

This Privacy Policy provides information about the processing of personal data by companies within the MV GROUP—specifically, how they collect, process, and store it. We understand the importance of personal data protection, so we respect the privacy of our customers and other data subjects (hereinafter referred to as “**data subjects**”) and protect their personal data.

The MV GROUP includes UAB MV GROUP Distribution LT, UAB MV GROUP Production, UAB MV GROUP, UAB MV GROUP Logistics and other companies (information about all group companies is available at www.mvgroup.eu/kontaktai); all MV GROUP companies are hereinafter collectively referred to as the “**MV GROUP**”, and each individually as the “**Company**” or the “**Data Controller**”.

Your Data Controller is the MV GROUP company to which you have provided your personal data in connection with a contractual relationship involving you, or whose services you (or the legal entity you represent) intend to use or are using, and/or which determines the purposes and means of personal data processing.

Each company within the MV GROUP implements and continuously updates appropriate organisational and technical security measures to protect personal data from accidental or unlawful destruction, alteration, disclosure, and any other unauthorised processing.

Detailed information on the processing of personal data at Bottlery and Nespresso stores, as well as on e-commerce platforms, is provided in the privacy policies of the respective stores and e-commerce websites.

1. Purposes, Categories, and Legal Bases for the Processing of Personal Data

1.1. Conclusion and Performance of Contracts with Customers. Compliance with Accounting Requirements

Legal basis for data processing	Data categories
Performance of a contract with the data subject (GDPR Article 6(1)(b)), compliance with legal obligations (GDPR Article 6(1)(c)), legitimate interest in entering into a contract (GDPR Article 6(1)(f))	Conclusion and performance of contracts (including documents securing contract performance, such as promissory notes) and preparation of declarations: customer’s, their employee’s, or representative’s name, surname, position, email address and/or phone number, date of birth or personal identification number, and preferences related to the provision of services. For the purpose of entering into and performing contracts with natural persons, additional personal data may also be processed. The categories of customer personal data processed in a specific case depend on the nature of the contract concluded and performed. In any event, data processing is limited to what is necessary for contract performance or statutory compliance.

Legal basis for data processing	Data categories
	Compliance with accounting requirements: when issuing invoices, the processed personal data includes the name, surname, address, and other information, if requested by the customer. When administering incoming invoices and transfer-acceptance deeds, only the personal data required by applicable laws and regulations is processed.

1.2. Direct Marketing and Loyalty Programs

Legal basis for data processing	Data categories
Consent (Article 6(1) (a) of the GDPR) or legitimate interests (Article 6(1) (f) of the GDPR) (if the conditions set out in the Law on Electronic Communications are met). In accordance with the provisions set out in the Law on Electronic Communications of the Republic of Lithuania, we may process your personal data for direct marketing purposes without your prior consent, in pursuit of our legitimate interests as a data controller (Article 6(1)(f) of the GDPR).	Name, surname, date of birth, address, city, phone number, email address, and other data. Information is also processed regarding goods purchased by customers, purchase and delivery timing, purchase amounts, methods, and frequency, when direct marketing content is provided to loyalty program participants or when an individual consents to receive offers specifically intended for loyalty program participants. If you have consented to receive offers and news, we process your personal data to provide you with such information, including general newsletters and information about offers, discounts, promotions, and sales provided by us and our partners. We may also invite you to participate in promotions or games to win prizes, or request your feedback on our services and products. Offers and information are provided through your chosen channels, such as email or SMS. Only individuals aged 14 and over may subscribe to our newsletters. Newsletters containing offers for alcoholic beverages or tobacco products may only be subscribed to by individuals who have reached the legal age required by law to purchase such products. You may object to or opt out of receiving offers and news at any time. Your refusal to receive offers and news will not prevent you from using the Services.

