Privacy Notice

Data processing related to the activities of CarryAll Hungary Kft. and the operation of the https://carryall.hu/ website

Introduction

This Notice, in accordance with the rules of the EU General Data Protection Regulation 2016/679 (GDPR), ensures transparency regarding the activities performed by CarryAll Hungary Kft. (hereinafter: Controller) involving the data of natural persons during the fulfillment of its tasks detailed below. It outlines the rules applied during these activities and provides insight into the measures taken to protect the data used. Furthermore, it provides information on the rights available to data subjects to protect their interests.

Data processing occurs in all cases where the Controller enters into a contract with its clients, business partners, subcontractors, or employees, issues invoices to its business partners, or conducts video surveillance (CCTV). In certain cases, to fulfill its legal obligations, the Controller transfers a portion of this personal data to external partners and/or authorities.

The regulations detailed in this Notice have been established based on Act V of 2013 on the Civil Code [Ptk.], Regulation (EU) 2016/679 of the European Parliament and of the Council 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) [GDPR], Act XLVIII of 2008 on the Basic Conditions and Certain Restrictions of Online Business Advertising Activity [Grt.], and Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information [Info tv.].

The Controller provides the mandatory information pursuant to Article 13 of the GDPR to data subjects and interested parties as follows:

1. Identification Data of the Controller:

- Name: CarryAll Hungary Kft.
- Represented by: Lóránt Bartus, Peter Thury Managing Directors
- Registered office and mailing address: 8200 Veszprém, Lőszergyári út 6., Hungary
- Tax number: 14603462-2-19
- E-mail address: info@carryall.hu
- Phone: +361 255 2710

2. Principles of Personal Data Processing

The Controller operates in compliance with the following principles:

- Purpose limitation: Defines the purposes for which the Controller stores and uses the data of natural persons during its activities.
- Data minimization: The scope of processed data is adequate, relevant, and limited to what is necessary in relation to the purposes.
- Accuracy: In the interest of the Data Subjects and regulatory compliance, the Controller shall promptly rectify or erase inaccurate personal data.

The Controller receives personal data directly from the data subjects. The Controller considers the fulfillment of tasks related to the protection of personal data processed in connection with its activities as binding, through which—where applicable—it helps demonstrate to Authorities, business

partners, and data subject clients that it has acted in compliance with the Regulation, the Info tv., and other relevant legislation (principle of accountability).

3. Definitions

This Privacy Notice uses the following terms:

- "personal data": any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
- "data subject": the natural person whose personal data is processed by the Controller.
- "consent of the data subject": any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
- "Controller": the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- "personal data breach": a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.
- "data protection officer": a person defined by the GDPR who performs expert activities in the field of personal data protection at the employing/appointing company and maintains contact with the data protection authority (NAIH). Their employment is mandatory in certain cases prescribed by law and recommended in others

4. Data Processing Procedures

During its activities, the Controller processes the data of business partners, employees, and clients—obtained in any manner or to any extent—in accordance with this Privacy Notice, undertaking a duty of confidentiality, and pursuant to the relevant Hungarian legislation and the provisions of the GDPR.

The Controller may lawfully store, organize within the framework of the law, and use to the necessary extent the data received in the course of its activities and the fulfillment of related tasks.

The Controller shall immediately terminate the data processing if its purpose has been fulfilled or has ceased to exist, and shall consider termination if requested by the data subject. The Controller does not employ profiling or automated decision-making.

5. Detailed Data Processing by Purpose Related to the Controller's Activities

Purpose of data processing: Conclusion of contracts with external service partners and subcontractors

- **Legal basis:** Performance of a contract (GDPR Article 6(1)(b))
- **Method:** Stored both in paper and electronic formats
- **Data processed:** In the case of a sole proprietor: name, phone number, e-mail address; In the case of a non-natural person (company, other organization) partner: name, phone number, and e-mail address of the employee/contact person managing the contract.
- **Duration of data processing:** 8 years following the termination or expiration of the contract (taking into account financial and accounting considerations).
- **Access to data:** The head of the Controller and employees performing related administrative tasks.

