EMPLOYER'S INTERNAL REGULATION
No. 1/2018

dated 10 May 2018

EP Global Commerce a.s.
based at Pařížská 130/26, Josefov, 110 00 Praha 1
ID No.: 05006350
("company")

Article 1
Purpose and Binding Nature of Internal Regulation

1.1 This internal regulation defines the rules governing the processing of personal data within the framework of the company's business and the handling of personal data in accordance with the generally binding laws, which as of publication of this internal regulation are primarily Act No. 101/2000 Coll., on the protection of personal data and on the amendment to certain laws, as amended ("law") and EU Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("regulation").

1.2 This internal regulation is binding for all employees and other co-workers of the company, as defined in Art. 2 g) and j) of this regulation.

Article 2
Definitions

2.1 For the purposes of this internal regulation the following terms have the definitions given below:

a) **personal data** – any information which in itself or with other information may directly or indirectly result in the identification of data subjects. Personal data includes first name and surname, if stated together with the address. Information is not classed as personal data if a disproportionate amount of time, effort and material resources is needed to determine the identity of data subjects.

b) **sensitive data** or also **special data** - personal data indicating the nationality or racial or ethnic origin of data subjects, political attitudes, membership of trade unions, religion and philosophical beliefs, convictions for a criminal offence, state of health and sexual life of data subjects and the genetic data of data subjects; sensitive data also includes biometric data enabling the direct identification or authentication of data subjects.

c) **data subject** - the individual to which the personal data relates.

d) **processing of personal data** – any operation or set of operations systematically performed with personal data by the controller or processor, either automated or otherwise. The processing of personal data particularly means the collection and storage of information on media, disclosure, modification or editing, searching, use, transfer, dissemination, publication, storage, replacement, sorting or combination, blocking and liquidation of data.

e) **controller** – any entity that determines the purpose and means for the processing of personal data, processes such data and is liable for it. The controller may authorise or empower a processor to process personal data, unless the applicable laws specify otherwise.

f) **processor** – an entity that processes personal data for the controller and as instructed by the controller

g) **employee** - 1) employees, 2) persons performing work on the basis of non-employment agreements, 3) members of the company's bodies and 4) interns

h) **job applicant** - 1) job applicants, 2) candidates for positions as members of the company and 3) applicants for internships

i) **business partner** – an individual who has concluded a contract with the company, under which services are provided by the company or by a business partner.

j) **company co-worker** – persons working for the company on the basis of an agreement other than an employment or other such contract

Article 3
Subjects of personal data

3.1 The company processes the personal data of the following data subjects:

a) job applicants,
b) employees,
c) company shareholders - individuals,
d) company co-workers,
e) independent business partners of the company, their employees and co-workers,
f) persons interested in doing business with the company.

3.2 The processing of subject's personal data is governed by the principles specified in Article 4 of this regulation.

Article 4
Principles for the Processing of Personal Data

4.1 Personal data must be processed in strict compliance with the principles specified in this article. Failure to abide by these principles constitutes a breach of the obligations stipulated by the Act on the Protection of Personal Data and the regulation.

4.2 Each instance of processing personal data must have a designated purpose and must be based on one of the legal titles specified in Article 5.1 of this regulation. For details, see Article 5 of this regulation.

4.3 Before personal data is actually first processed the data subject must be informed of the terms under which it is processed. Information memoranda are used for this purpose. For details, see Article 7 of this regulation.

4.4 Personal data may be processed only to the extent necessary for the given purpose, and for the amount of time necessary. If personal data is found to be redundant or no longer needed, the processing of that data must be ceased and the data must be deleted. For details, see Article 9 of this regulation

4.5 It is essential to adopt and ensure full compliance with technical and organisational measures to secure personal data. Details are given in Article 8 of this regulation. If the company contracts the processing of personal data out to a third party (processor), it always does so on the basis of a written agreement, which specifies the technical and organisational measures the processor is obliged to adopt to protect personal data. If these measures are not implemented or fail, the procedure defined in Art. 10 of this regulation must be followed.

Article 5
Legal Titles and Purposes of Processing

5.1 The company processes personal data on the basis of the following legal titles:

a) compliance with obligations arising from the law,
b) performance of contracts,
c) the company's legitimate interests,
d) the consent of data subjects.

5.2 The list of purposes for which data is processed and the associated legal titles are contained in the information memoranda, which form the annex and an integral part of this regulation.

5.3 If the legal title for processing personal data is the company's legitimate interest, before processing starts it must be assessed whether that interest outweighs the interest of data subjects in the protection of their personal data (balance test). This assessment is made in writing. The details of the test procedure are as specified in the balance test methodology.

5.4 If personal data is processed on the basis of the consent of data subjects, that fact is recorded in the consent register. Consent is obtained in accordance with the methodology for acquiring consent.

Article 6
Information Memorandum

6.1 Information memoranda for the individual categories of data subjects form the annex and an inseparable part of this regulation. These are documents intended to inform data subjects of the terms under which their personal data is processed.

6.2 Information memoranda are available in electronic form on the company website and are also available in paper form at the company's headquarters.

6.3 The information memorandum may be physically provided to data subjects before processing starts on their personal data (e.g. as an annex to the contract) or a link to the memorandum may be provided.