1.3. Processing of Personal Data of Shareholders, Beneficial Owners, Management Bodies, Other Bodies, and Their Members for the Purposes of Internal Administration and Compliance

Legal basis for data processing	Data categories
Compliance with legal requirements (Article 6(1)(c) of the GDPR)	Name, surname, personal identification number, date of birth, residential address, information about securities held, bank account details, payment details, and other personal data required to be processed by law. In fulfilling obligations related to the provision of information on ultimate beneficial owners to the JANGIS subsystem of the State Enterprise Centre of Registers (complying with legal obligations regarding the prevention of money laundering and terrorist financing), the following personal data of shareholders and the company's CEO are processed: name, surname, and personal identification number. In this case, the following personal data of ultimate beneficial owners is also processed: name of the state, name(s) of the state(s) of residence for tax purposes, the beneficial owner's ownership and/or control rights, and their scope.

Legal obligations related to the Company's management and other bodies include their formation, the organization of their activities, the submission of information regarding the Company's management bodies and their members to public registries and their registration, and compliance with other legal requirements.

1.4. E-commerce Operations

Legal basis for data processing	Data categories
Performance of a contract (Article 6(1)(b) of the GDPR)	Name, surname, email address, mobile phone number, delivery address, signature of the person receiving the goods, date and time of purchase and delivery, product names, quantities, purchase prices and discounts applied, payment method, and payment details.

1.5. Video surveillance for the purpose of protecting property and ensuring the safety of the Companies' employees and other individuals, as well as of safeguarding their lives, health, property, and other rights and freedoms.

Legal basis for data processing	Data categories
Legitimate interest in protecting property, health, and life (Article 6(1)(f) of the GDPR)	Video footage showing people entering the surveillance area (in stores, visitor centres, and office spaces)

1.6. Handling and Processing Complaints, Requests, and Reports from Individuals. Drafting and Implementing Other Legal Documents. Representation in Courts, Arbitrations, Supervisory, and Other Institutions (e.g., Commissions, Agencies, Associations).

Legal basis for data processing	Data categories
Performance of a contract (GDPR Article 6(1)(b)), compliance with legal obligations (GDPR Article 6(1)(c)), legitimate interests (GDPR Article 6(1)(f))	Contact information: name, surname, phone number, email address, social media account details—username, profile picture, message history, residential address, personal identification number/date of birth, content of the inquiry: the event regarding which the inquiry is made, its circumstances, date, location, request, claim, or feedback, product, other information provided in the inquiry; other documents and/or data submitted with the inquiry: e.g., purchase receipt details, photos, audio recording and information contained in the audio recording, data substantiating the individual's legal obligations to the Data Controller or the Data Controller's legal obligations to the individual.

1.7. Capturing Events in Photographs and Video Recordings

Legal basis for data processing	Data categories
Consent, including implied consent through conduct, i.e., by participating in an event after being provided with detailed information about the conditions for the processing of personal data (GDPR Article 6(1)(a)), performance of a contract (GDPR Article 6(1)(b)), or legitimate interests in disseminating information about the company's activities (GDPR Article 6(1)(f))	Images in photographs and videos depicting individuals participating in events organised by the MV GROUP

We process your personal data in order to disseminate information about our company's activities, to give you the opportunity to participate in our events, and to allow you to use our products or services.

We process personal data when you participate in events or other activities at our stores or other locations. To avoid being photographed or filmed, participants in events organised by the MV GROUP may choose not to attend or otherwise clearly express their objection, e.g., if you do not wish to be photographed and/or filmed, please clearly indicate this and/or inform the person capturing your image.

If photography and filming take place during the event, the photos and videos may be used for publicity purposes. By participating in the event, you agree that your image may be published in the public domain.

1.8. Event Planning and Management

Legal basis for data processing	Data categories
Consent (GDPR Article 6(1)(a)), performance of a contract (GDPR Article 6(1)(b)), compliance with legal obligations (GDPR Article 6(1)(c)), or legitimate interests (GDPR Article 6(1)(f))	Participants' personal data, to the extent necessary for the purpose and in accordance with legal requirements; lists of participants; photographs and video recordings depicting event participants

1.9. Organisation and Administration of Games, Contests, and Promotions

Legal basis for data processing	Data categories
Consent (GDPR Article 6(1)(a)), performance of a contract (GDPR Article 6(1)(b)), compliance with legal obligations (GDPR Article 6(1)(c)), or legitimate interests (GDPR Article 6(1)(f))	Name, surname, contact information, social media account name, social media account details, age, and other personal data of participants, to the extent necessary for the purpose and in accordance with legal requirements.

