific procedures concerning the processing of personal data, in particular concerning the management of the requests of the objects, the procedures for notifying the supervising body and the procedures for storing and destroying personal data.

1.4. The guideline has to be readily available to all employees at all times. Compliance with the provisions on data protection is the responsibility of the management body of VERTIGO SERVICES OOD, respectively a person authorized by the company.

2. Scope

2.1. The guideline is valid for all employees, executives, as well as for the management bodies of the company. Here are included in particularly all employees, hereunder the employed and the trainees who process and have access to persona data.

2.2. The requirements and prohibitions stipulated in this guideline apply to all operations with personal data, both electronically and on paper. Furthermore, all kinds of data objects (employees, customers, interested parties, goods and services providers etc.) fall within the scope of the guideline.

Basic data protection principles of VERTIGO SERVICES OOD

VERTIGO SERVICES OOD attaches great importance to data protection. In accordance with the policies and legal provisions adopted, the company accepts that each person has the right to determine the conditions for the transmission and use of his/her personal data, such as name, address, email address, telephone number, bank details, financial relations etc. Therefore data is generally not processed unless compliance with the applicable legal

provisions is guaranteed. The below listed data protection principles apply to VERTIGO SERVICES OOD.

What does the term “personal data” mean?

Personal data means any information relating to an identifiable natural person or a natural person that can be identified ("data subject"). This includes, in particular, the name, address, date of birth, email address, telephone number, family status, bank details or financial relations data, etc. More information can be found in item 3.

Right to information
The data subjects are entitled to receive information about the controller, the purposes, the processing period, as well as about the rights they have in relation to the processing of their personal data. For more detailed information, see item 4.

Minimizing data
VERTIGO SERVICES OOD collects only the personal data that are absolutely necessary for the performance of the respective tasks. When they are no longer required, the data is subject to deletion unless the law requires it to be stored for a longer period. More detailed information can be found in item 10.

Privacy
Personal data must be treated confidentially and not be disclosed to third parties who do not need them. In addition, the data is only available to employees of the relevant department who are required to perform their tasks. For more details, see items 6-8.

Expediency
We store customer data and supplier data in connection with the conclusion and execution of contracts with customers and suppliers. VERTIGO SERVICES OOD does not carry out direct marketing. The processing is carried out on the basis of the General Data Protection Regulation of the EU and the Law for Amendment and Supplement to the Personal Data Protection Act.

Conformity to law, consent
Personal data may be used and transmitted only for the purposes for which the subjects have given prior consent. In the absence of consent, they may be used and transmitted only if it is necessary for the performance of a contract, a legal obligation, to protect vital interests or to respect the legitimate interests of the controller. Processing must be traceable at all times and carried out in good faith.

Accuracy
It is important to ensure the use of accurate personal data only. If necessary, they should be corrected. Information on the data stored, the purpose of the storage and the deadlines for deletion should be provided at the request of the data subjects, but only to them, (see item 10 for more details). Upon request, the data must be provided in a standard machine-readable format. Detailed information can be found in item 13.

Right to erasure (right to "be forgotten"), deletion, termination of access (blocking)
Personal data should be deleted when they are no longer required for the intended purposes, and this is not inconsistent with the statutory storage deadlines, respectively fixed deadlines for safekeeping (for more information see item 10). The same applies also if the data subject withdraws the consent granted. If the subject wishes that his/ her data be deleted, the data will blocked if they are still absolutely necessary for performing individual operations. In all other cases, the data is deleted. For details, see items 10 and 11.

Service Providers
The transmission of personal data to service providers processing these data on behalf of VERTIGO SERVICES OOD (processors, joint controllers) is only performed on the basis of a relevant written contract for data processing or sharing. For more information, see item 9.

Data security and documentation
To ensure the confidentiality and availability of personal data, appropriate technical and organizational measures are necessary. This includes protection against unauthorized or unlawful processing, accidental loss, accidental destruction or accidental damage. Each responsible person (manager, executive director) has to prepare a register of all data processing activities and, if necessary, to supplement it and forward it to the data protection coordinators. For more details, see items 10 and 16.

Notification of violations
The competent supervisory authority - the Personal Data Protection Commission (https://www.cpdp.bg/) must be notified of all data protection violations. For this purpose, each violation must be communicated immediately to the manager, on the following email address: v.peshevska@vertigo.bg who in turn takes the next steps. Notification of the supervisory authority shall be carried out only by the management body. For details, see item 12.

