

Date

11 February 2026

Our reference

2023-225260

z2015-01024

Contact

070 8888 500

Subject

Decision approving Controller Binding Corporate Rules of Heineken

The Autoriteit Persoonsgegevens,

Pursuant to the request by **Heineken International B.V.**, on behalf of the group **Heineken N.V.** (hereinafter '**Heineken**'), received on **11 December 2015**, reference **2023-225260**, formerly z2015/01024, for approval of their binding corporate rules for controller;

Having regard to Articles 47, 57 and 64 of the 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, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR);

Having regard to the judgment of the Court of Justice of the European Union in Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems, C-311/18 of 16 July 2020;

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021;

Having regard to EDPB Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR) of 20 June 2023 (hereinafter "the Recommendations 1/2022");

Makes the following observations:

1. Article 47(1) of the EU General Data Protection Regulation 2016/679 (GDPR), provides that the competent Supervisory Authority shall approve Binding Corporate Rules (BCRs) provided that they meet the requirements set out under this Article.
2. The implementation and adoption of BCRs by a group of undertakings is intended to provide guarantees to controllers and processors established in the EU as to the



Date

11 February 2026

Our reference

2023-225260

protection of personal data that apply uniformly in all third countries and, consequently, independently of the level of protection guaranteed in each third country.

3. Before carrying out any transfer of personal data on the basis of the BCRs to one of the members of the group, it is the responsibility of any data exporter in a Member State, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country of destination in the case of the specific data transfer, including onward transfer situations. This assessment has to be conducted in order to determine whether any legislation or practices of the third country applicable to the to-be-transferred data may impinge on the data importer's and/or the data exporter's ability to comply with their commitments taken in the BCR, taking into account the circumstances surrounding the transfer. In case of such possible impingement, the data exporter in a Member State, if needed with the help of the data importer, should assess whether it can provide supplementary measures in order to exclude such impingement and therefore to nevertheless ensure, for the envisaged transfer at hand, an essentially equivalent level of protection as provided in the EU. Deploying such supplementary measures is the responsibility of the data exporter and remains its responsibility even after approval of the BCRs by the competent Supervisory Authority and as such, they are not assessed by the competent Supervisory Authority as part of the approval process of the BCRs.
4. In any case, where the data exporter in a Member State is not able to implement supplementary measures necessary to ensure an essentially equivalent level of protection as provided in the EU, personal data cannot be lawfully transferred to a third country under these BCRs. In the same vein, where the data exporter is made aware of any changes in the relevant third country legislation that undermine the level of data protection required by EU law, the data exporter is required to suspend or end the transfer of personal data at stake to the concerned third countries.
5. In accordance with the cooperation procedure as set out in the Working Document WP263 rev01,¹ the Controller BCRs application of **Heineken** was reviewed by the Autoriteit Persoonsgegevens as the competent supervisory authority for the BCRs (BCR Lead) and by two Supervisory Authorities (SA) acting as co-reviewers, *in this case the French and German (Nordrhein-Westfalen) SAs*. The application was also reviewed by the concerned SAs to which the BCRs were communicated as part of the cooperation procedure.
6. The review concluded that the Controller BCRs of **Heineken** comply with the requirements set out by Article 47(1) of the GDPR as well as the Recommendations 1/2022 and in particular that the aforementioned BCRs:

¹ Endorsed by the EDPB on 25 May 2018.



Date

11 February 2026

Our reference

2023-225260

- i) Are legally binding and contain a clear duty for each participating member of the Group including their employees to respect the BCRs by entering in an Intra-Group Agreement (*Section 5 of the application form and Article 1.4 of the BCRs*);
- ii) Expressly confer enforceable third-party beneficiary rights to data subjects with regard to the processing of their personal data as part of the BCRs (*Article 18.1 of the BCRs*);
- iii) Fulfil the requirements laid down in Article 47(2) of the GDPR:
 - a) The structure and contact details of the group of undertakings and each of its members are described in the Application form of the Recommendations 1/2022 that was provided as part of the file review in *Section 5 of the application form*;
 - b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question are specified in *Annex 2 to the BCRs*;
 - c) the legally binding nature, both internally and externally, of the Controller BCRs is recognized in *Article 1.4 of the BCRs*;
 - d) the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules are detailed in *Articles 1.5, 2-6, and 8-11 of the BCRs*;
 - e) the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 22 of the GDPR, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States in accordance with Article 79 of the GDPR, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules which are set forth in *Articles 7, 9, and 10 of the BCRs*;
 - f) the acceptance by the controller or processor established on the territory of a Member State of its liability for any breaches of the binding corporate rules by any member concerned not established in the Union as well as the exemption from that liability, in whole or in part, only if the concerned party proves that that member is not responsible for the event giving rise to the damage are specified in *Article 18.2 of the BCRs*;