1.10. Recruitment and Evaluation of Candidates for Employment or Internship, Administration of the Candidate Database, and Provision of Job Offers

Legal basis for data processing: Consent (GDPR Article 6(1)(a))
Data categories: General personal data of job applicants (interns): name, surname, date of birth, residential address, email address, phone number, information regarding work experience (employer, period of employment, duties, responsibilities, achievements), information regarding education (educational institution, period of study, degree obtained, qualifications), information regarding professional development (courses completed, certificates obtained), information about the languages the candidate speaks and their proficiency level, information technology skills, driving skills, and other competencies, other information provided by the job applicant in their resume (CV), cover letter (if submitted), or other job application (internship) documents. Employer feedback on the job candidate (intern), recommendations: the person providing the feedback or recommendation, and their contact information. Employer feedback on the job candidate (intern), recommendations: the person providing the feedback or recommendation, and their contact information. Information on the evaluation of the job candidate (intern): a summary of the interview with the job candidate (intern), the opinions and observations of the person(s) conducting the selection process, and the results of the candidate's testing (if conducted). Special categories of personal data: health data and data regarding unspent convictions for intentional offenses. The Company collects special categories of personal data from job

applicants only to the extent necessary for the recruitment process for a specific position and to the extent permitted by applicable laws.

We will collect and process your health data during the selection process in accordance with applicable laws to assess your fitness for work, the suitability of the workplace for your health condition, and/or your ability to work under conditions involving occupational risks. In all cases, we will collect special category data only during the final stages of the selection process.

We obtain the personal data of job applicants (interns) directly from the applicants themselves or from recruitment agencies, online job search portals, and/or other entities that provide job search, selection, and/or placement services. If we receive information about your application and (or) your resume, and/or other application documents from recruitment agencies, online job search portals, career social networks (e.g., LinkedIn), and/or other entities providing job search, recruitment, and/or placement services, we assume that you have received all necessary information regarding the processing of your data and have given your consent to the processing of your data to the relevant entity providing such services, which also includes the right to provide your data to potential employers (including the Company), authorizing such potential employers to process your data during the recruitment process for the position(s) and when evaluating your candidacy.

We will verify the references you provide or request feedback from your employer only if you give us your consent to contact the employer and/or other person you have named and obtain feedback about you.

1.11. Debt Recovery in Cases of Default on Obligations

Legal basis for data processing	Data categories
The data controller's legitimate interest in debt collection (Article 6(1)(f) of the GDPR)	Personal data of debtors and representatives of legal entities: name, surname, address, phone number, and email address.

1.12. Promoting Brand Awareness on Social Media

Facebook:

MV GROUP | Facebook: <https://www.facebook.com/WeAreMVGroup>;

UAB MV GROUP Logistics | Facebook: <https://www.facebook.com/logistikospaslaugos>;

MV GROUP Distribution Poland | Facebook:
<https://www.facebook.com/MVGroupDistributionPoland>;

MV GROUP Distribution Estonia | Facebook: <https://www.facebook.com/MvEesti>;

We are MV GROUP | Facebook: <https://www.facebook.com/groups/wearemvgroup>;

LinkedIn:

MV GROUP | LinkedIn: <https://www.linkedin.com/company/mvgroup/>;

YouTube:

We are MV GROUP | YouTube: <https://www.youtube.com/@wearemvgroup3966>;

Other MV GROUP companies on social media.

Legal basis for data processing	Data categories
Legitimate interests of the data controller (GDPR Article 6(1)(f)) to provide information about upcoming events, to share news, to increase brand awareness, to organise contests and games, to interact with our followers and social media page visitors, and to tailor the information we provide and other activities on our accounts to the needs of account visitors.	The social media account information you provide—your username, profile picture, chat history, reactions you have expressed to posted information, comments you have left, and content you have posted on our account (e.g., if you share photos or videos in comments, other information provided).

