Process Guarantor:		Publication No.: 1 Issue: 1 Version: 1 Number of Appendices: 1
DIRECTIVE No. 1/2018		
Wings4U, s. r. o. **Personal Data Protection**		
Date of entry into force: 2 Apr. 2018		

CONTENT

Changes and Amendments to Document

Change No.	Change ID	Subject of Change	Date	Processor

Document Revisions

Change No.	ID	Result of revision	Date	Processor
1				
2				
3				

1 Purpose

This directive sets out details on the rights and obligations of Wings4U, s. r. o. (hereafter "W4U") employees when processing personal data and the basic technical-organizational measures needed to ensure personal data protection in compliance with the provision § 13 par. 2 of the Act No. 101/2000 Coll., on Personal Data Protection and changes to certain laws in its most recent version (hereafter "law") with the aim of achieving a unified process for personal data protection within the conditions at W4U.

Subject to protection, per the terms of this directive, is all processing of personal data done by W4U employees, or eventually other persons, who process personal data based on contracts with W4U.

2 Scope of Coverage

This directive is binding for all employees and external employees/collaborators and suppliers (physical entities doing business) of W4U.

3 Abbreviations, Definitions and Terms

3.1 Abbreviations Used

PDPA Personal Data Protection Authority

3.2 Definitions and Terms

For the purposes of this directive:

3.2.1 **Personal Data** is any information related to a defined or definable personal data subject. A personal data subject is considered as defined or definable provided the personal data subject can be identified directly or indirectly based primarily on their name, code, ID label or one or more elements specific to their physical, physiological, mental, economic, cultural or social identity, telephone or email contacts including identifiable IP addresses or cookies.

3.2.2 **Sensitive Data** is personal data revealing information on nationality, race or ethnic origin, political views, union memberships, religion or philosophical convictions, criminal records (convictions), state of health and sex life of the personal data subject and genetic data of the personal data subject; sensitive data also includes biometric data that enables the direct identification of the subject or authentication of personal data subjects.

3.2.3 **Personal Data Subject** is a physical entity to whom personal data relate.

3.2.4 **Personal Data Administrator** (hereafter "admin") is W4U.

3.2.5 **Personal Data Processor** is any subject who, based on a specific law or authorization by an admin, processes data according to the law.

3.2.6 **Authorized Employee** is a W4U employee who has been chosen to process personal data.

3.2.7 **Authorized Subject** is a person who is authorized to familiarize themselves with personal data and whose authorization derives from a specific law or a contract (namely monitoring bodies, the Czech police force, courts, processors, service providers, etc.).

3.2.8 **Recipient** is any subject that has been given access to personal data.

3.2.9 **Processing Personal Data** is any operation or set of operations that are systematically done with personal data regardless of whether they are automated or done with other resources. This involves primarily collecting/gathering, storing on data media, accessing, editing or altering, searching, using, transferring, disseminating, publishing, archiving, exchanging, sorting or combining, blocking or liquidating personal data.

3.2.10 **Automated Processing of Personal Data** is processing that includes the operations:

- storage on data media
- carrying out logical or arithmetic operations with the data; changing, deleting, searching or extending, done in full or partially, using automated processes.

3.2.11 **Manual Processing of Personal Data** is any processing of data with the exception of automated processing (in paper form, documents).

3.2.12 **Archives (Record Keeping)** are an archive of databases serving to protect personal data (e.g. databases for the purpose of processing, databases allowed for the transfer of personal data to foreign countries, databases of contracts on processing, etc.).

4 Description

4.1 Basic obligations for personal data protection

4.1.1 The administrator stipulates the purpose, resources and means of processing personal data prior to beginning the actual processing of personal data.

4.1.2 In the event that provisions in the act on exemption from seeking consent (§5 par. 2 of the act) do not apply to the particular purpose for personal data processing, the administrator is obligated to ask the personal data subject for consent to processing of this data. When soliciting consent, the administrator must inform the personal data subject and educate them in compliance with items 4.1.3 and 4.1.4 of this directive. The administrator is obligated to prepare consent always in written form. Consent must be demonstrable for the full duration of the processing; it must be defined or limited to a clear purpose, including setting a deadline up to which consent is valid. In the event the personal data subject does not provide consent, their personal data cannot be processed on grounds other than justifiable/authorized or legal ones (e.g. due to a contract relationship).

4.1.3 In the event that the provisions in the act on exemptions from informational obligations (§ 11, par. 3 of the act) do not apply to the relevant purpose for personal data processing, the administrator is obligated to inform the personal data subject about the collecting of personal data, i.e. inform the person (§ 11 par. 1 of the act) of the following:

a) purpose and scope of processing personal data;

b) who will process the personal data and in what way;

c) who will be given access to the personal data;

d) of their rights to access personal data, to correction of personal data and to protection of data (i.e. right to ask for clarification or correction: blocking, making corrections, adding information or destroying data).