Special categories of personal data, risk assessment:
VERTIGO SERVICES OOD does not process special categories of personal data of its clients/suppliers and their employees, as well as visitors to the Business Center Vertigo. VERTIGO SERVICES OOD considers the risk to the security of the personal data processing as minimal.

3. Definitions

3.1. "Personal data" means any information relating to an identifiable natural person or legal entity ("data subject"); "Identifiable natural person" means a person who can be identified, directly or indirectly, in particular by an identifier such as name, identification number, location data, online identifier or one or more specific features of the physical, physiological, genetic, psychic, mental, economic, cultural or social identity of that individual.

3.2. “Special categories of personal data" are personal data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or membership of trade unions, as well as genetic data, biometric data solely for the purpose of identifying an individual, data on the state of health or the sexual life or the sexual orientation of an individual.

3.3. "Processing" means any operation or set of operations performed with personal data or with a set of personal data by automatic or other means such as collecting, recording, organizing, structuring, storing, adapting or changing, retrieving,

consulting, using, disclosing by transmission, spreading, or other means by which data becomes available, arranging or combining, limiting, deleting or destroying.

3.4. “Controller” means a natural person or legal entity, a public authority, an agency or other institution which, alone or jointly with others, defines the purposes and means of personal data processing.

3.5. "Data subject" is an identified or identifiable natural person whose personal data are processed by the company VERTIGO SERVICES OOD.

3.6. "Personal data processor" means a natural person or a legal entity, a public authority, an agency or other institution which processes personal data on behalf of the controller.

“Joint controllers” are two or more controllers, who together determine the goals and means of processing. They shall determine their responsibilities for performance of their duties according to the GDPR in a transparent manner.

3.7. “Third party" means a natural person or a legal entity, a public authority, an agency or other authority other than the data subject, the controller, the processor of personal data and the persons directly entitled to process the personal data under the direct authority of the controller or the personal data processor.

3.8. "Personal data violation" means a security breach that results in accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to personal data which is transmitted, stored or otherwise processed.

4. Obligation to provide information

4.1. VERTIGO SERVICES OOD provides a privacy policy statement to the subject before its data is recorded, e.g. for the purpose of starting work. If the statement does not cover the specific processing, the information is provided to the subject in a separate datasheet which has to be handed over to the subject.

5. Minimizing and relevance of the data

5.1. Every employee is required to collect only the data that is absolutely necessary for the performance of his/ her tasks, where he/ she must determine the purpose for which they will be used. Names and address are needed for the execution of the service/ management contracts and for the issuance of an invoice. However, these data are not used to send unsolicited advertising messages to the client. VERTIGO SERVICES OOD does not carry out profiling and automated decision making.

6. Privacy

6.1. Employees are not allowed to process personal data without permission. Before commencement of their activity, they should undertake an obligation of confidentiality in written form.

6.2. Executives Guidance will be briefed on the administrative and criminal provisions of the law in connection with data protection.

7. Data transmission

7.1. The transfer of personal data to third parties is permissible only on the basis of the law or with the consent of the data subject. VERTIGO SERVICES OOD does not transmit personal data to other countries inside or outside the European Union.

7.2. When the recipient of the personal data is outside the European Union or the European Economic Area, special measures are needed to guarantee the rights and interests of the data subjects. Transmission of data should not take place if the level of data security in the third country where the seat of the recipient is located is not sufficient or other appropriate guarantees are not available. Such guarantees are contained in particular in the standard data protection provisions agreed with the recipient.

7.3. Information on personal data may be provided to law enforcement authorities (prosecution, police, tax authorities etc.) only in writing, after consulting the company's legal adviser (attorney). In the event of a criminal complaint by VERTIGO SERVICES OOD, information about the committed act can also be provided without agreement. Transmission of information by telephone or e-mail is not allowed, as these communication methods do not allow the recipient to be identified.

8. Request of information about the data subjects, made by third parties

8.1. If third parties, especially state authorities, request information about data subjects, e.g. clients or employees of the company, such is only granted when:

- there is a legal obligation to provide information or the company has a legitimate interest in the provision of the information and
- the identity of the third party requiring information is established beyond doubt.
- The rights of third parties are not affected - in cases where the data are from the video surveillance.

8.2. Transmission of personal data to public authorities, in particular law enforcement (police, security authorities), is permissible

- only if a crime reporting is filed on behalf of VERTIGO SERVICES OOD or
- with the permission of the manager.

In all other cases, the transfer of personal data shall be carried out by the management body.