The personal data you provide when performing certain actions on social media platforms is processed and stored in accordance with the procedures and timeframes established by the social media platform operators, and we have no control over this. You can find more information about social media privacy in the privacy notices of the data controllers:

Facebook: <https://www.facebook.com/policies/cookies>

Instagram:

[Instagram Privacy | About Instagram](#)

LinkedIn: [LinkedIn Privacy Policy](#)

YouTube: [Privacy Policy – Privacy & Terms – Google](#)

The information you provide to the MV GROUP or to a company within the MV GROUP via their Facebook or LinkedIn accounts (including posts, use of the “Like” and “Follow” buttons, and other communications), or that is collected when you visit these accounts on Facebook or LinkedIn, is controlled by the social network operator; therefore, we recommend that you read the privacy notices of the social network administrators. When managing an account, the MV GROUP or a company within the MV GROUP selects appropriate settings, taking into account the target audience and the objectives of operational management and promotion. By allowing you to create an account, the social media platform operator may have restricted your ability to change certain settings; thus, we cannot influence what information the operator collects about you.

Generally, the social network operator processes your personal data for the purposes specified by the social network operator, in accordance with the social network operator’s privacy policy. However, when you use the social network, interact with the MV GROUP or a company within the MV GROUP on it, visit your account on it, or view posts there, the Company receives information about you. The scope of the data received depends on the account settings we have selected, agreements with the social network operator regarding the ordering of additional services, and cookies set by the social network operator.

You may exercise your right to object to the processing of personal data on social networks in accordance with the procedures established by the social network operators.

1.13. Processing of Requests Regarding the Data Subject's Rights under the GDPR

Legal basis for data processing	Data categories
Compliance with legal requirements; the legal obligation to ensure the exercise of data subjects' rights (Article 6(1)(c) of the GDPR).	Details provided in the request, e.g., name, surname, phone number, address, date of birth, email address, account number, legal entity code, a copy of an identity document, a request to exercise the data subject's rights, the date of the request, the location of the request, the specified method for providing a response to the request, the content of the request, and other information provided in the data subject's request, the response to the data subject, other information related to the exercise of the data subject's rights.

1.14. Provision of Tasting-Related Services

Legal basis for data processing	Data categories
Performance of a contract (Article 6(1)(b) of the GDPR)	First name, email address, phone number, and information regarding your service requests.

1.15. Administration and Evaluation of Information Regarding Possible Violations within the Company

Legal basis for data processing	Data categories	
Legal obligation (Article 6(1) of the GDPR and the Law on the Protection of Whistleblowers of the Republic of Lithuania).	Data of the reporting person and the person allegedly involved in the violation, identification data, and other information provided in the report: e.g., name, surname, personal identification number, workplace, position, phone number, personal email address, or residential address.	
	Information on the Relationship with the Company	Workplace (current or former service, employment, or contractual relationship with the Company, etc.) and position.

Legal basis for data processing	Data categories	
	Contact details	Phone number, personal email address, or home address.
	Data in relation to the provision of information	The fact that information was provided to the Company, the date and time (where applicable), the content of the report (including any personal data about you contained in the report or its attachments), and, where applicable, the fact that a response was provided to the report, along with the date and time (where applicable).
	Other personal data	Correspondence (where a natural person can be identified from it) and a signature.
	Data of the witness(es) specified in the report	
	Identification data	Name and surname
	Contact details	Phone number and email address.
	Other data	Place of employment and job title; the fact and content of the submission of a report regarding which you can testify; correspondence (where it is possible to identify a natural person from it).

1.16. Use of Cookies

Cookies are small text data files that are automatically created while you browse our website and are stored on your device (computer or mobile phone). Cookies are used to make the website function or to improve its performance and efficiency.

Detailed information on the use of cookies is provided in the **website's Cookie Policy**.