Provided consent to the processing of personal data is required per item 4.1.2 of this directive, the administrator is obligated, as part of their informational obligations, to inform the personal data subject as well about who the administrator will be and for what period consent is granted.

4.1.4 In the event the administrator obtained personal data directly from the personal data subject, the administrator must inform them whether provision of personal data is voluntary or mandatory, and in the event of mandatory provision they must share the results of refusal to provide the data (§ 11 par. 2 of the act). Prior to processing sensitive data, the administrator for the personal data subject must inform the subject of the right to access information (§ 12 of the act) and the right to request an explanation or correction (§ 21 of the act).

4.1.5 Notices on the processing of personal data are submitted to the Personal Data Protection Authority (hereafter PDPA) as follows:

a) the administrator prepares a notice on the processing of personal data for the PDPA by filling out a registration form, *Notice on Processing (Changes in Processing) of Personal Data*, according to § 16 of the act. The form is available on the website (www.uoou.cz) in the "Register" section. The administrator sends the notice to the PDPA in electronic format only;

b) the provisions in the previous paragraph relate to fulfilling changes already announced (registered) for information on processing personal data (the entire form must be filled in including the assigned registration number);

c) the administrator is obligated to notify the PDPA of personal data to which notification obligations relate; including notifications on the way they handled the personal data.

Provided the processing of personal data is not subject to the notification obligations vis-à-vis the PDPA, but still the information on processing has to be made accessible to the public in a suitable way (§ 18 of the act), the administrator carries out this obligation by publishing the notification on the W4U website.

4.1.6 The administrator must cease the processing of personal data as soon as the purpose thereforE expires or based on a request by the personal data subject (§ 21 par. 1 letter b) of the act). Personal data that cease to be processed must be destroyed, unless there are exceptions stipulated by special laws for the following:

a) storing personal data for the purpose of archiving;

b) storing personal data for the purpose of exercising rights as part of a civil court case, a criminal case or an administrative case (§ 20 par. 2 of the act).

4.1.7 When handing over personal data to other countries, the administrator must proceed in compliance with legal requirements (§ 27 of the act). In cases stipulated by the law, the administrator is obligated to ask the PDPA for permission to share personal data in a manner that is specified on the PDPA website.

4.1.8 Processors can process personal data for W4U only based on concluded (signed) contracts. The relevant contract must always include the following:

a) the scope and conditions for processing personal data;

b) the purpose of processing personal data;

c) the period for which the contract is valid;

d) guarantees (e.g. in the form of mutually confirmed rights and obligations between W4U and the processor for processing personal data) by the processor on technical and organizational measures ensuring personal data protection;

e) commitment to maintaining confidentiality of personal data and implementation of measures to protect it even after the contract ceases to be valid;

f) sanctions that the administrator will enforce in cases of breach of contract.

Media with personal data that pass through the hands of the processors are to be handed over by the administrator in compliance with a written contract concluded with the processor provided the law or a special law does not stipulate otherwise. The administrator will hand over media with personal data that are passed on to other authorized subjects (namely service providers, courts or police authorities, or other bodies in the public administration) based on a transfer protocol or a similar document.

4.1.9 Administrator employees who come into contact with personal data at the workplace of the administrator are obligated to maintain confidentiality of personal data and on security measures whose publication could endanger the security of the personal data. The obligation to maintain confidentiality remains intact even after termination of employment.

4.2 Exercising of rights and obligations for personal data protection

4.2.1 Only employees and external employees of W4U ensuring the technical administration of processing personal data, authorized employees and processors with whom a relevant contract has been concluded (see item 4.1.8 of this directive) can come into contact, within the company, with personal data. Authorized employees of W4U will execute under the company's internal conditions the rights and obligations assigned to them per the law and this directive.

4.2.2 The authorized person/W4U employee is obligated to

a) stipulate the purpose, resources for and means of processing personal data (see Item 4.1.1 in this directive);

b) ensure fulfillment of the notification duties for processing personal data, i.e. vis-à-vis cases stipulated in the law (see Item 4.1.5 in this directive);

c) prepare, using the electronic form, information on processing personal data meant for the public (public use) and send it to the authorized employee, who will ensure its placement on the W4U website. In case of changes to public information, proceed in a similar manner;

d) ensure the destruction (liquidation) of personal data (see Item 4.1.6 in this directive);

e) determine an authorized W4U employee and stipulate the scope and conditions under which they can process personal data. Proceed in a similar way in cases where this definition is changed/altered;

f) conclude contracts with data processors in the manner outlined in Item 4.1.8 of this directive;

g) carry out monitoring activities (checks) on the protection of personal data; in cases where deficiencies are discovered, then propose measures for rectifying them;

h) set conditions for authorized employees for the storing of data on data media (this applies to data containing personal information) in a properly secured location (site); e.g. a lockable room or cabinet, in a safe, in a filing room, etc.);

