



Privacy Policy

Best Camion Limited Liability Company
May 25, 2018.

The controller:

Name of the company: Best Camion Limited Liability Company

Headquarters: 2060 Bicske, 0321/23.

Company registration number: 07-09-010995

1. Purpose of the Policy

By creating this policy, the Company intends to ensure that the data subjects are able to receive appropriate information about the data processed by the Company and its contractors, their source, the purpose of the data processing, and the included data processing the names, addresses and activities related to data processing, the legal basis and the recipient of the data transfer in case of the transfer of personal data of the data subject.

2. Scope of the Rules

- Personnel scope of the Policy shall apply to:

(a) all employees of the Company, and

(b) workers hired on a case-by-case basis for work,

(c) the processor, and

(d) in addition to the above, any person who has any contractual relationship with the Company.

- Subject scope of the Policy

(a) all data generated by the Company,

(b) data processed or processed in the IT system,

(c) the data generated as a result of the processing,

(d) all hardware and software devices used in the Company, and

(e) data of public interest relating to the Company's activities or public interest data generated in the course of its operation.

3. Terms and Definitions

- data subject: any specific, identified on the basis of personal data or - directly or indirectly - identifiable natural person;

- personal data: the data relating to the data subject, in particular the name, identification mark and knowledge of one or more physical, physiological, mental, economic, cultural or social identities of the data subject, and the conclusion drawn from the data subject;

- special information: (a) personal data relating to racial origin, nationality, political opinion or party status, religious or other philosophical beliefs, membership of the representative organisation, sexual life,
- (b) personal data on health status, abnormal passion and criminal personal data;
 - criminal personal data: generated during or prior to criminal proceedings in connection with the offence or criminal proceedings, by bodies authorised to conduct criminal proceedings or detect criminal offences, or by the organization of the correctional system, with the data subject personal data relating to the criminal record;
 - public interest data: information or knowledge, in whatever way or form, which is not covered by the concept of personal data and which is in the management of a body or person performing a public or local government task or other statutory public task and which arises in connection with its activities or information on the nature, autonomous or aggregate nature of the data, including in particular scope, competence, organizational structure, professional activity, evaluation of its effectiveness, the types of data held and the legislation governing the operation, as well as information on management and contracts;
 - public data in the public interest: all data which do not fall within the concept of data of public interest, the disclosure, acquaintance or making available of which is required by law in the public interest;
 - consent: the voluntary and firm expression of the data subject's will, based on appropriate information, giving his or her unambiguous consent to the processing of personal data concerning him or her, in whole or in part;
 - objection: a statement by the data subject objecting to the processing of his or her personal data and requesting the termination of the processing or the deletion of the processed data;
 - data controller: the natural or legal person or entity without legal personality who, alone or in association with others, determines the purpose of the processing, makes and implements decisions on the processing (including the means used) or implements it with the data processor;
 - data management: any operation or set of operations on data, irrespective of the procedure used, in particular their collection, recording, recording, systematisation, storage, alteration, use, interrogation, transmission, disclosure, coordination or linking, blocking, erasure and destruction, and to prevent further use of the data, to take photographs, sound or images and to record physical characteristics (eg fingerprints or palm prints, DNA samples, irises) that can be used to identify the person;
 - data transfer: making the data available to a specific third party;
 - disclosure: making the data available to anyone;
 - erasure: making the data unrecognizable in such a way that it is no longer possible to recover it;
 - data designation: the identification marking of the data for the purpose of distinguishing it;

- data blocking: for the purpose of limiting further processing of the data to a permanent or specified period of time;
- data destruction: total physical destruction of the media containing the data;
- data processing: the performance of technical tasks related to processing operations, irrespective of the method and means used to carry out the operations and the place of application, provided that the technical task is carried out on the data;
- data processor: any natural or legal person or body without legal personality who, under a contract, including a contract concluded pursuant to the provision of law, processes data;
- dataset: the sum of the data processed in a single register;
- third party: a natural or legal person, or an organisation without legal personality, other than the data subject, the controller or the data processor;
- EEA State: a Member State of the European Union and another State party to the Agreement on the European Economic Area, as well as a State of which the European Union is a national under an international agreement concluded between the European Union and its Member States and a State not party to the Agreement. It shall have the same status as a national of a State party to the Agreement on the European Economic Area;
- third country: any State which is not an EEA State;
- personal data breach: unlawful processing or processing of personal data, in particular unauthorized access, alteration, transmission, disclosure, deletion or destruction, as well as accidental destruction or damage.