1.17. Processing of Personal Data for Other Purposes

Companies within the MV GROUP may process personal data for other purposes specified in the Privacy Policy available on the website of the relevant MV GROUP company.

Additionally, for each specific purpose, a company within the MV GROUP may process categories of personal data other than those specified in this Privacy Policy. In such cases, the information provided in the relevant company's Privacy Policy within the MV GROUP shall take precedence.

2. Where do we obtain personal data from, and in which cases do we transfer your personal data?

In most cases, personal data is provided directly by the data subject. In certain cases, we may obtain personal data from third parties, such as recruitment agencies, job search portals, and other entities that provide job search, selection, and/or mediation services.

Your personal data may be provided to state and municipal authorities, as well as other persons performing functions assigned to them by law, if such an obligation is provided for by legal acts. We transfer your personal data upon their request or in pursuit of our legitimate interest to establish, exercise, or defend legal claims.

Your personal data may be disclosed to state and municipal authorities and other entities performing functions assigned to them by law, if such an obligation is provided for by law. We transfer your personal data upon their request or to pursue our legitimate interest in asserting, exercising, or defending legal claims.

In cases where it is necessary to achieve the relevant purposes, your personal data may be transferred to the following third parties:

- To other companies within the MV GROUP, when they perform functions necessary to achieve the relevant purpose.
- We may transfer your data to third parties who assist us in conducting our business and administering the provision of our Services. Such parties may include data centres, hosting and related service providers, advertising, recruitment, call centre, and marketing service providers, companies that develop, provide, support, and maintain software, companies that provide information technology infrastructure services, companies providing communication services, companies analysing and providing services related to internet browsing or online activity, security or other service providers, companies providing advertising, event, and game organization services; companies providing newsletter distribution and public relations services; companies providing short SMS messaging and delivery services, where necessary to deliver goods you have purchased, for the purposes of direct marketing, e-commerce, and participation in loyalty programs.
- To other third parties when necessary to achieve the relevant purpose, as well as when required by applicable laws or in cases and in accordance with procedures provided for by

law, in order to safeguard our rights, the safety of our customers, employees, and resources, and to assert, exercise, and defend legal claims.

- In each case, we provide the data processor with only as much data as is necessary to fulfil a specific task or provide a specific service.
- Personal data may also be disclosed to competent government or law enforcement authorities, such as the police, the prosecutor's office, or other supervisory authorities, but only upon their request and only when required by applicable laws or in cases and in accordance with procedures provided for by law, in order to ensure our rights, the safety of our customers, employees, and assets, and to assert, exercise, and defend legal claims.
- The data processors we engage may process your personal data only in accordance with our instructions and may not use it for other purposes or disclose it to other parties without our consent. Furthermore, they are required to ensure the security of your data in accordance with applicable laws and the written agreements concluded with us.
- Where there is a legitimate basis (e.g., when it is necessary for the conclusion or performance of a contract with you and you have been duly informed of such a transfer), data may be transferred to our business partners, contractors, and the like.
- Transfer of personal data for the purposes of conducting recruitment for a job position(s), evaluating candidates, managing a database of job applicants, and making job offers.
- In other cases, with the individual's consent or after carefully assessing the purpose and legal basis for providing and receiving the data, and ensuring that no more data is transferred than is necessary to achieve the purpose, while also ensuring the security of the transferred data.

When the Company processes personal data for the purpose of recruiting employees or interns, the Company may also transfer the personal data of candidates for employment or internships to other companies within the group to which the Company belongs, provided that they are involved in the evaluation processes for candidates for managerial positions or internships.

3. Transfer of Personal Data outside the European Economic Area

In most cases, personal data is processed and transferred within the territory of the European Union (EU) and the European Economic Area (EEA); however, where necessary for the provision of certain services, data may be transferred and processed outside these territories, provided that an adequate level of personal data protection is ensured. Personal data may be transferred outside the EU or the EEA, e.g., when such a transfer is necessary for the conclusion and performance of contracts and the proper provision of services. In such cases, measures are taken to ensure that any transfer of personal data outside the EU and the EEA is carried out properly and that data subjects' rights to privacy are protected to the maximum extent possible. When transferring personal data outside the EU and the EEA, we comply with the requirements of Chapter V of the GDPR.