Purpose of data processing: Fulfillment of delivery orders

- **Legal basis:** Performance of a contract (GDPR Article 6(1)(b))
- **Method:** Stored both in paper and electronic formats
- **Data processed:** Name, address, e-mail address, and phone number of the recipient.
- **Duration of data processing:** 8 years from the fulfillment of the order (taking into account financial and accounting considerations).
- **Access to data:** The head of the Controller and employees performing related administrative tasks.
- **Data transfer:** Data is transferred to the subcontractor (courier) performing the delivery.

Purpose of data processing: Tracking of shipments (delivery, receipt, payment)

- **Legal basis:** Performance of a contract (GDPR Article 6(1)(b))
- **Method:** Electronically, via a mobile device with GPS tracking operated by the transport subcontractor, according to the information provided by them.
- **Data processed:** Name, address, e-mail address, phone number of the recipient, time of receipt, data related to the payment for the goods, and identification data of the courier.
- **Duration of data processing:** 8 years from the fulfillment of the order (taking into account financial and accounting considerations).
- **Access to data:** The head of the Controller and employees performing related administrative tasks.

Purpose of data processing: Processing data of job applicants, evaluation of applications and CVs

- **Legal basis:** Consent of the data subject (GDPR Article 6(1)(a))
- **Method:** Paper-based and electronic
- **Data processed:** Name of the natural person, date and place of birth, mother's name, residential address, qualification data, photograph, phone number, e-mail address, and employer's notes made about the applicant.
- **Duration of data processing:** Until the evaluation of the application/candidacy. Personal data of non-selected applicants will be deleted, as well as the data of any person who withdraws their application.
- **Access to data:** The head of the Controller authorized to exercise employer rights and the employee performing labor-related tasks.
- **Data transfer:** No data transfer takes place.

Purpose of data processing: Occupational health fitness

- **Legal basis:** Compliance with a legal obligation (GDPR Article 6(1)(c); Act I of 2012 on the Labour Code).
- **Method:** Paper-based
- **Data processed:** The fact of occupational fitness and the conditions necessary for it.
- **Duration of data processing:** Until the termination of the employment relationship.
- **Access to data:** The head of the Controller authorized to exercise employer rights and the employee performing labor-related tasks.

Purpose of data processing: Employment

- **Legal basis:** Compliance with a legal obligation (GDPR Article 6(1)(c); Act I of 2012 on the Labour Code; Act V of 2013 on the Civil Code).
- **Method:** Paper-based and electronic
- **Scope of data processed:** Employee's name, birth name, place and date of birth, nationality, mother's name, residence, tax identification number, social security (TAJ) number, bank account number, voluntary pension fund membership, pension registration number, current account number, start of employment, number of weekly working hours, copy of certificates proving educational qualifications, occupational fitness certificate, job title, data and number of children, driver's license number, (...) and other data required by law.
- **Duration of data processing:** Generally 5 years following the end of the employee's employment, but certain data (e.g., those related to payroll or the determination of pension eligibility) are kept for a longer period in accordance with applicable laws: 8 to 50 years, or in the latter case, cannot be deleted.
- **Access to data:** Controller, appointed accountant (service provider), authorities. The employee has the right to receive information regarding their recorded personal data and its processing. This right includes the ability to request a copy of their own data from the records.

Purpose of data processing: Invoicing

- **Legal basis:** Compliance with a legal obligation (GDPR Article 6(1)(c); Act C of 2000 on Accounting; Act CL of 2017 on the Rules of Taxation).
- **Method:** Electronic
- **Data processed:** Name, residential address/registered office, tax number.
- **Duration of data processing:** 8 years.
- **Access to data:** Controller, accounting partner, National Tax and Customs Administration (NAV).

Purpose of data processing: Customer service, administration via telephone (recording of phone calls)

- **Legal basis:** Compliance with a legal obligation (GDPR Article 6(1)(c); Act CLV of 1997 on Consumer Protection).
- **Method:** Electronic.
- **Data processed:** Name, delivery identification data.
- **Duration of data processing:** 3 years.
- **Access to data:** Controller, Consumer Protection Authority.

