



Informational Memorandum on the Processing of Employees' Personal Data

Owner (Department):

Compliance

Contents

Contents	1
Purpose of this Document	2
1. Contact	2
2. Categories of Personal Data	2
3. Method of Obtaining Employees' Personal Data	4
4. Period for Which Employees' Personal Data Are Processed	5
5. Recipients of Employees' Personal Data	5
6. Place of Processing of Employees' Personal Data	6
7. Method of Processing Employees' Personal Data	6
8. Purpose of Processing Employees' Personal Data	6
8.1.1 Performance of the Contract Concluded with the Employee	6
8.1.2 Fulfilment of Legal Obligations	7
8.1.3 Fulfilment of the Employer's Legitimate Interests	7
8.1.4 Fulfilment of Purposes Defined in Consent to Personal Data Processing	8
9. Employees' Rights in the Area of Personal Data Protection	8
10. Annex - Facultative	9
Abbreviations Used	9



Purpose of this Document

This information describes how, for what purpose, and to what extent BlueLink International CZ s.r.o., with its registered office at Na Florenci 2116/15, 110 00 Prague 1, Company ID No.: 26762030, registered in the Commercial Register maintained by the Municipal Court in Prague, Section C, Insert 91995 (hereinafter the “Employer”), processes the personal data of its employees and further provides information on the rights employees have in connection with the processing of their personal data.

The processing of personal data is carried out by the Employer as controller in accordance with 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 (hereinafter the “GDPR”), and related applicable legislation.

All processing of your personal data takes place only to the necessary extent, always taking into account the type and category of personal data and with the aim of preserving your privacy to the greatest possible extent. As the Employer, we always assess whether a given processing activity is necessary and whether it disproportionately interferes with your rights and freedoms as data subjects.

We retain your personal data only for the period necessary to fulfil the purpose of the processing. Our interest is to retain only up-to-date and accurate data, and therefore we continuously update the personal data processed. Appropriate security of your personal data is an essential part of proper personal data processing. For this purpose, we have implemented measures to ensure sufficient protection of your personal data against any unauthorized access.

1. Contact

The controller of your personal data is the Employer, BlueLink International CZ s.r.o., with its registered office at Na Florenci 2116/15, 110 00 Prague 1, Company ID No.: 26762030, registered in the Commercial Register maintained by the Municipal Court in Prague, Section C, Insert 91995.

If anything remains unclear after reading this document, you may contact the Data Protection Officer with any questions or when exercising any of your rights in the area of personal data protection, at:

-

2. Categories of Personal Data

2.1 The Employer processes the following categories of employees’ personal data as controller:

- Identity data of the employee:** first name, surname, permanent residence, date of birth, place of birth, nationality, identity card number or, where applicable, number of another identity document, and in the case of a foreign national also data pursuant to the relevant legal regulations, in particular the Employment Act.
- Personal identification number of the employee:** processed with respect to the special protection regime applicable to personal identification numbers under currently valid legislation and processed



exclusively where required by a specific legal regulation, in particular for communication with public authorities in connection with taxation of employee income and payment of social security and health insurance contributions.

- c. **Personal contact details of the employee:** email address and telephone number.
- d. **Work contact details of the employee:** email address and telephone number.
- e. **Employment-related data concerning the employee:** employee number, job title, information on whether the employee is a foreign national working in the Czech Republic, salary/remuneration including fixed and variable components, date of commencement of work, effective date and termination date of the employment contract or any agreement on work performed outside an employment relationship, duration of the employment relationship, information on weekly working hours, place of work, and other data pursuant to Section 37 or Section 77a of the Labour Code.
- f. **Other personal data:** contained in the employment contract or any agreement on work performed outside an employment relationship and, in the case of an employee who drives a passenger car in connection with performance of the agreed type of work, personal data contained in the driving license.
- g. **Data concerning the employee's personal life:** marital status, names and surnames of children, dates of birth of children, personal identification numbers of children, and data contained in documents submitted by the employee to the Employer in connection with annual tax settlement, in particular mortgage agreements, insurance contracts, land registry extracts and similar documents.
- h. **Professional data of the employee:** previous employers, experience, previous positions, salary previously achieved, education, and other data contained in the CV submitted by the employee.
- i. **Financial data:** data for payment of salary and other benefits to the employee, including bank name, account number and IBAN.