3. Principles of data processing

The Company carries out data processing solely on the basis of the provisions of the applicable legislation. Personal data can be processed only for the purposes of exercising the right or fulfilling an obligation. The use of personal data processed by the Company for private purposes is prohibited. Data processing must at all times comply with the principle of purpose limitation.

The Company processes personal data only for a specific purpose, in order to exercise rights and fulfil obligations, to the minimum extent and for the time necessary to achieve the objective. In case of cessation of the purpose of data processing or unlawfulness of data processing, the data shall be deleted.

The Company processes personal data only on the basis of the prior written consent of the data subject or, in case of legal requirements, legal authorization. The Company shall always communicate to the data subject the purpose of data processing and the legal basis of data management to the data subject before recording the data.

The executives of the Company determine the tasks of the employees related to data management. The purpose of their activities is to ensure the accuracy of the data at all stages of data processing in a legal and fair manner and to ensure the protection of the

personal data of the data subject in the event of unauthorised access, alteration, transmission, deletion or destruction.

The agents of other organizations or enterprises involved in data processing in relation to the Company are obliged to keep the information known as business confidentiality.

4. Legal basis of data processing

Personal data may be processed if:

- the data subject agrees to it, or
- it is ordered by law or by the authority of the law, within the scope specified therein by law or by decree of local government for purposes based on public interest/mandatory data processing /.

In the case of compulsory data processing, the types of materials to be processed, the purpose and conditions of data processing, the availability of data, the duration of data processing and the person of the data controller are determined by law or municipal regulation.

Personal data may also be processed if obtaining the data subject's consent would be impossible or disproportionate and the processing of personal data is necessary for the fulfillment of a legal obligation to the Company or for the purpose of enforcing the interests of the Company, and the exercise of that interest is proportionate to the restriction of the right to the protection of personal data.

Before starting the processing, the data subject must be informed whether the processing is based on consent or is mandatory. The data subject shall be clearly, understandable and in detail informed of the personal data to be processed and of all facts relating to the processing of his data, in particular the purpose and legal basis of the processing, the person entitled to the processing, the processing of data, and who can get to know the information.

If the personal data are collected on the basis of the consent of the data subject, the Company shall, unless otherwise provided by law, collect the data for the purpose of fulfilling the legal obligation applicable to him or for the purpose of asserting the legitimate interests of the third party, if such interest is proportionate to the restriction of the right to the protection of personal data, without further specific consent.

The Company carries out its activities in the course of data processing, in particular, but not limited to the following laws:

- 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;
- Act CXII of 2011 on Information Self-Determination and Freedom of Information,
- Act CXXXIII of 2005 on the rules of protection of persons and property and private investigators,
- Act V of 2013 on the Civil Code,

- Act C of 2000 on Accounting,
- Act CXVII of 1995 on Personal Income Tax, - Act XCIII of 1993 on Labor Safety,
- Act I of 2012 on the Labour Code.

5. Rules on data security and information security

The Company stores personal data on paper or on a computer network. Paper-based data may only be stored in a properly lockable room with an alarm system in such a way that it cannot be accessed by an unauthorized person. The staff member of the Company conducting data management may leave the premises during the day only by blocking the entrusted media or closing the premises, and by closing the paper media upon completion of the work.

If the purpose of processing personal data stored on paper media is achieved, the Company shall arrange for the destruction of the paper media. Minutes shall be taken of the destruction of the documents to be destroyed. The annulment is carried out by an employee appointed by the managing director of the Company.