Purpose of data processing: Data protection complaint handling

- **Legal basis:** Compliance with a legal obligation (GDPR Article 6(1)(c); Act V of 2013 (Civil Code); Act CLV of 1997 on Consumer Protection).
- **Method:** Paper-based and/or electronic.
- **Data processed:** Data subject's name, phone number, e-mail address, information voluntarily provided by the data subject in the complaint.
- **Duration of data processing:** 3 years.
- **Access to data:** Controller; in case of an audit, the Authority; potentially the Controller's legal counsel.

6. Information on the use of cookies on the website:

Data subjects: All persons visiting the Controller's website at https://carryall.hu/. Data generated during the browsing of the website is not stored or processed by the Controller, nor by the developer or operator of the website, in any way that is specifically linked to a Data Subject. Consequently, no processing of identifiable personal data under the GDPR takes place.

The IP Address
An IP address (Internet Protocol address) is a series of numbers that identifies your computer when connecting to an internet service provider, a local area network (LAN), or a wide area network (WAN). Web servers automatically identify your computer based on the IP address as long as you are online. The Controller's web service provider may collect IP addresses for the purpose of monitoring site usage. We do not associate users with IP addresses for the purpose of personal information collection, which means that while every user is recorded, the user remains anonymous.

Cookies
This website may also use a technique known as "cookies." A cookie is a small text file placed on your computer's hard drive by the website provider. Cookies provide additional functions for the website and help us measure website usage more accurately. In any case where we use cookies, we do not collect information that personally identifies you.
You have the option to enable or decline cookies. Most internet browsers automatically enable cookies, but you can decline them by modifying your browser settings, or, if you prefer, you can receive a warning before a cookie is stored. If you would like to learn more about these functions and refine your cookie settings, please consult your internet browser's instructions or help screen. If you choose to decline cookies, you may not be able to fully utilize the interactive features of our website or other websites.

Deleting Cookies
If you do not accept the use of cookies, certain functions will not be available to you. You can find more information on deleting cookies at the following links, depending on which browser you use:

- Firefox: [Link]
- Mozilla (HU): [Link]
- Chrome: [Link]
- Edge: [Link]

Purpose of data processing: Video surveillance (CCTV)

- **Legal basis:** Legitimate interest of the Controller (GDPR Article 6(1)(f)).
- **Method:** Electronic.
- **Data processed:** Facial image (video recording; the camera does not record audio).
- **Purpose of surveillance:** Protection of human life, physical integrity, and property.
- **Duration of data processing:** 30 days.
- **Access to data:** Controller.

Further information regarding video surveillance
The Controller does not use an electronic surveillance system in rooms where surveillance could violate human dignity, specifically in changing rooms, showers, restrooms, medical rooms (including waiting areas), or rooms designated for employees' rest breaks.
The storage unit for the cameras is located in a physically protected, locked room, stored in a way and place inaccessible to unauthorized persons. Viewing images captured by the cameras is password-protected and is the exclusive right of employees specifically authorized for this task. The device logs every instance of viewing in a traceable manner.

Raising Awareness: The Controller places warning signs about the application of the electronic surveillance system in clearly visible locations within the given area, in a way that facilitates the

orientation of persons wishing to enter the area. This information is provided for every camera (individually).

Example sign:

A detailed description of the area monitored by the cameras can be found in the annex to the Privacy Notice. If you wish to view it, please contact the Controller at the provided e-mail address.

7. Disclosure and Transfer of Personal Data

In certain cases related to its activities, the Controller transfers personal data to third parties. Data transfer may occur in paper or electronic format, ensuring in both cases that the data is accessible only to the recipient.

- **Paper-based transfer:** Via personal delivery or by post, addressed specifically to the recipient.
- **Electronic transfer (e-mail):** Personal data does not appear in the body of the message. If necessary, personal data is sent in an attached Excel or compressed file, always protected by a unique password. The password is provided to a specific person/recipient via a separate channel (e.g., telephone, SMS), whereby the Controller guarantees that the personal data remains inaccessible to unauthorized persons throughout the entire transmission process.