2.2 The Employer further processes special categories of employees' personal data, i.e. sensitive data, to the following extent:

- a. Information on any initial, periodic, extraordinary and, where applicable, exit medical examinations and occupational health and safety training, health status and disability information.
- b. Information on the employee's criminal integrity to the extent set out in extract(s) from the Criminal Register submitted by the employee.
- c. Biometric data of the employee for the purposes of employee login to devices, applications, online services and networks, as described below, provided that the employee has chosen this method of login voluntarily.
 - i. Fingerprint Authentication
 - The fingerprint reader scans the employee's finger.
 - The system converts unique points and patterns into a numerical code, which is stored in the secure hardware part of the processor.
 - When logging in, the reader scans the finger again and recreates a code which it compares with the stored code.
 - i. Facial Authentication
 - An infrared camera illuminates the employee's face with invisible light.
 - A pattern projector projects a grid of points onto the face and an infrared sensor then creates a detailed depth map.
 - The data from the camera is converted into a unique numerical mathematical model.



- These biometric data are not stored anywhere as a classic photograph.
- The data are stored only on the device.
- On each subsequent login, the system scans the face again, compares it with the stored mathematical model and, if there is a match, logs the employee in.

The above applies on condition that the employee voluntarily chooses this login method.

- 2.3 The Employer also processes personal data in the form of video recordings captured by the CCTV system installed at the workplace, including date, time and location data, under the conditions set out in the Employer's internal regulation, which is available to employees on the Employer's intranet.
- 2.4 The provision of personal data for the purposes under Sections 8.1.1 to 8.1.3 is a statutory requirement, as without the provided data the Employer could not fulfil its legal obligations. For the purposes under Section 8.1.4, provision is voluntary, i.e. at the employee's discretion, and failure to provide personal data for these purposes has no consequences for the employment relationship between the employee and the Employer.

3. Method of Obtaining Employees' Personal Data

- 3.1 The Employer obtains personal data primarily directly from employees, namely:
- a. For the purpose of deciding on the establishment of an employment relationship.
 - b. For the purpose of preparing all documentation necessary for the establishment of an employment relationship.
 - c. As provided during the duration of the employment relationship.
- 3.2 In exceptional cases, the Employer obtains employees' personal data from third parties, such as a bailiff, insolvency administrator or other public authority.
- 3.3 If personal data are obtained pursuant to Section 3.2, the Employer informs the employee within a reasonable period, no later than one month after obtaining the personal data, of the source from which the personal data originate.
- 3.4 The personal data referred to in Section 2.3 are obtained by the Employer from the CCTV system, in particular for the purpose of protecting the property of the Employer and third parties, protecting the life and health of persons, ensuring workplace safety, preventing unlawful conduct, and clarifying damage-related or other incidents. Details of the operation of the CCTV system are governed by the Employer's internal regulation, which is available to employees on the Employer's intranet.
- 3.5 The personal data referred to in Section 2.2 (c) are obtained by the Employer from employees on the basis of consent to the processing of personal data.



4. Period for Which Employees' Personal Data Are Processed

- 4.1 The Employer processes employees' personal data for the duration of the employment relationship with the employee, further pursuant to Section 4.3, and, where applicable, for the period specified in the consent to personal data processing.
- 4.2 On the date of termination of the employment relationship, the Employer deactivates the employee's profile in its systems and will continue to process the employee's personal data stored in the systems only in accordance with Section 4.3.
- 4.3 In relation to certain personal data of the employee, the Employer has a legal obligation to retain such data even after termination of the employment relationship, for the period defined by the relevant legal regulations. This primarily concerns personal data included in:
 - a. Copies of pension insurance records.
 - b. Accounting documents.
 - c. Records of social security insurance premiums and contributions to the state employment policy.
 - d. Payroll sheets or accounting records concerning data required for pension insurance purposes, where accounting records of these facts always include documents on the type, commencement and termination of the employment relationship, records of occupational accidents and occupational diseases, and working time records including unpaid leave records.
- 4.4 For the purposes of defending the Employer's rights and claims in any dispute arising in connection with the employment relationship with the employee, the Employer is entitled to retain the employee's personal data, or documents containing the employee's personal data, which it may need for these purposes.
- 4.5 Personal data obtained from the CCTV system are processed by the Employer for the period set out in the Employer's internal regulation, which is available to employees on the Employer's intranet.