4.2.3 When executing his/her rights and obligations for protecting personal data, the W4U executive is further liable for the following:

a) requesting (obtaining) personal data subjects' consent to the processing of their personal data (with the exception of cases where the processing thereof is set out in the law or it is exempted from this obligation);

b) providing information and guidance on the rights of personal data subjects as stipulated by law;

c) processing of only exact personal data in compliance with the purpose of processing;

d) storing personal data only for the purposes for which it has been gathered/collected;

e) open collecting of personal data, i.e. for no other purpose or activity than those declared;

f) protection of data subjects' rights (§ 21 of the act);

g) will not combine (aggregate) personal data obtained for different purposes;

h) demonstrable familiarizing of authorized employees with this directive;

i) fulfillment of obligations without undue delay; deletion of our personal data provided it is prescribed for one of the following reasons:

   1) the personal data are no longer needed for the purpose for which they were collected or processed;

   2) the citizen revokes his/her consent (provided processing is based on consent) and there are no other legal grounds for processing (the data);

   3) the citizen raises an objection against the processing on grounds of authorized interests of the personal data administrator, such as maintaining employee records;

   4) personal data have been processed in breach of the law;

   5) legal obligations stipulated by EU law or that of a member state.

4.2.4 The authorized employee is obligated as part of his/her duties to fulfill measures for protection of personal data stipulated by law and in this directive, mainly:

a) process personal data per conditions and in the scope stipulated by the law and this directive;

b) request the personal data subject's consent (with the exception of cases where the law allows for exemptions from this obligation). In cases where the relevant personal data subject does not give consent, do not process the personal data and immediately inform the authorized person in the company about this fact;

c) provide personal data subjects information, in written form, as required by law and guidance on their rights;

d) process only exact personal data in compliance with the purpose of processing;

e) collect/gather personal data only in compliance with the stipulated purpose and in the scope necessary for processing;

f) store personal data only for the period that is essential for the purpose of processing and which is stipulated as part of eventual consent. Should you determine that the purpose for processing specific personal data has expired, inform W4U executives about this fact;

g) process personal data only for the purposes for which it has been collected;

h) collect/gather personal data only in an open matter; i.e. not for any purposes or activities other than those declared;

i) do not combine personal data acquired for different purposes;

j) submit, at the request of the personal data subject, an explanation or rectify any status where processing of personal data is in breach of protection of privacy or the subject's personal life or is in breach of the law (mainly by means of blocking, making corrections, adding (information) or destroying personal data) - § 21 of the act;

k) handover, without unnecessary delay, at the request of the personal data subject information on the processing of their personal data (§ 12 of the act);

l) store devices containing personal data in a fully-secured location (site) and proceed such, when working with them, so that no other person could use these devices/media as an information source;

m) hand over personal data (in print or electronic form) only when authorized to do so. Personal data is to be handed over only to other authorized employees, processors or other authorized subjects;

n) carry out regular destruction of documentary materials (hand-written documents, drafts, notes) used for processing; this using adequate technical and software resources (e.g. shredders);

o) do not make copies of data storage media with personal data, or of personal data as such, for purposes other than work-related ones and do not allow others to do so. Treat copies made the same as you would original documents;

p) make sure persons who do not have authorization to process personal data cannot do so;

q) inform, without delay, W4U executives in the event you have discovered that personal data protection measures have been breached (also if you suspect such a breach);

r) ensure that physical entities authorized to use systems for processing personal data have access only to personal data that corresponds with their authorization (level); and this based on special user permissions set up exclusively for these entities (persons);

s) make electronic records that help determine and verify when, by whom and for what purposes personal data has been recorded or otherwise processed;

t) preventing unauthorized access to data storage media;

u) carrying out encryption and anonymization of personal data;

v) ability to ensure constant confidentiality, integrity, availability and resilience of systems and processing services: the introduction of measures and their proper functioning will be checked regularly;

w) ability to recover the availability of personal data and access thereto in a timely manner in the event of physical or technical incidents; and

x) regular testing, evaluation and assessment processes on the effectiveness of implemented technical and organizational measures to ensure the security of processing (to be done by an external auditor);

y) firewall tool; anti-virus tools and tools for checks on unauthorized access;

z) encrypted data transfer using information technologies (IT);

aa) data backup is done by the mother company and to another site via encrypted data transfer and only authorized W4U personnel have access thereto;

bb) when processing personal data, personal data will be stored exclusively on secured servers or on secured data storage devices, should this involve personal data in electronic format;

cc) when processing personal data in formats other than electronic format, this personal data will be stored in locations (sites) with adequate levels of security to which only authorized persons will have exclusive access.

5 Related Documents

- Act No. 101/2000 Coll., on Personal Data Protection and on changes to related laws in their most recent versions;

6 Final Provisions

Breach of the obligations stipulated in this directive, or of the act, can be classified as breach of work obligations, and this in a severe manner, as a misdemeanor or felony by law.

This directive enters into force on 2 Apr. 2018.

7 Appendices

Appendix 1: Personal data identification and classification at W4U

Appendix 2: Persona data protection training plan and Security Ten Commandments for W4U IS users