In the case of computer-based data storage, data processing can only be carried out on the computer owned by the Company. Data on the computer can only be accessed with a valid, personalized user name and password. If the purpose of data processing is achieved, or if the deadline for processing has expired, the file containing the data must be irretrievably deleted.

Antivirus protection of the computer handling personal data and the prevention of access by unauthorized persons must be ensured continuously.

6. Different data management at the Company

6.1. Data processing related to applicants' data

The Company manages the CVs of the applicants, whether on paper or electronically, to the Company, in the same way. The stored CVs are retained by the Company because of the jobs that have become vacant or have become vacant, but will be destroyed after 1 year.

The company shall notify the data subject in writing of the fact that resumes are stored. The consent given to data processing may be withdrawn from the data subject at any time.

Purpose of data processing: the selection of appropriate workers for the purpose of filling vacancies and establishing a future employment relationship.

Scope of data processed: name, date of birth, mother's name, address, qualification data, photo, other data provided by the data subject in the CV.

Legal basis for data processing: consent as per Subsection (a) of § 5, § /1/ (a) and § 6 (/6/) of Infotv.

Duration of data storage: 1 year from the date of receipt.

Method of storing data: on a paper basis, electronically.

6.2. Processing of data on the certificate of good conduct

The Company reserves the right to employ employees in specific jobs who are morally meeting their expectations, so before establishing the employment relationship, the applicant may request the presentation of certificate of good conduct.

In any case, the Company informs the data subject beforehand that the purpose of the knowledge and handling of criminal personal data is to decide the question of suitability for the given job, so the duration of data processing is only up to the decision.

The data of the certificate of good conduct can be accessed only by the executives of the company during the recruitment procedure. The certificate of good conduct is not stored by the Company, and it is not copied either.

The Company processes criminal personal data only with the consent of the data subject (§ 5 (1) (a) of Infotv.

6.2. Copy ID cards

In order to maintain the principle of data recording and data quality, the Company may make masked photocopies or scanned images of the identity cards of the employees who have modified the data of the new entrants or employees who have modified their data.

This means that those parts of the official cards which contain data that must be provided to the Company by the employee entering the company remain legible. The copy, scanned image is made for the purpose of reconciling the data, and the Company will delete or destroy it after 30 days at the latest.

Purpose of data processing: to ensure the adequacy of the personal data to be transmitted by the employer during the establishment of the employment relationship.

6.3. Handling of medical fitness data

The Company has contracted with a healthcare provider for the purpose of deciding on medical fitness, therefore it does not handle the detailed medical data of the employee, only the existence of fitness or the document relating to the decision on the incompetence of the prospective worker.

With regard to workers with disabilities, the Company manages data on the health status of workers with disabilities on the basis of legal requirements.

6.4. Data processing related to the establishment, maintenance and termination of employment

The purpose of data processing: The purpose of data processing related to employment is to fulfill employers' obligations during the establishment, maintenance and termination of the employment relationship.

The processing of personal data when applying for work is carried out only after having informed the person concerned in writing, shall be the sole responsibility of the administrator. Only the administrator shall have access to these personal data for the purpose of assessing the suitability of the candidate for recruitment.

The Company may make the filling of individual positions subject to the presentation of a moral certificate and the decision to recruit an employee may be affected by this.

The Company maintains a salary and labour register of its employees, which uses the employee's data on payroll, social security and statistical information and, pursuant to Act CXVII of 1995 (Szja tv.) in connection with the use of it.

Legal basis of data processing: Consent of the person concerned (Section 5 (1) (a) and Article 6 /6/ bek. of Infotv.), with the signature of the information leaflet contained in the annex and Act I of 2012 on the Labour Code and Act CXVII of 1995.

Duration of data processing: Only until the employment of the employee or, if data processing is required by law or municipal decree, the period stipulated in the relevant legislation.