5. Recipients of Employees' Personal Data

- 5.1 Depending on the purpose of processing employees' personal data pursuant to Article 8, the Employer may disclose employees' personal data to the following recipients:
 - a. Relevant state administration authorities, such as law enforcement authorities, tax administrators, financial supervisory authorities and social security authorities.
 - b. Relevant courts.
 - c. Contractual partners of the Employer, such as payroll/HR providers, IT providers, occupational health providers.
- 5.2 Personal data are disclosed to recipients only to the extent necessary and in the form necessary to achieve the purpose of processing personal data. In the case referred to in Section 5.1(c), personal data are disclosed only to contractual partners with whom the Employer has signed agreements protecting the rights and freedoms relating to employees' personal data.



6. Place of Processing of Employees' Personal Data

- 6.1 Personal data are processed and stored in the European Union. In electronic form, personal data are processed by the Employer's contractual partners. Paper documents containing personal data are stored by the Employer on the Employer's premises with restricted access and also by the Employer's contractual partners.
- 6.2 Before transferring employees' personal data, the Employer always carefully assesses all circumstances so that the protection of such data reaches an appropriate level.

7. Method of Processing Employees' Personal Data

- 7.1 The Employer processes employees' personal data both manually and automatically.
- 7.2 Automated processing of employees' personal data takes place in the Employer's information system, which is owned by the Employer. The Employer does not carry out automated decision-making within the meaning of Article 22 GDPR
- 7.3 The Employer has adopted measures ensuring that only authorized and trained employees of the Employer and personal data processors have access to employees' personal data and that such employees and processors maintain confidentiality regarding employees' personal data.
- 7.4 The Employer has concluded written personal data processing agreements with all processors, under which the processors are obliged to ensure such security of employees' personal data as includes identical safeguards for personal data processing processes at those processors as those established by the Employer.

8. Purpose of Processing Employees' Personal Data

- 8.1 The Employer processes employees' personal data for the following purposes:

8.1.1 Performance of the Contract Concluded with the Employee

For the performance of the employment contract or any of the agreements on work performed outside an employment relationship, the Employer processes the categories of employees' personal data under Article 2, Section 2.1(a) to (i), and Section 2.2(a), for the following purposes:

- a. Maintaining employee records.
- b. Providing performance based on the employment contract or an agreement on work performed outside an employment relationship.
- c. Exercising employee rights.
- d. Managing, planning and organizing work.
- e. Recording and reporting working time.
- f. Recording family members within personnel records.
- g. Termination of employment.



8.1.2 Fulfilment of Legal Obligations

For the fulfilment of legal obligations, the Employer processes the categories of employees' personal data under Article 2, Section 2.1(a) to (i), Section 2.2(a), including data obtained from third parties pursuant to Article 3, Section 3.2, for the following purposes:

- a. Maintaining employee records.
- b. Calculating and paying salary and compensation to employees.
- c. Paying statutory contributions for employees.
- d. Processing administration related to business trips.
- e. Ensuring occupational health and safety.
- f. Ensuring equal treatment and diversity in the workplace.
- g. Investigating and reporting personal data security breaches.
- h. Complying with requests from supervisory authorities, courts and regulatory authorities of the Czech Republic, the European Union and, where applicable, other Member States.
- i. Complying with audit, tax and accounting obligations.

8.1.3 Fulfilment of the Employer's Legitimate Interests

For the fulfilment of the Employer's legitimate interests, the Employer processes the categories of employees' personal data under Article 2, Section 2.1(a) to (i), Section 2.2(b) and Section 2.3, in particular for the following purposes:

- a. Protection of the Employer's property and customers' property.
- b. Access to the workplace and operation of workplaces.
- c. Protection of the life and health of persons, ensuring workplace safety and prevention of unlawful conduct.
- d. Maintaining internal directories, employee access portals, use of other business collaboration and sharing tools.
- e. Monitoring compliance with internal regulations and accountability requirements.
- f. Workforce management and headcount, forecasting and planning.
- g. Legal defence in the event of disputes, where necessary for reporting, investigating or defending matters involving criminal offences, misdemeanours or other incidents that occurred on the Employer's premises or on the premises of the Employer's customers.
- h. Securing internet connection.
- i. Detecting and investigating security incidents, including processing personal data of persons affected by the incident and compromised data.
- j. Investigating and reporting data security breaches.
- k. Identification within internal communication tools, such as email.
- l. Preparation of statistical and analytical reports.
- m. Reporting, administration and optimization of internal processes.