Date

11 February 2026

Our reference

2023-225260

- g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of Article 47.2 of the GDPR are provided to the data subjects in addition to Articles 13 and 14 of the GDPR, is specified in *Articles 1.5 and 6 of the BCRs*;
- h) the tasks of any data protection officer designated in accordance with Article 37 of the GDPR or any other person or entity in charge of monitoring the compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling are detailed in *Article 13 of the BCRs*;
- i) the complaint procedures are specified in *Article 17 of the BCRs*;
- j) the mechanisms put in place within the group of undertakings for ensuring the monitoring of compliance with the binding corporate rules are detailed in *Article 16 of the BCRs*. Such mechanisms include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. The results of such monitoring are communicated to the person or the entity referred to in point (h) above and to the board of the controlling undertaking of the group of undertakings (in this situation to **Heineken N.V.**, as well as to the data privacy organization) and are available upon request to the competent supervisory authority;
- k) the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authorities are specified in *Article 21 of the BCRs*;
- l) the cooperation mechanism put in place with the supervisory authority to ensure compliance by any member of the group of undertakings is specified in *Articles 16.2 and 18.6 of the BCRs*. The obligation to make available to the supervisory authority the results of the monitoring of the measures referred to in point (j) above is specified in *Article 16.1 of the BCRs*;
- m) the mechanisms for reporting, upon request, to the competent supervisory authority any legal requirements to which a member of the group of undertakings is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules are described in *Article 14.4 of the BCRs*;
- n) finally, provide for an appropriate data protection training to personnel having permanent or regular access to personal data (*Article 15 of the BCRs*).

7. The EDPB provided its **Opinion 1/2026** in accordance with Article 64(1)(f) of the GDPR.



Date

11 February 2026

Our reference

2023-225260

DECIDES AS FOLLOWING:

1. The Autoriteit Persoonsgegevens approves the Controller BCRs of **Heineken** as providing appropriate safeguards for the transfer of personal data in accordance with Article 46(1) and (2) (b) and Article 47(1) and (2) GDPR. For the avoidance of doubt, the Autoriteit Persoonsgegevens recalls that the approval of BCRs does not entail the approval of specific transfers of personal data to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not be construed as the approval of transfers to third countries included in the BCRs for which an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.
2. The approved BCRs will not require any specific authorization from the concerned SAs.
3. In accordance with Article 58(2)(j) GDPR, each concerned SA maintains the power to order the suspension of data flows to a recipient in a third country or to an international organization whenever the appropriate safeguards envisaged by the Controller BCRs of **Heineken** are not respected.
4. **Annex 1** forms an integral part of this decision and shall be considered a binding appendix thereto.
5. **Annex 2** contains the Controller BCRs which are approved by this decision, and forms an integral part of this decision.

The Hague, 11-02-2026

Yours sincerely,

Autoriteit Persoonsgegevens

Chair

**Date**

11 February 2026

Our reference

2023-225260

Legal remedy

If you do not agree with this decision, you can submit a notice of objection.² The notice of objection must be signed and dated, include the name and address of the (legal) person submitting it and should entail a description of the decision against which the objection is being lodged and the grounds on which it is based. The notice of objection must be received by the Autoriteit Persoonsgegevens within six weeks after this decision is taken. Please address the notice to the Autoriteit Persoonsgegevens and submit the notice via PO Box 93374, 2509 AJ The Hague, The Netherlands.³

It is also possible to submit a notice of objection via our web form on the website, see <https://www.autoriteitpersoonsgegevens.nl/over-de-autoriteit-persoonsgegevens/bezwaar-maken>.

Please note that submitting a notice of objection will not automatically suspend the effect of this decision.

² The Dutch General Administrative Law Act ("Algemene wet bestuursrecht") applies to this procedure.

³ Article 6:7 in conjunction with article 6:8 (1) of the Dutch General Administrative Law Act.



Date

11 February 2026

Our reference

2023-225260

ANNEX 1 TO THE DECISION

The Controller BCRs of **Heineken** that are hereby approved cover the following:

a. Scope.