In the case of electronic data transmission, data is sent from a computer that is password-protected, virus-protected, and used exclusively within the Controller's scope of activities.

The Controller transfers data—under the legal bases of "performance of contract" or "compliance with legal obligation"—to the following partners acting as data processors or independent controllers:

a) Tax Authority (NAV):

- **Contact details:** 8200 Veszprém, Brusznyai Árpád utca 22-26.; Tel: +36(88) 577 300.
- **Legal basis for transfer:** Compliance with a legal obligation (GDPR Article 6(1)(c); Act C of 2000 on Accounting; Act CL of 2017 on the Rules of Taxation).
- **Purpose of transfer:** Statutory compliance.
- **Data transferred:** Name, address, tax number.
- **Timing and method:** Occasionally, electronically.

b) Financial Service Partner (MBH Bank):

- **Privacy info:** MBH Bank Privacy.
- **Purpose of transfer:** Payroll, financial settlement of invoices.
- **Legal basis for transfer:** Performance of a contract (GDPR Article 6(1)(b)).

- **Scope of data transferred:** Surname, first name, account number, other banking details.
- **Timing and method:** Occasionally, electronically.

c) Financial Service Partner (Raiffeisen Bank):

- **Privacy info:** Raiffeisen Bank Privacy.
- **Purpose of transfer:** Payroll, financial settlement of invoices.
- **Legal basis for transfer:** Performance of a contract (GDPR Article 6(1)(b)).
- **Scope of data transferred:** Surname, first name, account number, other banking details.
- **Timing and method:** Occasionally, electronically.

d) Card Payment Service Provider (myPOS Limited):

- **Privacy info:** myPOS GDPR.
- **Purpose of transfer:** Providing card payment options.
- **Legal basis for transfer:** Performance of a contract (GDPR Article 6(1)(b)).
- **Scope of data transferred:** Surname, first name, account number, residence (...), and data requested by the bank for the secure execution of the transfer.
- **Timing and method:** Occasionally, electronically.

e) Accounting Service Partner (PureAqua Kft.):

- **Contact details:** +36(88) 794 243.
- **Purpose of transfer:** Fulfillment of accounting (and related) tasks.
- **Legal basis for transfer:** Performance of a contract (GDPR Article 6(1)(b)).
- **Scope of data transferred:** Invoicing data.
- **Timing and method:** Occasionally, electronically.

f) Invoicing Software Provider (KBOSS Kft. - Számlázz.hu):

- **Privacy info:** Számlázz.hu Privacy.
- **Purpose of transfer:** Invoicing.
- **Legal basis for transfer:** Compliance with a legal obligation (GDPR Article 6(1)(c)).
- **Scope of data transferred:** Invoicing data (name, address, tax ID, etc.).
- **Timing and method:** Occasionally, electronically.

g) Fire and Safety Service Provider (WENFIS Mérnök Iroda Kft.):

- **Contact details:** 2100 Gödöllő, Méhész köz 5.; Tel: +36 20 669 0090.
- **Legal basis for access:** Compliance with a legal obligation (GDPR Article 6(1)(c); Act XCIII of 1993 on Occupational Safety).
- **Scope of data transferred:** Data determined by law and related to specific inspections.
- **Duration of access:** 5 years.
- **Timing and method:** Occasionally, paper-based and electronically.

h) Storage space provider

- **Hetzner Online GmbH**

- **Contac details:** Industriestr. 25 , 91710 Gunzenhausen, DE
- **Privacy policy:** https://www.hetzner.com/legal/privacy-policy/
- **Purpose of transfer:** processing order data
- **Legal basis for access:**fullfill contractual obligationsCompliance with a legal obligation (GDPR Article 6(1)(b)
- **Scope of data transfer:** first name, surname, address, email, phone number
- **Timing and method**: electronically

