PERSONAL DATA PROCESSING
BY SZYPERSKA SP. Z O.O.

CONTENTS

1. General data processing rules

1.1 This document (hereinafter referred to as the "Policy") sets out the rules of personal data processing and protection to be observed and applied at Szyperska Sp. z o.o. with its registered office in Poznan (61-754), ul. Szyperska 14, NIP 7010991013, KRS 0000850889, (hereinafter referred to as the "Company" or the "Controller").

1.2 Persons (whether employed by the Company or by an entity acting on behalf of the Company – "Processor") who have access to personal data the Controller of which is the Company are required to familiarise themselves with and apply the principles contained in this Policy.

1.3 Personal data in the Company is:

1.3.1 processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency");

1.3.2 collected for specified, explicit and legitimate purposes; processed for a defined period of time ("purpose limitation");

1.3.3 adequate, relevant and limited to what is necessary in relation to the purposes for which such data is processed ("data minimisation");

1.3.4 accurate and, where necessary, kept up to date ("accuracy");

1.3.5 kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which such data is processed ("storage limitation").

1.4 All personal data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality"). The building and all premises where personal data is processed are secured against unauthorised access.

1.5 The Company follows the "clean desk, screen and printer" principle to mitigate the risk of unauthorised access to personal data, implying the obligation to secure all personal data in locked desks, cabinets or safes and to password-lock a computer screen before leaving a workstation unattended and to collect printouts containing personal data or other confidential information from printers immediately after printing.

1.6 The obligation to duly secure the premises, personal data and documents, in which personal data is processed, applies to all users.

1.7 The location and placement of, as well as processing measures for, personal data shall be carefully selected, taking into account the required security aspects of personal data processing. In particular, aspects of power supply, air conditioning and ventilation, fire protection, physical access control shall be considered.

1.8 Personal data shall only be processed using authorised business equipment and IT systems.

2. Exercise of rights of natural persons whose data is processed

2.1 The Controller shall ensure that all rights of natural persons are preserved in accordance with the conditions laid down in the GDPR, in particular:

2.1.1 the right to be informed (fulfilment of the duty of information), to obtain confirmation as to whether personal data is processed by the Controller, to access such data, including to obtain a copy thereof;

2.1.2 the right to withdraw consent;

2.1.3 the right to have inaccurate data rectified or incomplete Data completed;

2.1.4 the right to erasure ("right to be forgotten");

2.1.5 the right to restriction of processing;

2.1.6 the right to data portability;

2.1.7 the right to object to personal data processing;

2.1.8 the right not to be subject to decisions taken pursuant to the automated data processing, including profiling.

2.2 If the erasure of data made available to other parties by the Controller is requested, the Controller – taking account of available technology and the cost of implementation – shall take reasonable steps to inform controllers that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

2.3 Personal data shall not be erased in cases referred to in Article 17(3) of the GDPR – in particular where this is necessary for compliance with a legal obligation requiring processing under Union or Polish law, and for the establishment, exercise or defence of claims.

2.4 The above requests and rights of data subjects shall be the responsibility of the Controller's designee, provided that all specific conditions described in Articles 15 to 22 of the GDPR are met. The exercise of rights set out in point 2.1 and the provision of any information shall take place without undue delay.

3. Dealing with personal data security breaches

3.1 In the event of a personal data breach, the Controller shall, without undue delay but no later than 72 hours after the breach is identified, notify the supervisory authority thereof, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons.

3.2 When a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Controller shall communicate the breach to the data subject without undue delay, unless there are circumstances referred to in Article 34(3) of the GDPR.

4. Rules for processing data of tenants, their representatives and visitors

4.1 The following information relates to the Company's processing of data of tenants, their representatives and visitors. Tenants are required to provide the following information to all their representatives, visitors and employees whose data they provide to the Company in connection with the Company's provision of rental services for the premises.

PRIVACY NOTICE FOR TENANTS, THEIR REPRESENTATIVES AND VISITORS

This information is provided in accordance with Article 13 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), hereinafter referred to as: the "GDPR".

Data Controller

Szyperska Sp. z o.o. with its registered office in Poznan (61-754) at ul. Szyperska 14, is the controller of your data (hereinafter referred to as: the "Controller").

Contact in personal data matters

You can contact the Controller by sending a letter to the address given above or by sending an e-mail to: rafalproczek@investika.cz .