Article 1.1 of the BCRs:

This Procedure applies to the Processing of Employee Data and CSB Data that have been subject of Restricted Transfers by HEINEKEN as Controller.

Annex 1: Definitions

RESTRICTED TRANSFER shall mean a Transfer to a Third Country.

THIRD COUNTRY shall mean a country outside the EEA to which Personal Data are transferred, where such Transfer is not covered by an Adequacy Decision.

b. EEA countries from which transfers are to be made:

Austria, Belgium, Bulgaria, Croatia, Czech Republic, France, Germany, Greece, Hungary, Ireland, Italy, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia and Spain.

c. Third countries to which transfers are to be made:

Algeria, Australia, Bahamas, Brazil, Burundi, Cambodia, Canada, China, Congo, Cote d'Ivoire, Ecuador, Egypt, Ethiopia, Haiti, India, Indonesia, Jamaica, Japan, Laos, Malaysia, Martinique, Mexico, Myanmar, Mozambique, Namibia, New Caledonia, New Zealand, Nigeria, Panama, Papua New Guinea, Peru, the Philippines, Reunion, Rwanda, Sierra Leone, Singapore, Solomon Islands, South Africa, South Korea, St. Lucia, Suriname, Taiwan, Timor-Leste, Tunisia, the United Kingdom, the United States of America, and Vietnam.

d. Purposes of the transfer:

The purposes are detailed in Annex 2 to the BCRs.

They include the following:

Employee data:

- *Human Resources and Managing Workforce: Managing work activities and personnel generally, including recruitment, appraisals, performance management, promotions and succession planning, rehiring, administering salary, and payment administration and reviews, wages and other awards such as stock appreciation rights and bonuses, wellness and healthcare, early retirement, pensions and savings plans, training, leave, managing sickness leave, promotions, transfers, secondments, honoring other contractual benefits, providing employment references, loans, performing Employee surveys, performing background checks, managing disciplinary matters, grievances and terminations, reviewing employment decisions, outplacement and employability, making business travel arrangements, managing business expenses and reimbursements, planning and monitoring of training requirements and career development activities and skills, and creating and maintaining one or more internal Employee directories.*



Date

11 February 2026

Our reference

2023-225260

- *Health, Safety and Security: Activities involving the protection of the interests and assets of Heineken and its Employees, including screening and monitoring of Employees before and during employment, the authentication of Employee access rights and identity, and performing due diligence research, ensuring business continuity and crisis management, providing references, protecting the health and safety of Employees and others, safeguarding and maintaining IT infrastructure, office equipment, facilities and other property, facilitating communication with Employees and their nominated contacts in an emergency.*
- *Business Operations: Operating and managing the IT, communications systems and facilities (including for facilitating communication with Employees), managing product and service development, improving products and services, managing company assets, allocating company assets and human resources, strategic planning, project management, business continuity, compilation of audit trails and other reporting tools, maintaining records relating to business activities, budgeting, financial management and reporting, communications, managing mergers, acquisitions, sales, re-organizations or disposals and integration with upon mergers or acquisitions.*
- *Compliance with law: Processing Employee Data as needed for compliance with laws that Heineken is subject to, including social security laws, disclosure of Employee Data to tax authorities and use of Employee Data for reporting under and to comply with laws and regulations in the field of Environmental, Social and Governance. Also Processing Employee Data for monitoring compliance with the the HEINEKEN Code of Business Conduct and other HEINEKEN internal policies, including HEINEKEN's procedures with regard to the use of company resources (telephone, email, Internet) es, and other monitoring activities as permitted by applicable law.*
- *Workforce Analytics: Analytics for succession planning, workforce management, and data security, such as analytics to ensure business continuity, to design Employee retention programs and diversity initiatives, to offer training opportunities and to identify patterns in the use of technology systems to information entrusted to HEINEKEN as well as to protect HEINEKEN's Employees and property.*

CSB data:

- *Business communication: Communicating with (prospective) Customers or Business Partners such as, answering questions or replying to communications.*
- *Assessment and acceptance of a Customer, Supplier or Business Partner: Customer, Business Partner or Supplier assessment and acceptance processes, such as, confirming and verifying identity (this may involve the use of a credit reference agency or other Third Party), due diligence, and screening against publicly available government and/or law enforcement agency sanctions lists and other third-party data sources.*
- *Concluding and executing agreements: Conclusion and execution of agreements, including administrative processes, such as, sending invoices, making payments, delivering or receiving services, including related customer services; required screening activities (e.g., for access to HEINEKEN's premises or systems and on compliance with the HEINEKEN Code of Business Conduct), the delivery of customer services, to record and financially settle delivered services, products and materials to and from HEINEKEN, and the settlement of payment transactions in the*



Date

11 February 2026

Our reference

2023-225260

context of which HEINEKEN may provide Personal Data to the counterparty or other parties as necessary, e.g., for verification or reconstruction purposes.