Where permitted by law and necessary for the reasons set out in Section 2 of this Privacy Notice, we disclose information about you:

- based on a decision by the European Commission on adequacy, meaning that the European Commission has recognised the country in which the third party is established and/or operates as ensuring an adequate level of personal data protection;
- we have entered into a contract with the third party based on the Standard Contractual Clauses (SCCs) approved by the European Commission;
- we have obtained authorisation from the State Data Protection Inspectorate;
- we have utilised, where possible, other available personal data protection measures and derogations.

4. What rights does a data subject have, and how can they exercise them?

- **The right to access your personal data that we process**

You have the right to obtain confirmation from us as to whether we are processing your personal data, as well as the right to access the personal data we process and information regarding the purposes of data processing, the categories of data processed, the categories of data recipients, the duration of data processing, the sources of the data, automated decision-making, including profiling, and its significance and consequences for you.

- **Right to rectify personal data**

If the data you provided to us in your registration form has changed, or if you believe that the information we process about you is inaccurate or incorrect, you have the right to request that this information be changed by logging into your account, and if you are unable to do so, you have the right to correct the data by contacting us using the contact details provided below.

- **Right to withdraw consent**

If we process your data based on your consent, you have the right to withdraw it at any time, and the processing will cease. In certain cases, this may mean that we will no longer be able to provide you with access to our services. You can manage your consent to receive offers and information about products (withdraw or re-grant it) in your account under the Newsletters section. When sending direct marketing content to a data subject via email or other means, we provide the customer with a convenient, free, and simple (easy) option to opt out of receiving further such information. In the informational message or newsletter, simply click the link to unsubscribe from the informational messages and newsletters service. Upon unsubscribing from the informational messages and newsletters service, the data subject's consent (to receive future newsletters) for the processing of personal data for direct marketing purposes is also revoked.

- **Right to lodge a complaint**

If you believe that we are processing your data in violation of data protection laws, we always ask that you contact us directly first. We believe that through good-faith efforts, we will be able to address all your concerns, fulfil your requests, and correct any errors we may have made. If you are

not satisfied with the solution we propose or, in your opinion, we do not take the necessary actions in response to your request, you have the right to lodge a complaint with the supervisory authority (in Lithuania—the State Data Protection Inspectorate (L. Sapiegos g. 17, Vilnius, Lithuania; email address: ada@ada.lt).

- **Right to object to data processing when processing is based on legitimate interests**

You have the right to object to the processing of your personal data when such processing is based on our legitimate interests. However, given the purposes of providing the services and the balance of legitimate interests of both parties (both you, as the data subject, and us, as the data controller), your objection may mean that, upon ceasing the processing of your data based on our legitimate interests, we will not be able to allow you to continue using the services.

- **Right to erasure (right to be forgotten)**

Under certain circumstances specified in data protection laws (such as when personal data is processed unlawfully, the basis for processing has ceased to exist, etc.), you have the right to request that we erase your personal data.

- **Right to restrict data processing**

Under certain circumstances specified in data protection laws (when personal data is processed unlawfully, you contest the accuracy of the data, you have objected to data processing based on our legitimate interests, etc.), you also have the right to restrict the processing of your data. However, we must note that due to the restriction of data processing and during the period of such restriction, we may be unable to provide you with our services.

- **Right to data portability**

You have the right to receive or transmit your personal data to another data controller (right to data portability). This right applies only to data that you have provided to us based on your consent or under a contract, and only where the data is processed by automated means.

- **Right to object to fully automated processing of personal data**

You have the right to object to being subject to a decision based solely on automated processing, including profiling, if such decision-making may have legal consequences or similarly significant effects on you.