Purpose of processing	Legal basis for processing
▪ In the case of Tenants who are natural persons, personal data will be processed: ▪ for the purposes necessary for the performance of the contract you have concluded with the Controller; ▪ for the purposes necessary for compliance with legal obligations to which the Controller is subject, in particular those arising from accounting regulations; ▪ for the purposes of the legitimate interests pursued by the Controller, in particular to ensure contact with you prior to entering into and throughout the term of, the contract, to ensure and to establish, exercise or defend potential claims.	▪ Article 6(1)(b) of the GDPR, where processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; ▪ Article 6(1)(c) of the GDPR in conjunction with the Accounting Act; ▪ Article 6(1)(f) of the GDPR, where the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party;
In the case of persons representing a Tenant, or the Tenant's contact persons, employees or visitors, personal data will be processed: for the purposes of the legitimate interests pursued by the Controller such as ensuring contact and performance of the contract, and verification of authority to make declarations of intent on behalf of the Tenant, and ensuring adequate security of the building and access to the premises by authorised persons.	▪ Article 6(1)(f) of the GDPR, where the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party;

Who do we share your personal data with?

The recipients of your personal data may be – on a need-to-know basis – entities working with the Controller in connection with services provided to the Controller and with facilitating its ongoing business processes, in particular IT system and service providers, and other entities providing services to the Controller and facilitating its ongoing business processes (such as property management entities, entities providing courier, consultancy, financial services, etc.). The data may also be shared with the Controller group companies for administrative purposes.

How long will your personal data be stored?

Personal data will be processed for the term of your contract with the Controller, and thereafter for the period of the statute of limitations for any claims under universally applicable law.

Personal data processed for the purpose of complying with the Controller's legal obligations will be processed for the period specified by law.

What rights do you have in relation to personal data processing?

You have the right to:

- access your personal data,
- have your personal data rectified,
- have your personal data erased,
- restrict personal data processing,
- transmit your personal data, including the right to receive data and transmit them to another controller, or to request, if technically feasible, that those data be sent directly to another controller – to the extent that data processing is carried out based on an agreement;
- make a reasoned objection to personal data processing,
- lodge a complaint with a supervisory authority with respect to personal data protection.

Are you obliged to provide personal data? Source of personal data

The provision of personal data is voluntary but necessary for entering to and performing the premises lease agreement and for ensuring adequate access to the premises. In the case of representatives or contact persons, the Controller has obtained these data from the Contractor in the context of the conclusion and performance of the agreement.

What categories of data are processed?

The Controller processes the data of representatives to the extent that such data is indicated in the contract (identification details) and in the National Court Register, and in the case of contact persons – identification details and business contact details.

In the case of employees and visitors of tenants, the Controller may process their basic identification details.

5. Video surveillance

5.1 The following information relates to the Company's processing of video surveillance data. The privacy notice should be given by a reception staff member for reading to all those who have so requested at the reception desk.

PRIVACY NOTICE – SURVEILLANCE

This information is provided in accordance with Article 13 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), hereinafter referred to as: the "GDPR".

Data Controller

Szyperska Sp. z o.o. with its registered office in Poznan (61-754) at ul. Szyperska 14, is the controller of your data (hereinafter referred to as: the "Controller").

Contact in personal data matters

You can contact the Controller by sending a letter to the address given above or by sending an e-mail to: rafalproczek@investika.cz .

Purpose of processing	Legal basis for processing
for the purposes of the legitimate interests pursued by the Company regarding ensuring the safety of persons and the protection of the property of both the Company and the tenants of the premises.	▪ Article 6(1)(f) of the GDPR, where the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party;

Who do we share your personal data with?

Your data may be shared on a need to know basis with recipients who may be entities working with the Controller in connection with services provided to the Controller, in particular companies providing personal and property security services, and other entities providing services to the Controller and facilitating its ongoing business processes – in particular building management entities.

How long will your personal data be stored?

Your data will be processed for 30 days.

What rights do you have in relation to personal data processing?

You have the right to:

- access your personal data,
- have your personal data rectified,
- have your personal data erased,
- restrict personal data processing,
- object to personal data processing,
- lodge a complaint with a supervisory authority with respect to personal data protection.