- *Monitoring and investigating compliance: Monitoring and/or investigating compliance with applicable laws, regulations, and/or HEINEKEN policy or conditions, anti-money laundering and anti-terrorism screening.*
- *Website and/or mobile app usage: Providing functionalities of websites and mobile apps, including administering user accounts, improving performance, saving preferences or products, enabling sharing functionalities.*
- *Compliance with law: Complying with obligations under applicable laws and regulations, such as, tax or business conduct related obligations.*
- *Protecting health, safety, security and ensuring integrity: Protection of the interests of HEINEKEN, its Employees, Customers, Suppliers and Business Partners and activities such as via access controls to HEINEKEN's systems and premises, sanctions checks against publicly available sanctions lists, protecting premises using CCTV cameras and other activities involving health and safety, the protection of HEINEKEN and Employee assets, and the authentication of Customer, Supplier or Business Partner status and access rights.*
- *Business process execution and internal management and management reporting: General management, order management, company assets management, including the IT systems and infrastructure; credit assessment (including setting credit limits) and risk management, conducting audits and investigations; reviewing and monitoring compliance with HEINEKEN Code of Business Conduct and other terms applicable to the relationship with Customers, Suppliers and Business Partners; finance and accounting; implementing business controls; provision of central processing facilities for efficiency purposes; managing mergers, acquisitions and divestitures; management reporting and analysis; archive and insurance purposes; legal or business consulting; preventing, preparing for or engaging in dispute resolution, conducting audits and investigations.*
- *Organizational analysis and development, management reporting, and acquisitions and divestitures: Aggregating or anonymizing Personal Data to prepare and perform management reporting and analysis, conducting Customer, Supplier and Business Partner surveys, processing Personal Data in the context of mergers, acquisitions and divestitures and in order to manage such transactions.*
- *Development and improvement of products and services: Development and improvement of HEINEKEN products and/or services and research and development. This includes assessing, analyzing and improving products and (Customer) services, using and combining Personal Data to analyze Customer behavior and to adjust our products and services accordingly, compiling analytics reports on the use of HEINEKEN websites or apps, assessing (online) campaigns and adjusting products and services accordingly, to ensure that it is relevant to Customers, including analyzing how often Customers read newsletters, how often they visit HEINEKEN websites or apps, which pages they click on what goods or services they purchase through HEINEKEN websites or apps.*
- *Relationship management and marketing: Maintaining and promoting contact with Customers, Suppliers and Business Partners, account management, customer service, recalls, collection of Personal Data through HEINEKEN websites, and the development, execution and analysis of*

**Date**

11 February 2026

Our reference

2023-225260

market surveys and marketing strategies. This includes sending newsletters, offers, or other relationship management or marketing communications, as well as promotions or invitations to events.

- *Administering events and promotions: Organizing and administering events, and measuring response to events and/or promotions.*

e. Categories of data subjects concerned by the transfer:

The categories of data subjects whose Personal Data are Processed under this Privacy Procedure are:

- *BUSINESS PARTNER shall mean any Third Party, other than a Customer or Supplier, that has or has had a business relationship or strategic alliance with HEINEKEN (e.g., joint marketing partner, joint venture or joint development partner).*
- *CSB DATA shall mean any Personal Data of any (employee of or any person working for) Customer, Supplier, Business Partner and/or any other Individual whose Personal Data HEINEKEN Processes in the context of the provision of its products or services.*
- *CUSTOMER shall mean any person, private organization, or government body that purchases, may purchase or has purchased a HEINEKEN product or service.*
- *DEPENDENT shall mean the spouse, partner or child belonging to the household of the Employee or emergency contact of the Employee.*
- *EMPLOYEE shall mean the following persons:*
 - *an employee, job applicant or former employee of HEINEKEN including temporary workers working under the direct supervision of HEINEKEN (e.g., independent contractors and trainees). This term does not include people working at HEINEKEN as consultants or employees of Third Parties providing services to HEINEKEN;*
 - *a (former) executive or non-executive director of HEINEKEN.*
- *INDIVIDUAL shall mean (as relevant): (i) an Employee; or (ii) any (employee of or any person working for) Customer, Supplier or Business Partner and any other individual whose Personal Data HEINEKEN Processes in the context of the provision of its products or services.*
- *STAFF shall mean all Employees and other persons who Process Personal Data as part of their respective duties or responsibilities using HEINEKEN information technology systems or working primarily from HEINEKEN premises.*
- *SUPPLIER shall mean any Third Party that provides goods or services to HEINEKEN (e.g., an agent, consultant or vendor).*
- *THIRD PARTY shall mean any person, private organization or government body outside HEINEKEN.*