8. Rights of the Data Subject

- **Right to be informed:** The data subject may request information from the Controller regarding the processing of their personal data. Within the shortest possible time, but no later than 30 days from the submission of the request, the Controller shall provide the data subject with written information in an intelligible form regarding the data processed, the purpose, legal basis, and duration of the processing, and—if data has been transferred—to whom and for what purpose the data was disclosed.
- **Right to rectification:** The data subject may request that the Controller rectify their personal data. The Controller shall comply with this request within 15 days.
- **Right to erasure ("right to be forgotten"):** The data subject may request the erasure of their personal data, which the Controller shall fulfill within a maximum of 15 days. The right to erasure does not apply if the Controller is legally obligated to further store the data, nor in cases where the Controller is entitled to continue processing the data in accordance with Section 6(5) of the Info tv. (e.g., in connection with invoicing).
- **Right to restriction of processing (blocking):** The data subject may request that the Controller block personal data if the permanent erasure of the data would prejudice the data subject's legitimate interests. Personal data blocked in this manner may only be processed for as long as the purpose precluding erasure remains valid.
- **Right to data portability:** Under this right, the data subject is entitled to receive the personal data concerning them, which they have provided to a Controller, in a machine-readable format and have the right to transmit those data to another controller without hindrance from the Controller to which the personal data was provided.
- **Right to object:** The Controller shall examine the objection within the shortest possible time, but no later than 15 days from the submission of the request, decide on its validity, and provide information on the decision in writing. If the Controller fails to comply with the data subject's request for rectification, blocking, or erasure, it shall provide the factual and legal reasons for the refusal in writing or electronically within 30 days of receiving the request.

9. Other Provisions Regarding Data Processing

Termination of Data Processing
The Controller shall delete all personal data:

- where the purpose of data processing has ceased;
- where the data subject's consent for processing is not available;
- where the data subject has withdrawn their right to processing or has prohibited processing; or
- where there is no legal basis for the processing.

Instead of erasure, the Controller shall block the personal data if the data subject so requests, or if, based on the information available, it can be assumed that erasure would prejudice the data subject's legitimate interests. Personal data blocked in this manner shall only be processed for as long as the purpose precluding erasure remains valid.

10. Procedural Rules for Handling Data Protection Complaints

The Procedure: The Controller shall treat and handle as a complaint any observation submitted in writing by a data subject, provided it concerns data protection and alleges a grievance related to an action or omission by the Controller that is inconsistent with this Privacy Notice (hereinafter: complaint).

A complaint may be filed in writing within 30 days of detecting the specific grievance, via a notification sent to the Controller’s electronic or mailing address. Exceeding this deadline results in the loss of rights.

The complaint must contain at least: the complainant's name, address (e-mail address), phone number, the date of the grievance, a specific description of the complaint, the complainant's signature, and a statement that they consent to the processing of their data provided in the complaint for the duration of the complaint procedure, simultaneously with signing the complaint. In the absence of these data and the statement, the Controller will waive the investigation of the complaint and notify the Complainant in writing.

The Controller processes the Complainant's data exclusively in connection with the complaint and will not disclose it to third parties—except for statutory requests from authorities or courts—nor use it for business purposes.

The Controller shall investigate the complaint and provide a reasoned written response within 30 days of receipt, using the same method as the complaint submission (e-mail or post). If the 30-day period is insufficient for the investigation, the Controller shall inform the complainant. In such cases, a reasoned written response will be provided within 3 months of the notification.

If, following the investigation, the Controller determines that the complaint was factual and justified, it shall inform the Complainant of the method and extent of the remedy simultaneously with the decision.

In case of rejection, the Controller shall inform the Complainant in writing that they may further appeal to the National Authority for Data Protection and Freedom of Information (hereinafter: Authority) or, in case of injury, to the Court. The contact details for the NAIH are provided below.

Pursuant to Section 52(1) of the Info tv., the Authority only investigates complaints if the data subject has already contacted the controller regarding the exercise of their rights specified in the notification prior to reporting it to the Authority.