9. Personal data processor, joint controllers

9.1. Suppliers of goods and services that can gain access to personal data are carefully selected before the order is placed. In the event of data processing on behalf of the company VERTIGO SERVICES OOD, the data processor is obliged to provide, through appropriate technical and organizational measures, sufficient guarantees that the processing will be carried out in accordance with the requirements of the GDPR and that the rights of the data subjects are protected.

9.2. The choice of suppliers of goods and services must be documented and take into account the following aspects in particular:

- professional competence of the contractor to perform the particular data processing,
- technical and organizational security measures,
- market experience of the supplier,
- other aspects which make it possible to assess the reliability of the provider (documentation in connection with data protection, willingness to cooperate, response time, etc.).

9.3. It is necessary to conclude a contract for the processing of data. Before the final assignment, the data protection coordinator (resp. the person in charge of the data

protection) must be informed in order to verify that the content of the prepared data processing contract complies with the requirements of art. 28 of the GDPR.

9.4. Contracts with suppliers of goods and services are scanned and stored in a separate folder on the server in order to ensure the transparency of the contracts under art. 28 of the GDPR and traceability of their content.

10. Right to erasure (right to "be forgotten"), deletion, termination of access (blocking)

10.1. Personal data is deleted when they are no longer required for the intended purpose and the deletion is not inconsistent with the legal storage time limits, respectively self-imposed storage time limits.

10.2. In the case of data transmission based on consent given by the data subject, e.g. when sending a newsletter, the data is deleted when the subject withdraws his/ her consent.

10.3. The following storage/ safekeeping time limits (which are also erasure deadlines) apply; if not otherwise specified, the time limits expressed in years start running after the end of the year in which the event that gave rise occurred. The relevant safekeeping times[1] are:

Documents	**Time limits**
Client contracts	
▪ Completed	6 years (statutory time limit)
Invoices	
▪ Consumers	6 years
▪ Enterprises	6 years (statutory time limit)
Rent (accounting document)	6 years (statutory time limit)
Repair (accounting document)	6 years (statutory time limit)
Constructions (accounting document)	6 years (statutory time limit)
Applicants	3 years after refusal
Travel expenses reports	5 years
Human resources management	
▪ File of employee	5 years after the termination of the contract
▪ Labor attestations	3 months
▪ Payrolls	50 години
• Documents for applying for a job	3 years
Inspections/ Audits	10 years
Video surveillance recordings (CCTV footage)	30 days (statutory time limit), except in the case of an investigation and/ or order initiated by law enforcement bodies

[1]The term “safekeeping times” means statutory time limits. The self-imposed time limits are storage times.

10.4. If your document is not mentioned above, the following safekeeping times apply:

Books and records, inventories, annual financial reports, activity reports, opening balance sheet, working instructions and other organizational and accounting documents, as well as customs documentation are kept for 10 years; received commercial or business correspondence, copies of outgoing commercial and business correspondence - 5 years, signed contracts - 6 years as of the date of termination of the legal relationship. All other documents should only be stored until they are necessary for the purposes for which they were collected.
For questions about safekeeping times, you can contact VERTIGO SERVICES OOD:

11. Documentation and accountability

11.1. In order to prove the conformity to the law and above all the compliance with the principles according to art. 5, 6 and 7 of this guideline, all data protection documents must be made available in a way that allows them to be downloaded in their entirety and without delay. The manager of VERTIGO SERVICES OOD is responsible for the correctness, actuality and completeness of the documentation.

11.2. A register shall be kept for all data processing activities of the competence of VERTIGO SERVICES a record is kept. This register shall contain all data required under art. 30 of the GDPR. Each responsible person (manager, executive director or department head) has to make a register of all data processing activities that are performed in the sector he/ she is responsible for. The conformity of the data processing to the law has to be justified.

12. Accidents related to data security

12.1. In the breaches of the security of personal data, for example due to data leakage (such as theft of files) resulting from an IT incident or unauthorized access to data after losing an information medium (e.g. a notebook, USB stick), the manager, as a rule, has to inform the Personal Data Protection Commission within 72 hours. If the preconditions according to art. 34 of the GDPR are present, the data subjects affected by the breach shall also be notified. In these cases all employees are required to inform the manager and the data protection coordinator of the loss of data.

12.2. The manager shall notify the Personal Data Protection Commission and the affected personal data subjects.

12.3. The company department which is in charge of the accident shall immediately propose measures to address the breach and to reduce any possible adverse effects. If the measures cannot be delayed, they must be taken immediately. All measures are documented.