The Company processes the following personal data relating to the employee:

- Worker's name, Name of birth, Place of birth, date, Nationality, Mother's name, Place of residence, Tax identification mark, Social Security number, Tax identification mark, Bank account number, Pension fund membership, Pensioner number, Current account number, Beginning of employment, Number of working hours, School attainment copy of certificate, Labor suitability certificate, Job title, Data and number of children, Phone number of persons to be notified in case of accident, Existence of driving licenses.

For workers with disabilities, pursuant to 21. § 21/A. § 21/B of Act CXCI. of 2011, the scope of the above data is supplemented with specific personal data defined in accordance with the section 3. § 3 of the Infotv.:

- Expert Committee opinion,
- Decision on the changed ability to work.

Legal basis of data processing: Section 10, subparagraphs /1/ and /3/ of Act I of 2012 on the Labour Code and the consent of the data subject (Section 5 (1) (a) and 6 /6/ para. of the Infotv.)

Deadline for data storage: until the date of completion of the purpose of data processing, but not more than the date of termination of employment or the period specified in the legislation on pension payments.

Method of data processing: on paper and electronically.

Details of the relatives of employees:

In order to ensure the benefits and rights of the employee, the Company may also process the data of the employee's relatives for the necessary period and extent. Such data may be necessary for the establishment of surcharge leave, family tax allowance, exempt benefits in kind. In the event that the employee provides the data of a third party, he is obliged to obtain the consent of the third party for data processing from the third party and to provide the Company with a statement of consent.

Purpose of data processing: to provide benefits related to employment

Scope of processed data: data required by law

Legal basis of data processing: Section 5 (1) (a) of the Infotv.

Deadline for data storage: until the date of completion of the purpose of data processing, but not more than the date of termination of employment or the period specified in the legislation on pension payments.

Method of data processing: on paper and electronically.

6.5. Investigation of working condition

The purpose of data processing: Employees can only stay and carry out work in the Company's workspaces in a safe working condition, in compliance with instructions and regulations related to occupational safety.

The employee is obliged to cooperate with his staff and to carry out his work in such a way as not to endanger the physical integrity of others or his own.

Employees are prohibited from staying under the influence of alcohol or other psycho-altering agents in the Company's workspaces.

Since the ability to work cannot be ensured under the influence of these mind-altering agents, according to Act I of 2012 on the Labour Code and Act XCIII of 1993 on occupational safety, the employer is obliged to make sure that the employees comply with the ban on alcohol consumption related rules.

The employer's control practice should not lead to a violation of human dignity, so the examination can only be carried out in accordance with the Company's labor safety instructions.

The protocol for the probe inspection of an employee is set out in the Annex to the Privacy Policy.

Scope of data managed: Worker's name, mother's name, place of birth, date, position, results of inspection.

Legal basis of data processing: Section 60, paragraph /1/ of Act XCIII of 1993 on occupational safety, and Section 52 (1/ a) of Act I of 2012 on the Labour Code.

Duration of data processing: Deadline resulting from the possibility of enforcing claims based on rights and obligations derived from the fact of control.

Method of data processing: on paper and electronically.

6.6. Processing of data relating to the control of technical means provided to the employee by the employer

The Company provides its employees with the necessary technical tools for performing certain jobs, such as computers, laptops, company phones, mobile phones, e-mail addresses, internet etc. On the rules of legal use, the employer instructs employees and regularly informs them.

The purpose of data processing: In accordance with the legitimate business interests of the company, control of employees in accordance with Section 11 (/1/ -/2/) of the Labour Code

The scope of the data processed: personal data recorded during the audit, in particular private email addresses, phone numbers, photos, own documents, Internet events, history, cookies.

Legal basis of data processing: Labor Code (Act I of 2012) Section 11 (/1/-/2/), consent of the data subject (§ 5 (1) (a) of Infotv.

Deadline for data storage: 1 year from the date of verification, up to the limitation period of the request for verification.

Method of data storage: on paper and electronically.