Those categories are specified in Annex 1 to the BCRs.

f. Categories of personal data transferred:

Categories of personal data:



Date

11 February 2026

Our reference

2023-225260

- *Basic personal details: Name, employee identification number, organization, work or business contact details (email, phone numbers, physical or business address).*
- *Other personal Details: Home contact details (email, phone numbers, physical address), language(s) spoken, gender, date of birth, age, national identification number, social security number, marital/civil partnership status, domestic partners, dependents, emergency contact information, region, profession, login and passwords, internal identification number.*
- *Documentation required under immigration laws: Citizenship, passport data, details of residency, visa or work permit.*
- *Compensation and payroll: Base salary, bonus, benefits, compensation type, salary step within assigned grade, details on stock appreciation rights and other awards, currency, pay frequency, effective date of current compensation, salary reviews, banking details, working time records (including vacation and other absence records, leave status, hours worked and department standard hours), pay data and termination date.*
- *Position information: Description of current position, job title, corporate status, management category, job code, salary plan, pay grade or level, job function(s) and subfunction(s), company name and code (legal employer entity), branch/unit/department, location, employment status and type, full-time/part-time, terms of employment, employment contract, work history, hire/re-hire and termination date(s) and reason, length of service, retirement eligibility, promotions and disciplinary records, date of transfers, and reporting manager(s) information.*
- *Talent management information: Details contained in letters of application and resume/CV (previous employment background, education history, professional qualifications, language and other relevant skills, certification, certification expiration dates), details on performance management ratings, development programs planned and attended, e-learning programs, performance and development reviews, willingness to relocate, driver's license information, and information used to populate Employee biographies.*
- *Management records: Details on directorships and appointments, board minutes, board decisions.*
- *System and application access data: Information required to access HEINEKEN systems and applications such as user and system IDs for HEINEKEN network or servers, email account, instant messaging account, passwords, access logs, activity logs, and electronic content produced by Employees using HEINEKEN systems.*
- *Business communications: Information included in requests from, or correspondence with, a (prospective) Customer, Supplier or Business Partner and online interactions with HEINEKEN.*
- *Order information: Terms of contract, ordered or delivered products or services, order history, and other data generated during the performance of the agreement.*
- *Payment and transaction information: (Outstanding) invoices, bank account number or credit card number, wire transfer details, payment history, information about transactions, billing and shipping information.*
- *Analytics information: Information about the use of and interactions with HEINEKEN's websites, apps, newsletter, and online advertisements or other services, including, IP address, device information, click and surf behavior, session length, and responses to customer satisfaction surveys.*
- *Sanctions information: Information included on publicly available government and/or law enforcement sanctions lists.*



Date

11 February 2026

Our reference

2023-225260

- *Company information: Chamber of commerce details, VAT details, tax details, which may include Personal Data for independent contractors or other small businesses.*
- *Security information: Security, authentication, fraud prevention, and risk-management related data.*
- *Compliance information: Records related to Individuals' preferences (marketing preferences, consent documentation) and data subject rights requests.*
- *Racial or ethnic data: Photos (e.g. a copy of a passport containing a photo) and video images of an Individual which, in some countries, qualify as racial or ethnic data.*
- *Physical or mental health data: Any information or opinion of physical or mental health and data relating to disabilities, disability status, and absence due to illness or pregnancy.*
- *Criminal data: Information relating to criminal behavior, criminal records or proceedings regarding criminal or unlawful behavior.*
- *Sexual preference: Information on sexual preference.*
- *Religious or philosophical beliefs: Information related to dietary requirements or religious holidays.*

Those categories are specified in *Annex 2 to the BCRs*.



Date

11 February 2026

Our reference

2023-225260

ANNEX 2 TO THE DECISION

Copy of the Controller BCRs of **Heineken**.