12.4. In cases where it is permissible not to notify the supervisory authority, the reasons for this shall be documented in accordance with art. 33, par. 5 of the GDPR;

The personal data controller shall document any breach of the security of personal data, including the facts relating to the personal data breach, its consequences and the action taken to deal with it. This documentation provides a possibility for the supervisory authority to verify whether this article has been complied with.

13. Rights of the personal data subjects

13.1. Personal data subjects, in particular employees, clients, contact persons for suppliers of goods and services, are entitled to require transparency of the processing (in particular information under articles 13, 14 of the GDPR, as well as rights to access under art. 15 of the GDPR), accuracy of processing (in particular right to rectification under article 16 of the GDPR, to deletion under art. 17 and limitation of processing under article 18 of the GDPR), limitation of the processing (in particular

the right to object under article 15 of the GDPR), as well as the transfer of data (article 20, par. 1 of the GDPR).

13.2. When processing requests, it is necessary to establish the identity of the data subject without doubt. To do so, if possible from an organizational point of view, request to see an ID card or other official document with a photo. Copies of ID cards cannot be made and stored!

13.3. The management body of the company shall take appropriate measures to ensure that the data subjects are provided with all information under art. 13 and art. 14 of the GDPR and with all notifications under art. 15 to Art. 22 and art. 34 of the GDPR related to the processing of data in a precise and transparent manner, in an understandable and easily accessible form, in a clear and simple language within the statutory time limits.

13.4. The management body shall take appropriate measures to prevent further processing in the event that a data subject exercises his right of objection (art. 21 of the GDPR).

13.5. Every personal data protection inquiry has to be documented.

14. Complaints

14.1. Every personal data subject has the right to file a complaint against the processing of his/ her personal data if he/ she considers that the processing violates his/ her rights. The employees in particular may at any time report violations of this guideline.

14.2. The management body has to take the necessary steps to ensure that each complaint receives a reply, respectively the justified complaints are satisfied within a reasonable time.

14.3. Employees and clients of VERTIGO SERVICES OOD can contact the data controller anytime on the following email address: v.peshevska@vertigo.bg The controller may, if necessary, designate a person/ coordinator (contact person for the personal data related issues).

15. Awareness raising and training

15.1. The employees' awareness of personal data protection issues has to be raised in an appropriate way. The content of the respective training events covers the legal requirements as well as the current guideline. The controller (if necessary, after consultation with the person in charge of the data protection) resolves the other issues related to the training content, format and cycle.

15.2. The participation in the trainings shall be documented.

16. Data security

16.1. Taking into account the state of the art, the costs of deployment, the nature, scope, context and purposes of the processing, as well as the risks with different probabilities and burdens on the rights and freedoms of natural persons, the controller and the processor of personal data take appropriate technical and organizational measures to ensure an adequate level of data protection. These measures include, but are not limited to:

- the ability to ensure confidentiality, integrity, availability and sustainability of data processing systems and services,
- the ability to rapidly restore the availability of and the access to personal data in the event of a physical or technical incident,

- the process of regular testing, assessment and evaluation of the effectiveness of technical and organizational measures to ensure the security of the processing.

16.2. To ensure IT security (data security and data protection), a unified management system is introduced. Technical and organizational measures are subject to permanent documentation.

16.3. The following specific technical measures are taken by VERTIGO SERVICES OOD and will be updated and improved as necessary: in a room designated for the purpose and with the appropriate temperature and controlled access, a server containing the customer/ supplier data is places. Access to their data is available only to the managers of VERTIGO SERVICES OOD.

17. Special categories of personal data

Special categories of personal data (e. g. data on racial and ethnic origin, political opinions, religious and philosophical beliefs etc.) may in principle be processed only with the consent of the data subject or, as an exception, on the basis of an express legal provision that allows this. In addition, for the protection of special personal data, additional technical and organizational measures need to be taken (e. g. transport encryption, granting rights of minimum scope).

18. Video surveillance

18.1. **Conformity of the video surveillance to the law:**

Upon execution of the property management contracts for the building with our clients, we have undertaken to ensure the safety and security of the building's occupants, the employees of our clients and the visitors. We carry out video surveillance in fulfillment of our contractual obligation to you as well as due to our legitimate interest in protecting our property and safety (art. 6, par. 1, item b) and art. 6, par. 1, item f) of Regulation (EC) 2016/679 of 27 April 2016).

18.2. The Video Surveillance Registry is filled with data from an automatic 24/7 video surveillance for the movement of employees and visitors to the drive-ins to Business Center Vertigo and on the floors. Recordings of video images are stored on a separate PC installed in the security guards' room. The managers of the data processor and the security service have access to the records. The cameras are owned by VERTIGO SERVICES OOD and the company does not carry out video surveillance outside of the common areas and in individual tenants' premises.