Within this framework, under Section 14 of the Info tv., the data subject may request information from the controller regarding the processing of their personal data, the rectification of their personal data, and—with the exception of mandatory data processing—the erasure or blocking of their personal data.

11. Procedural Rules for Handling Data Subject Objections

The data subject may object to the processing of their personal data at any time. The Controller shall examine the objection within the shortest possible time, but no later than 15 days from submission, decide on its validity, and inform the applicant of the decision in a formal, verifiable manner consistent with the application (e.g., in writing or via e-mail).

If the Controller establishes that the objection is well-founded, it shall immediately terminate the processing—including further data collection and transfer—block the data, and notify all parties to whom the personal data concerned by the objection had previously been transferred, who are then obliged to take measures to enforce the right to object.

If the data subject disagrees with the Controller's decision or if the Controller fails to meet the 15-day deadline, the data subject may turn to the court or the Data Protection Authority (NAIH) within 30 days of the communication of the decision or the last day of the deadline.

The Authority facilitates the enforcement of data subject rights by issuing formal letter templates: [NAIH Complaint Management Link]

Complaint Notification:

- **NAIH:** 1055 Budapest, Falk Miksa u. 9-11.
- **E-mail:** ugyfelszolgalat@naih.hu
- **Phone:** +36 (1) 391-1400
- **Website:** www.naih.hu

12. Data Security

The Controller stores the personal data of data subjects electronically exclusively on the business computer, which is equipped with both electronic and physical protection. This prevents unauthorized access, modification, transfer, disclosure, erasure, or destruction, including accidental destruction, damage, or inaccessibility resulting from technical changes.

Paper-based data storage always takes place in a locked room, in a locked cabinet, in a manner inaccessible to unauthorized persons.

13. Personal Data Breach and Management

Personal Data Breach: any activity, intervention, or omission that allows the unlawful processing or handling of personal data, in particular unauthorized access, alteration, transfer, disclosure, erasure or destruction, as well as accidental destruction and damage.
Anyone observing such an incident in connection with the Controller's activities should report it as soon as possible via e-mail to: info@carryall.hu.

The Controller shall record the report and immediately begin an investigation. If the breach affects an IT system, the Controller shall inform the service providers responsible for operating the affected databases.

To investigate and manage the breach, the Controller collects all information necessary for identification, damage mitigation, and the formulation of further remedial measures. Where possible, the following are recorded (per Annex No. 1):

- the time and place of the breach;
- a description, circumstances, and effects of the breach;
- the scope and number of data compromised;
- the range of persons affected by the compromised data.

Furthermore—in compliance with legal requirements—the Controller shall notify the Authority (NAIH) within 72 hours.

Data Protection Officer: The Controller does not process large quantities and/or specifically sensitive personal data in connection with its core activities and is not a public authority; therefore, it does not consider the appointment or employment of a data protection officer necessary, nor is it required by current legal regulations.

Note: The Controller reserves the right to continuously update this Privacy Notice and to unilaterally modify the information detailed herein, following changes in legislation. Any modifications are available at the Controller's office during working hours.

Veszprém, 2024. January

CarryAll Hungary Kft.

1. **Annex**

Data protection incident register (sample, with examples)

sorszám	incidens észlelés időpontja (év, hó, nap, óra, perc)	megnevezése	érintettek köre	érintett személyes adatok	incidens hatása	intézkedés
1 / 2024	……	hacker támadás	ügyfél adatbázis	név, e-mail cím, telefonszám	zsarolás-veszély	NAIH + érintettek tájékoztatása
2 / 2024						
3 / 2024						

2. **Annex**

Camera map (includes all cameras)

sorszáma	Hol van a kamera?	Mit lát?	Hol van a központi egysége	Egyéb megjegyzés
1.	Raktárban mennyezetre függesztve	a raktár főbejáratán belépőket, rámpákat	központi iroda, IT	
2.	Raktárban mennyezetre függesztve	Polcokat, előkészítőt		
3.	Raktárban mennyezetre függesztve	visszárú zónát		