6.7. Management of electronic monitoring system (camera) data

The purpose of data processing: The Company, as data controller, operates an electronic monitoring system in order to comply with the rules of safe work, prevent accidents, protect physical integrity and prevent and/or detect possible offences or offences against property.

The Company does not operate the monitoring system for the purpose of monitoring its employees, nor is it intended to influence the behaviour of employees at the workplace.

No camera systems can be found in rooms intended for working breaks, toilets, dressing rooms, public spaces. The operated camera system does not record sound.

The Company informs the persons entering its territory about the fact of surveillance with a camera with visible attention signs.

The placement of cameras and workers' information regarding the electronic monitoring system are set out in the annex to this privacy policy.

Only the executives of the Company have access to the recordings.

Scope of data managed: The portrait of the persons entering the Company's territory is visible on the camera system and other conclusions that can be drawn from the recordings recorded by the surveillance system.

Legal basis of data processing: In the case of the company's customers and guests, the voluntary consent of the person concerned on entry into the territory, in the case of employees, the provisions of Act CXXXIII of 2005 on the rules of protection of persons and property and private investigators and the Labour Code Provisions I of 2012 and the consent of the data subject (§ 5 (1) (a) of Infotv.

Duration of data processing: Under the provisions of Act CXXXIII of 2005 on the Rules of Person and Property Protection and Private Investigation, in the absence of use, 3 days. Use of the recorded image as evidence in judicial, administrative proceedings.

In the absence of use, the Company will delete the camera footage after the deadline set by law. During use, the recording may be saved for more than 3 days if the authority orders to save the camera footage during the evidence process or if the data subject requires, by demonstrating the legitimate interest of the data subject, that the data controller saves the recording concerning him. The Managing Director of the Company shall assess the validity of the application received and, in case of the validity of the application, ensure the extraction of the recording and its blocking in accordance with the statutory requirements.

In the event of an official request, the Company shall immediately hand over the saved recording to the requesting authority. If no request is made for the blocked recording, the recording will be destroyed by the Company after 30 days.

6.8. Management of access control system data

The Company operates an entry-exit-personnel registration system in order to register the entry and exit of employees to and from the work area. The purpose of the operation of the entry control – personnel management system: to protect life and physical integrity based on the knowledge of the exact number of employees in the area.

Legal basis for data processing: Act I of 2012 on the Labour Code and Act CXXXIII of 2005 on the rules of protection of persons and property and private investigators.

Scope of managed data: name, main number, card ID, entry, exit date.

Duration of data processing: The Company shall destroy the personal identification data of the data subject immediately upon the termination of the right of access, the data generated during the operation of the system and the data generated on paper, except for the data to be stored as accounting documents, no later than 6 months after the data is generated.

6.9. Taking photos and video recordings for educational or informational purposes

The purpose of data processing: The Company can make an informative film about the work, its applied technologies, the presentation of the workflows, the events organized within the framework of the company, as well as photographs containing the employees of the Company.

Employees are not obliged by the Company to participate in the recordings, this is solely the individual decision of the employees.

The employer declares that the purpose of the recordings is not to monitor the activity of employees during work and does not represent the worker in a negative form. The Company declares that the recruitment is without prejudice to the rights of the working person, to the protection of reputation, honor or human dignity.

Scope of data managed: Photo, video, or audio recording

Legal basis of data processing: Voluntary consent of the data subject pursuant to Section 5 (1/ a) of Act CXII of 2011 on Freedom of Information and Informational Self-Determination.

Duration of data processing: To the end of the event that caused the recording or to reach the purpose of education.

7. Operation of the website (website)

The Company has its own website, its address: www.bestcamion.hu

One can access the website operated by the Company without providing his personal data. The Company's website does not collect personal information about visitors, so personal data will not be held by our Company.

The Company does not implement data processing within the scope of the Info Act by operating the website.

However, when using the login menu section of the website, personal data is processed, the purpose of which is to communicate with visitors, electronic mail.