Article 7
Exercising of Data Subjects' Rights

7.1 The data subject has the following rights, which are exercised through the company as the controller:

a) the right to information about how personal data is processed (as given in the information memorandum - see Article 6 of this regulation)
b) the right to access to personal data, i.e. the right to confirmation from the company of how its personal data is processed and under what terms and the right to acquire copies of such personal data
c) the right to correct personal data
d) the right to delete personal data
e) the right to restrict the processing of personal data
f) the right to the portability of personal data
g) the right to file an objection against the processing of personal data
h) the right to revoke consent to the processing of personal data at any time

7.2 The company is obliged to accept requests from data subjects to access their personal data by all means of communication, assuming that the identity of the applicant is adequately verified. However, if the right is exercised pursuant to Art. 7.1. h) of this regulation, the revoking of consent must be no more complicated than the granting of such consent.

7.3 Requests filed by a data subject must be processed as soon as possible, no later than within one month of receipt of the request. This deadline may be extended in exceptional cases, given the complexity of the case.

Article 8
Organisational and Technical Measures to Protect Personal Data

8.1 The company is obliged to adopt and maintain organisational and technical measures to protect personal data. This article specifies the nature and scope of such measures.

8.2 The company's headquarters is situated in a building with an electronic security system, connected to a continuous security agency service. The entrance to the company's premises is secured.

8.3 The access key and access chip may only be provided to employees with an employment contract and selected co-workers of the company. If the key or chip is lost to an unauthorised person, the lock must be changed immediately, or the access chip blocked.

8.4 Upon termination of an employee's employment contract or a co-worker's contract with the company, the access key and/or access chip must be returned immediately.

8.5 Third parties may only access the company's premises or its branches in the presence of employees or co-workers of the company. Third parties must announce themselves at the company's reception desk. It is prohibited for third parties to move around the company's premises unaccompanied.

8.6 Personal data processed in paper form is stored in lockable rooms or safes, lockable drawers and cabinets.

8.7 Personal data processed in electronic form is stored on servers which are regularly backed up as standard. The company's servers are situated in:

a) the company's headquarters (server room);
b) secure premises with an external IT contractor.

8.8 The company's information system is protected against unauthorised external access, particularly by the appropriate firewall, intrusion detection, antivirus system, and similar methods. Access through the firewall is regularly checked.

8.9 Personal data may only be accessed by persons authorised to process such data by the company. Access to the company's information system is protected by the individual password of each employee or co-worker. If the employment contract or other contractual relationship is terminated, a member of the IT department is obliged to immediately cancel that employee or co-worker's access.

8.10 Company employees and co-workers are obliged to keep their passwords secret and ensure that they cannot be obtained by third parties. In the event that a password is obtained by a third party, the relevant employees or co-workers are obliged to immediately change their password and report the fact to an employee of the IT department.

8.11 Accessing the company's information system with someone else's password is prohibited. This does not apply if the employee's or co-worker's contract with the company has been terminated and tasks cannot be performed for the company in any other way.

8.12 A member of the IT department and the external IT services contractor are responsible for managing passwords and access rights.

8.13 Personal data may only be copied in order to carry out work tasks and only to the extent necessary for the purpose. The copying of personal data in electronic form to the hard disk of individual computers or other media is only permitted provided that access to such data is blocked by the access password of the given employee or co-worker.

8.14 Personal data in paper form transferred outside the company is handed over in person, via post or via a courier. When personal data is provided via electronic mail the e-mails are encrypted.

8.15 Personal data may also be processed outside the company premises. Personal data is processed outside the company premises by company employees and co-workers working on a home-office scheme and/or who have an electronic device with remote access. An employee or co-worker possessing personal data outside the company premises or a branch of the company is responsible for protecting such data against unauthorised access.

8.16 Employees are entitled to use the company's production and work equipment, including computers and telecommunication equipment, for their personal use. When doing so employees are obliged to comply with all the security measures when using the company's production and work equipment, particularly as regards encryption, the use of user accounts and the use and handling of passwords.

8.17 Company employees and co-workers are obliged to maintain strict confidentiality regarding the data they process and the security measures adopted by the company to protect such data. The duty of confidentiality continues to apply after the termination of an employment or other contractual relationship.

Article 9

Archiving and Liquidation of Personal Data

9.1 The company is obliged to archive personal data according to the type of document it is contained in.

9.2 Company employees and co-workers are obliged to liquidate personal data as soon as the reason for processing it ceases to apply.

9.3 Paperwork containing personal data is liquidated using a shredder or external shredding firm.

9.4 Personal data in electronic form is liquidated by deleting the data from the server, from the backup disk or other medium.

Article 10

Security Incidents and How They Are Dealt With

10.1 A security incident is any incident which could potentially endanger the security, credibility, availability or integrity of personal data. A security incident may involve failure to follow the rules for the protection of personal data specified in Article 8 of this regulation, or another incident resulting in the loss, unauthorised use or disclosure of personal data.

10.2 Company employees and co-workers are obliged to immediately report each security incident that comes to their attention and which has not yet been reported, to their superior.

Article 11

Final Provisions

13.1 Existing employees of the company and its co-workers were acquainted with this internal regulation on the date it was published. Each new employee and co-worker must be acquainted with this internal regulation before starting work or cooperation.

13.2 This internal regulation is issued for an indefinite period, although will be updated at regular intervals.

13.3 This internal regulation becomes valid and effective upon publication. This internal regulation repeals and fully supersedes all previous regulations and measures relating to the protection of personal data within the company.