6. Rules for processing data of employees and representatives of business partners

6.1 The following information relates to the Company's processing of data of employees and representatives of business partners. Business partners are required to provide the following information to all their representatives and employees whose data were provided to the Company in connection with the provision of an agreement.

PRIVACY NOTICE FOR EMPLOYEES AND REPRESENTATIVES OF BUSINESS PARTNERS

This information is provided in accordance with Article 13 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), hereinafter referred to as: the "GDPR".

Data Controller

Szyperska Sp. z o.o. with its registered office in Poznan (61-754) at ul. Szyperska 14, is the controller of your data (hereinafter referred to as: the "Controller").

Contact in personal data matters

You can contact the Controller by sending a letter to the address given above or by sending an e-mail to: rafalproczek@investika.cz .

Purpose of processing	Legal basis for processing
In the case of Business Partners who are natural persons, personal data will be processed: ▪ for the purposes necessary for the performance of the contract you have concluded with the Controller; ▪ for the purposes necessary for compliance with legal obligations to which the Controller is subject, in particular those arising from accounting regulations; ▪ for the purposes of the legitimate interests pursued by the Controller, in particular to ensure contact with you prior to entering into and throughout the term of, the contract, to ensure or to establish, exercise or defend potential claims.	▪ Article 6(1)(b) of the GDPR, where processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; ▪ Article 6(1)(c) of the GDPR in conjunction with the Accounting Act; ▪ Article 6(1)(f) of the GDPR, where the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party;
In the case of persons representing Business Partners, or contact persons, personal data will be processed: for the purposes of the legitimate interests pursued by the Controller such as ensuring contact and performance of the contract, and verification of authority to make declarations of intent on behalf of the Business Partner.	▪ Article 6(1)(f) of the GDPR, where the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party;

Who do we share your personal data with?

The recipients of your personal data may be – on a need-to-know basis – entities working with the Controller in connection with services provided to the Controller and with facilitating its ongoing business processes, in particular IT system and service providers, and other entities providing services to the Controller and facilitating its ongoing business processes (such as property management entities, entities providing courier, consultancy, financial services, etc.). The data may also be shared with the Controller group companies for administrative purposes.

How long will your personal data be stored?

Personal data will be processed for the term of your contract with the Controller, and thereafter for the period of the statute of limitations for any claims under universally applicable law.

What rights do you have in relation to personal data processing?

You have the right to:

- access your personal data,
- have your personal data rectified,
- have your personal data erased,
- restrict personal data processing,
- transmit your personal data, including the right to receive data and transmit them to another controller, or to request, if technically feasible, that those data be sent directly to another controller – to the extent that data processing is carried out based on an agreement;

- object to personal data processing,
- lodge a complaint with a supervisory authority with respect to personal data protection.

Are you obliged to provide personal data? Source of personal data

The provision of personal data is voluntary but necessary for the conclusion of a contract with the Controller. In the case of representatives, employees or contact persons, the Controller has obtained this data from the Business Partner in the context of the conclusion and performance of the contract.

What categories of data are processed?

The Controller processes the data of representatives to the extent that such data is indicated in the contract (identification details) and in the National Court Register, and in the case of contact persons – identification details and business contact details.

In the case of Business Partners, the processing comprises all data necessary for the performance of the relevant obligation, as contained in the contract or a VAT invoice.

7. Personal data entrustment rules

7.1 When the Company entrusts data to external entities (the "Processor"), the following provisions shall apply to the parties, unless a separate entrustment agreement has been concluded.

7.2 In order to fulfil the obligations under the underlying agreement, the Controller entrusts the Processor with the processing of personal data comprising ordinary personal data to the extent indicated and necessary for the performance of the underlying agreement.

7.3 The Processor, by accepting these provisions, declares at the same time that it provides sufficient guarantees to implement appropriate technical and organisational measures so that the processing complies with the GDPR requirements and protects the rights of data subjects and no civil or administrative proceedings are pending against it for improper processing.

7.4 The Processor shall only process personal data at the documented request of the Controller, unless such an obligation arises from a legal provision. In that case, the Processor shall inform the Controller of this legal obligation at least 7 days in advance, unless the Processor is prohibited by law from providing such information due to an important public interest.

7.5 Data processing shall only take place in the territory of the European Economic Area.

7.6 The Processor shall:

a) provide the Controller with all necessary information relevant to the protection of the personal data entrusted to it for processing,

b) may only process personal data provided by the Controller to the extent and for the purpose compatible with the underlying agreement.