18.3. At the entrances of the Business Center Vertigo and on the respective spots in the common parts of the building are placed warning signs signaling that the object is under constant video surveillance. Data from this registry is stored for 30 days.

18.4. **Access of the data subject to CCTV footage:**

The data subject has the right to request access to a CCTV footage containing his/ her personal data (on which he/ she is filmed), but when personal data can be disclosed to a third party in this way, the controller is obliged to provide the respective natural person with access to that part of the footage which concerns only this person. For this purpose, the controller must take appropriate technical measures to erase/ mask the images of other persons subject to the video surveillance. In the absence of such technical possibility, access to CCTV footage may be granted only with the consent of all persons who are subjects to the video surveillance or with an explicit police and / or court order.

18.5. The physical protection of personal data is carried out by 24-hour security guards.

19. Register of external visitors

The access to Business Center Vertigo is controlled by keeping a special register for external visitors. It is kept by the security service on paper. Only the respective authorized person from the security service, the receptionist and the managers of VERTIGO SERVICES OOD have access to it. If necessary, access is provided for the needs of law enforcement authorities only after the respective legal procedures required by the registry have been completed. The name and surname of the respective visitor, the date and time of entry and exit of the building are entered in the register. The security service has the right to require an identity card upon exercising control of the access.

20. Assessment of impact on the personal data protection

20.1. Where there is a likelihood that a particular type of processing, especially where new technologies are used, and given the nature, scope, context and purpose of the processing, poses a high risk to the rights and freedoms of natural persons before the processing is carried out, the controller makes an assessment of the impact of the planned processing operations on the protection of personal data. One set of similar processing operations, which represent similar high risks, can be considered in one assessment.

20.2. An impact assessment on data protection is needed in particular in the following cases:

- systematical large - scale surveillance of publicly accessible areas or
- systematic and detailed assessment of personal aspects with regard to natural persons, for example the introduction of profiling,
- large-scale processing of special categories of data for racial and ethnic origin, political opinions, membership of trade unions, religious or philosophical beliefs, health data, genetic, biometric data or data on sexual life or on sexual orientation (art. 9, par. 1 GDPR) or data on convictions and violations (art. 10 of the GDPR).

20.3. Impact assessment is a process for determining the levels of impact on a specific individual or group of individuals, depending on the nature of the personal data being processed and the number of individuals affected in violation of the confidentiality, integrity or availability of personal data. Protection levels based on established levels of impact are as follows:

- For the Personnel Register - "low level" of protection;
- For the Video Surveillance Register – “low level" of protection;
- For the External Visitors Register – “low level” of protection.

21. Consequences of violations

Infringement of the provisions of this guideline may have as a consequence labor-law related measures. In addition, violations of the General Data Protection Regulation are punishable by a fine.

22. Person in charge of the data protection

VERTIGO SERVICES OOD finds that at the time of the adoption of this guideline and due to the nature and extent of the processing of personal data in the company, the appointment of a person in charge of the personal data protection is not necessary. The company also declares with this guideline that if there are preconditions for the appointment of such an official in the course of the business, measures will be taken immediately.

23. Data protection coordinator/ responsible person

23.1. If necessary, VERTIGO SERVICES OOD will appoint a data protection coordinator/ responsible person, who should work to comply with the legal provisions related to data protection. In this function he will be subordinated directly to the management body and accountable directly to them.

23.2. The management body of the company assists the coordinator/ responsible person in performing the tasks and provides him/ her with the resources (equipment and tools) needed to accomplish the tasks.

23.3. The personal data protection coordinator/ responsible person of VERTIGO SERVICES OOD is responsible for the internal communication on data protection issues and assists those responsible in the company in implementing the data protection provisions.

23.4. The personal data protection coordinator/ responsible person plans and controls standardized processes related to requests for information, correction, deletion, as well as objections of data subjects (against use and processing of their data for advertising purposes).

23.5. The personal data protection coordinator/ responsible person organizes staff training and confidentiality briefing and records them. To this end, he/ she is informed in good time by the payroll department for newly employed staff and trainees.

23.6. Employees, customers and visitors may address data protection issues to the data protection coordinator, and until such is appointed, to the managing body.

24. Updating the guideline

24.1. In the light of developments in data protection legislation and technological and organizational changes, this guideline will be reviewed on a regular basis in view of the need for updating or supplementing it.

24.2. Amendments to this instruction require a written form to be effective. Employees and management staff should be notified immediately and in an appropriate manner of the amended requirements.