Personal data are processed for this purpose only where the interests and fundamental rights and freedoms of employees as data subjects do not override the Employer's legitimate interest.

Before commencing processing for this purpose, the Employer always carefully balances the interests of employees against its own interests. If an employee does not agree with the processing of personal data for this purpose, the employee has the right to object and the Employer will carry out a new assessment.



8.1.4 Fulfilment of Purposes Defined in Consent to Personal Data Processing

- a. Employees' personal data are also processed on the basis of consent to personal data processing granted by the employee to the Employer.
- b. Consent to personal data processing granted by the employee is stored by the Employer in the personal folder of the Employee.
- c. The scope and purpose of processing the employee's personal data under consent to personal data processing are defined in the current wording of such consent. In particular, this concerns the processing of employees' personal contact details and photographs.
- d. Granting consent to personal data processing is entirely voluntary and failure to grant consent has no negative impact on the employee's position with the Employer.
- e. Each employee may withdraw consent to personal data processing at any time by sending an email to hr@bluelinkservices.com.

9. Employees' Rights in the Area of Personal Data Protection

9.1 The Employer processes employees' personal data in a transparent manner and each employee may exercise the following rights at any time during processing:

- a. **Right of access:** to their personal data, i.e. to confirmation whether or not the Employer processes personal data and, if so, to access information pursuant to Article 15(1) GDPR and to obtain a copy of the personal data that the Employer processes about the employee.
- b. **Right to data portability:** of personal data provided by the employee to the Employer in a structured, commonly used and machine-readable format to another controller, where the processing is based on consent and is carried out by automated means. If this right is exercised, the personal data will either be provided to the employee in a secure Excel file that is machine-readable, enabling the employee to store it or make it available to other personal data controllers, or directly to another controller designated by the employee, but only where such transfer is technically feasible.
- c. **Right to request rectification of inaccurate data:** if the employee discovers that data processed by the Employer concerning the employee are inaccurate, or to have incomplete personal data completed, by submitting a request for change in the HR system.
- d. **Right to request restriction of processing:** of personal data when:
 - i. The employee contests the accuracy of the personal data, for a period enabling the Employer to verify the accuracy of the personal data.
 - ii. The processing of personal data is unlawful but the employee opposes erasure of the personal data and requests restriction of their use instead.
 - iii. The Employer no longer needs the personal data for the purpose of processing, but the employee requires them for the establishment, exercise or defense of legal claims.
 - iv. The employee has objected to processing of personal data based on legitimate interest, pending verification whether the legitimate grounds of the controller override the legitimate grounds of the employee.
- e. **Right to request erasure:** of personal data in cases specified by the GDPR, namely:
 - i. The data are no longer necessary for the Employer for the purposes for which they were collected or otherwise processed.



- ii. The data are processed on the basis of the employee's consent and the employee has withdrawn that consent.
- iii. The employee has objected due to disagreement with the processing of personal data based on legitimate interest.
- iv. Erasure is necessary to fulfil a legal obligation.
- v. The processing is unlawful.

If there is no legal basis for doing so, the Employer will not erase employees' personal data or restrict their processing.

- f. Right to notification: of all rectifications or erasures of personal data to recipients to whom the controller has disclosed personal data. If the employee requests it, the Employer will inform the employee of those recipients.
- g. Right to contact the competent supervisory authority: if the employee believes that their rights have been infringed in connection with the processing of their personal data, usually the Office for Personal Data Protection, Pplk. Sochora 27, 170 00 Prague 7, or the competent court.
- h. Right to object: to processing of personal data based on legitimate interest or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority. Any employee may raise an objection by written communication addressed to the DPO at:
 - dpo@bluelinkservices.cz or
 - BLUELINK INTERNATIONAL S.A.S.
DPO
Immeuble Osmose
74 avenue Vladimir Ilitch Lénine
94 112 Arcueil Cedex
France

The Employer will no longer process the personal data unless it demonstrates compelling legitimate grounds for processing which override the interests or rights and freedoms of the employee as data subject, or for the establishment, exercise or defence of legal claims.

10. Annex - Facultative

Abbreviations Used

Definition, abbreviation or symbol	Explanation
DPO	Data Protection Officer
GDPR	General Data Protection Regulation of European Union
CV	Curriculum Vitae
IBAN	International Bank Account Number
CCTV	Camera security system



EU	European Union
BL	BlueLink International CZ s.r.o.
HR	Human Resources