7.7 The Processor undertakes to ensure that persons who will carry out processing on its behalf: (i) be appropriately authorised, (ii) have adequate knowledge of personal data protection, and (iii) are bound to secrecy or subject to an appropriate secrecy obligation.

7.8 The Processor undertakes to restrict access to personal data only to duly authorised persons requiring such access for the performance of the underlying contract.

7.9 The Processor shall take all measures, in particular apply technical and organisational measures to ensure the protection of the personal data entrusted for processing, as appropriate to the risks

and categories of personal data to be protected, in particular in accordance with Article 32 of the GDPR, secure personal data from being accessed or taken by unauthorised persons, from being processed in violation of applicable regulations, and from being altered, lost, damaged or destroyed.

7.10 The Processor further undertakes not to disclose information to unauthorised persons about personal data, and the protection measures and safeguards applied by it or the Controller.

7.11 If the Processor becomes doubtful as to the lawfulness of any instructions or orders given by the Controller, the Processor shall promptly inform the Controller thereof.

7.12 In addition, the Processor shall continuously monitor changes in generally applicable laws and, where necessary, notify the Controller of the need to make changes to personal data processing processes or documentation describing them.

7.13 The Processor shall not use the services of a different processor (the "Subprocessor") without the Controller's prior consent (the "Subentrustment") expressed at least in document form.

7.14 The Processor shall ensure that Subprocessors are subject to the same personal data protection obligations as the Processor hereunder (in particular the obligation to implement appropriate technical and organisational measures, and guarantee the power of the Controller to directly exercise, towards the Subprocessor, the rights it has towards the Processor to audit or inspect the processing of the entrusted personal data referred to in the Entrustment Agreement).

7.15 Full liability for the Subprocessor failing to comply with its personal data protection obligations towards the Controller shall lie with the Processor.

7.16 Taking into account the nature of personal data processing, the Processor shall, to the extent possible, assist the Controller via appropriate technical and organisational measures in complying with its obligation to respond to data subjects' requests in exercising their rights set out in Chapter III of the GDPR. The Processor shall notify the Controller at the latest within 3 business days of receiving any such request and shall consult the Controller prior to responding to that request.

7.17 Taking into account the nature of personal data processing and available information, the Processor shall assist the Controller in complying with the obligations set out in Articles 32 to 36 of the GDPR.

7.18 The Processor shall promptly make available any information to the Controller, upon request, as necessary to demonstrate compliance with the obligations set out in the Entrustment Agreement and the GDPR.

7.19 The Processor shall immediately, but no later than within 24 hours of becoming aware of the information - inform the Administrator of any breach of security of the personal data entrusted to the Processor (i.e. unauthorised or unlawful personal data processing, loss, destruction or damage).

7.20 In the case referred to above, the Processor shall provide the Controller with all possible and detailed information referred to in Article 33 of the GDPR, in particular including the date and time of the occurrence and becoming aware of the breach, a description of any circumstances, the category and approximate number of personal data records affected by the breach, a description of the potential consequences and the remedial measures taken by the Processor.

7.21 The Processor shall promptly inform the Controller of any legal or administrative proceedings relating to the personal data entrusted to the Processor, including issued administrative decisions, as well as any performed inspection of the processing of such personal data.

7.22 The Processor shall be liable for any damage caused to third parties due to any improper processing of personal data by the Processor.

7.23 The Processor shall be fully liable for any damage suffered by the Controller and the persons whose personal data has been entrusted to the Processor for processing if such damage results from the Processor's actions in violation of the GDPR, national data protection statutes and the provisions hereof.

7.24 The Controller may audit (having previously agreed the date and scope of the audit with the Processor) the manner in which personal data is processed by the Processor that shall provide the Controller with all information necessary to demonstrate compliance with the obligations set out herein. In the course of the audit, the authorised representatives of the Controller are authorised, in particular, to enter the premises where the personal data is processed, request information on the course of personal data processing (including agreements), and inspect documentation and IT systems to verify the applied personal data processing safeguards.

7.25 The Processor shall, upon termination of the Entrustment Agreement, no longer process the personal data entrusted to it and shall return all such personal data to the Controller and delete all existing copies thereof.