5. Exercising Your Rights

To exercise your rights as set forth in this Privacy Policy, you may:

- Submit a request to exercise your data subject rights in person at the registered office of a specific MV GROUP company (www.mvgroup.eu/kontaktai) or to the Data Protection Officer at the email addresses specified in this Privacy Policy.
- When contacting us regarding data processing and the exercise of your rights, please submit a properly completed Data Subject recommended Request Form, which can be filled out at this link: [Form](#).

- If the request is submitted through a representative, the request must be accompanied by a document confirming the representative's authority or a copy thereof, certified in accordance with the procedure established by law.
- To protect data subjects' data from unauthorised disclosure, upon receiving your request to provide data or exercise your other rights, we may need to verify your identity; for this purpose, we may ask you to provide proof of your identity. Upon receiving a request signed with a qualified electronic signature, the data controller will assess its content and the available information regarding the data subject. If there are reasonable doubts regarding the data subject's identity, the data controller may request additional verification methods, including the submission of a request signed with a qualified electronic signature. For this purpose, we may ask you to provide your name, surname, email address, or phone number, and we will verify whether the data you provide matches the relevant data. While performing this verification, we may also send a verification message to the provided contact (via SMS or email), requesting that you complete an authorisation step. If the verification process is unsuccessful (e.g., the data provided does not match our records, or you fail to authenticate yourself via the SMS or email message received), we will conclude that your identity as the data subject cannot be established, and your request will be rejected.

Once your identity is successfully verified, we will provide information on the actions taken in response to your request without undue delay, and no later than one month from receiving both the request and the required verification. Taking into account the complexity and number of requests, we have the right to extend the one-month period by a further two months, and we will inform you thereof before the end of the first month and provide the reasons for such an extension.

If your request is submitted electronically, we will also provide our response electronically unless this is not possible (e.g., due to an exceptionally large volume of information) or you request that we respond in another manner.

If there are legal grounds to deny your request, we will notify you in writing and provide a reasoned explanation for our decision.

6. How can you contact the Data Controller or the Data Protection Officer?

If you have any questions, comments, or complaints regarding how we collect, use, and store information about you, or if you wish to exercise your rights as a data subject, you may contact the relevant data controller (a list of companies is available at www.mvgroup.eu/kontaktai) or the Data Protection Officer/person responsible for data protection:

Data Controller	Email address
UAB MV GROUP Distribution LT	dataprotection@mvgroup.eu
UAB MV GROUP Production	dataprotection@mvgroup.eu

Data Controller	Email address
UAB MV GROUP Logistics	dataprotection@mvgroup.eu
UAB MV GROUP Distribution PL	dataprotection.distributionPL@mvgroup.eu
UAB MV GROUP Distribution EE	dataprotection.distributionEE@mvgroup.eu
UAB MV GROUP Distribution LV	dataprotection.distributionLV@mvgroup.eu
UAB MV GROUP	dataprotection@mvgroup.eu

7. How long do we retain personal data?

We retain personal data no longer than is necessary for the purposes of data processing or as required by law, if such laws provide for a longer retention period. Personal data may be stored for longer than specified if required by law or when necessary for the Company to defend itself against claims, complaints, or lawsuits filed against it, as well as when personal data is required for an investigation or as evidence in civil, administrative, or criminal proceedings.

Purposes of data processing	Data retention period
Conclusion and performance of contracts (including documents securing contract performance, e.g., promissory notes) and preparation of declarations. Compliance with accounting requirements.	During the term of the contract and for 10 years after the contract's expiration (performance). During the term of an Authorship Contract or Contract for the Provision of Intellectual Services (taking into account the period specified in the contract for which economic copyrights have been transferred) and for 10 years after the expiration (performance) of the contract. Accounting and tax documents are retained in accordance with legislative requirements to ensure compliance. Invoices are retained for 10 years after issuance. Upon expiration of the retention period, personal data is no longer retained as of the last calendar day of the year in which the retention period ended.
Direct marketing and participation in loyalty programs	As long as your consent to receive offers and news is in effect, but no longer than five (5) years from the date you gave your consent, unless you withdraw your consent during this period or a different validity period is specified. We may retain your consent and