Scope of processed data: name, e-mail address

Legal basis of data processing: Voluntary consent of the data subject pursuant to Section 5 (1/ a) of Act CXII of 2011 on Freedom of Information and Informational Self-Determination.

Duration of data processing: Until the fulfilment of the purpose of data processing, for a maximum of two years.

8. Internal register of data processing and data transfer by the Company

Pursuant to Section 15 of Act CXII of 2011 on Information Self-Determination and Freedom of Information, the Company maintains data management and data transfer records on data management and related data transfer processes.

The documentation of the data management and transfer records is contained in the annex to the Privacy Policy.

9. Use of a data processor

The Company may transmit data to data-processing enterprises or organizations for the purpose of performing statutory tasks.

In the case of employee data, data processing begins after signing the declaration on worker data management.

The processor shall not take decisions concerning processing without the consent of the controller, shall not carry out processing for purposes other than the provisions of the controller, but shall perform its tasks only on the instructions of the controller.

The data processor is obliged to ensure the physical and software protection of the data to be processed on the basis of the rules laid down in the data protection and data security policy of the Company.

In the course of its activities, the Company uses the following data processing companies:

- Accounting, payroll:
- Occupational health:
- Work and accident protection:
- Property protection activities:
- Information technology activities:

The disclaimer of data processing companies is set out in the annex to the data protection policy.

10. Transmission of data abroad

Personal data will be transferred to the data controller in a third country if the data subject has expressly consented to this and the appropriate level of protection of personal data is ensured in the third country.

Transfers to EEA countries should be considered as having taken place within Hungary.

11. Entitlements and remedies of the person concerned by the data processing

The data subject may request information about the processing of his personal data, and may request correction of his personal data, or, if no exception is made by law and does not require compulsory processing in respect of a particular data, the data subject may request the erasure of his data from the Company.

The Company is obliged to answer the requests received within a maximum of twenty-five days from the date of receipt. The information shall cover the information set out in in Paragraph 15 (/1/) of the Infotv. , insofar as the information of the data subject cannot be denied under the Info Act. The Company may reject an application only on the grounds set out in Section 9 (/1/) or (19) of the Infotv.

The data subject may request the correction of the incorrect data, or the Company shall correct the incorrect data, and, in case of the reasons set out in Article 17 (/2/) of the Infotv., he will take care of the deletion of the personal data processed.

The data subject may object to the processing of his personal data,

(a) where the processing or transfer of personal data is solely necessary for the fulfilment of a legal obligation for the controller or for the exercise of a legitimate interest of the controller, data importer or third party, except in the case of compulsory processing;

(b) where the use or transfer of personal data is for direct marketing, polling or scientific research; and

c) in other cases as defined by law.

The Company shall examine the objection within the shortest time and within a maximum of fifteen days from the submission of the application, make a decision on its merits and inform the applicant in writing of its decision.

If the Company establishes the validity of the data subject's objection, the processing, including further data collection and data transfer, shall be terminated and the data blocked, and shall notify all those to whom the personal data subject to objection have been transferred earlier and who are obliged to take action to enforce the right to object.

If the Company causes damage to someone else by unlawful handling of the data subject or breach of data security requirements, it is obliged to reimburse them. If the Company violates the data subject's right to privacy by illegally handling the data subject's data or violating the data security requirements, the data subject may claim damages from the Company.

The Company shall be exempt from liability for damages caused and payment of damages if it proves that the damage or the violation of the personal rights of the data subject was caused by an unavoidable cause outside the scope of data processing. There is no need to compensate for the damage and no claim for damages to the extent that the damage was caused by the intentional or grossly negligent conduct of the injured party or the breach of the right to privacy.

If the data subject does not agree with the Company's decision or information on the processing of his personal data, or if the Company fails to meet the deadline specified in the law, the data subject may apply to a court or the National Data Protection and Freedom of Information Authority (1125 Budapest, Szilágyi Erzsébet fasor 22 / C.) for legal redress within thirty days of the notification of the decision or the failure to meet the deadline.

Best Camion Kft.

Miklos Antonius Markus