Purposes of data processing	Data retention period
	proof thereof for a longer period if necessary to defend against claims, complaints, or lawsuits brought against us.
Processing of personal data of shareholders, beneficiaries, management bodies, other bodies, and their members for the purposes of internal administration and compliance with legal obligations	The Company retains this data for as long as necessary to achieve the purposes for which it is processed, as well as in accordance with the statutory requirements for the retention of such data, statute of limitations periods for asserting or defending legal claims, and, if such claims are asserted, for as long as necessary for this purpose. Information intended to ensure a shareholder's property right to receive a share of the company's profits (dividends) is retained for as long as the person is a shareholder of the Company and, taking into account the statute of limitations, for an additional 10 years. Upon expiration of the retention period, personal data is no longer retained as of the last calendar day of the year in which the retention period ended.
E-commerce operations	The terms specified in the privacy policies of specific online stores apply.
Video surveillance for property protection	No longer than 30 days.
Handling and processing complaints, requests, and reports from individuals; drafting and executing other legal documents. Representation in courts, arbitration proceedings, and before regulatory and other institutions (e.g., commissions, agencies, associations).	For no longer than 1 (one) year from the date the decision is made by the Company, provided there is no dispute between the parties and the data is not used for legal proceedings. If a violation is identified, the data will be retained for the duration of the applicable statute of limitations. Upon expiration of the retention period, personal data is no longer retained as of the last calendar day of the year in which the retention period expired.
Capturing events in photographs and video recordings	Personal data collected during events (photos, videos) is stored for no more than five (5) years from the end of the year in which it was collected. If a different retention period for personal data is specified in a contract, consent, or event notice, the

Purposes of data processing	Data retention period
	retention period specified in the contract, consent, notice, or other document shall apply. Historical photographs and video recordings (particularly significant to the Companies) are stored indefinitely. Personal data collected for event registration is stored for six (6) months after the end of the event, unless a different retention period for personal data is specified in the invitation or event notice. Upon expiration of the retention period, personal data is no longer retained as of the last calendar day of the year in which the retention period expired.
Organisation and administration of games, contests and promotions	Personal data is stored no longer than the period during which a complaint regarding the game or promotion may be filed.
Conducting recruitment for job openings (internships) and evaluating candidates	[Data is stored] while we are conducting the selection process for the position(s) you have chosen, but no longer than six (6) months.
Managing a database of job candidates (interns) and making job (internship) offers	[Data is stored] for the period specified in the consent to be included in the candidate database, but no longer than three (3) years. Upon expiration of the retention period, personal data is no longer stored as of the last calendar day of the year in which the retention period ended.
Debt collection in cases of non-compliance with obligations	Until the bailiff's enforcement proceedings are completed. If no enforcement proceedings have been initiated, then [data is retained for] five (5) years from the date the enforcement document was issued.
Promoting awareness on social media	Information regarding the retention periods for personal data is provided in the privacy policies of social media platforms and in this Privacy Policy, depending on the specific purpose of data processing.

Purposes of data processing	Data retention period
Processing requests regarding the rights of data subjects as provided for in the GDPR	Requests are retained for five (5) years from the date the response is provided. Upon expiration of the retention period, personal data is deleted as of the last calendar day of the year in which the period ended.
Provision of tasting-related services	No longer than 1 (one) year from the date the service was provided. Upon expiration of the retention period, personal data is no longer retained as of the last calendar day of the year in which the retention period ended.
Administration and evaluation of information regarding potentials violations within the Company, as specified in the reporting rules	Five (5) years from the date of the last decision made regarding this information. Upon expiration of the retention period, personal data is no longer stored as of the last calendar day of the year in which the retention period ended.
Use of cookies	Data is stored in accordance with the terms specified in the cookie list.

8. Changes to the Privacy Policy

We reserve the right to update this Privacy Policy by posting changes on www.mvgroup.eu. We encourage you to visit our website regularly to review the latest version.

Effective as of 27 February 2026