THE PRIVACY POLICY (hereinafter – Policy) of **JSC "Eskom"**, Hotel **Mercure Palanga Vanagupe Resort** (hereinafter – the Hotel), company code 125996247, address Vanagupe str. 31, LT-00173 Palanga, Lithuania (hereinafter – the Data Controller), establishes the conditions for processing personal data when using the Data Controller's website www.mercurevanagupe.lt and Hotel services.

The conditions set out in this Policy apply each time a person visits the Hotel premises or the Website, regardless of the type of device used (computer, mobile phone, tablet, TV, etc.).

By using the Website and Hotel services, the Data Subject agrees to and does not object to the Data Controller collecting and processing their personal data (including data provided directly or indirectly when visiting the Website and using Hotel services) for the purposes and in accordance with the procedures outlined in this Policy and applicable legal acts.

1. KEY TERMS

- Personal Data – any information relating to a natural person whose identity is identified or can be directly or indirectly identified, by reference to identifiers such as name, surname, personal identification number, location data, internet identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
- Data Controller, Hotel – JSC "Eskom", Hotel Mercure Palanga Vanagupe Resort, company code 125996247, address: Vanagupe str. 31, LT-00173 Palanga, phone: +370 460 41199, email: HC108-FO@accor.com.
- Data Subject – a natural person who uses or expresses interest in the Hotel's services, visits the Website, applies for job openings announced by the Data Controller, or participates in contests/games organized by the Hotel.
- Website – the website operated by the Data Controller: www.mercurevanagupe.lt.
- Participant – a natural person participating or intending to participate in games, promotions, and/or contests organized by the Data Controller.
- Inquirer – a natural person interested in the services provided by the Data Controller or wishing to contact the Data Controller for other inquiries.
- Client – a person who has purchased goods or services from the Data Controller or has entered into an agreement with the Data Controller for the purchase of goods and/or the provision of services.
- Candidate – a person participating or intending to participate in a recruitment process carried out by the Data Controller.
- Data Processor – entities that process personal data controlled by the Data Controller based on the Data Controller's instructions and in accordance with service agreements.
- Minors – individuals under the age of 18. Minors may not provide any personal data without the consent of their parents or legal guardians. If parents/guardians become aware that a minor has provided personal data without their approval, they may contact the Data Controller via email at HC108-FO@accor.com, and all related data will be deleted.
- Regulation – Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (General Data Protection Regulation).
- This Privacy Policy is prepared in accordance with the Regulation, the Law on Legal Protection of Personal Data of the Republic of Lithuania, and other legal acts of the European Union and the Republic of Lithuania. The terms used in this Policy are understood as defined in the Regulation and the Law on Legal Protection of Personal Data of the Republic of Lithuania. The Policy may be updated or amended at any time.

2. PROCESSING OF PERSONAL DATA

The Data Controller ensures that, when adopting and implementing this Policy, it follows the fundamental principles:

- Personal data is processed lawfully, fairly, and transparently in relation to the Data Subject.
- Personal data is collected for specified, explicit, and legitimate purposes.
- Only the personal data necessary and appropriate for achieving the purposes for which they are processed is collected (principle of data minimization).
- Efforts are made to ensure that personal data is accurate and, if necessary, corrected, updated, or deleted within a reasonable period (principle of accuracy).
- Personal data is stored in a form that allows the identification of Data Subjects no longer than necessary for the purposes for which the personal data is processed.
- Further processing of personal data for archival purposes in the public interest or for statistical purposes is not considered incompatible with the original purposes (principle of purpose limitation).

- Personal data may be stored for longer periods if they are processed solely for archival purposes, in the public interest, or for statistical purposes, implementing appropriate technical and organizational measures necessary to protect the rights and freedoms of the Data Subject (principle of storage limitation).
- Personal data is processed in a manner that, by applying appropriate technical or organizational measures, ensures the security of personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage (principle of integrity and confidentiality).
- The Data Controller is responsible for compliance with the above principles and must be able to demonstrate such compliance (principle of accountability).

3. INFORMATION COLLECTED ABOUT DATA SUBJECTS

- Information directly provided by the Data Subject.
- Information on how the Website is used.
- When visiting the Website, information is collected that reveals the specifics of the services provided by the Data Controller or is automatically generated in visit statistics. More on this in the "Use of Cookies" section.
- Information from third-party sources.
- The Data Controller may obtain information about Data Subjects from public and commercial sources (as permitted by applicable laws) and link it with other information obtained from or about the Data Subject. Information about the Data Subject may also be obtained from third parties, such as social networks, through social media accounts.
- Other collected information.
- The Data Controller may also collect other information about the Data Subject, their device, or the use of Website content with the Data Subject's consent.
- The Data Subject may choose not to provide certain information, but in such cases, the use of the services offered by the Data Controller may be restricted.

4. PURPOSES OF PERSONAL DATA PROCESSING

4.1. PROCESSING OF PERSONAL DATA FOR CONSULTATION AND INQUIRY PURPOSES

- The Data Controller processes the following personal data of individuals contacting them for consultation, inquiries, or other matters: name, surname, phone number, and email address.
  If a representative of the Data Subject contacts the Data Controller, the following information about the representative is processed: name, surname, relationship with the Data Subject, phone number, and email address. Contact details are not shared with third parties.

4.2. PROCESSING OF PERSONAL DATA FOR ACCOMMODATION, SERVICE PROVISION, AND ACCOUNTING MANAGEMENT PURPOSES

- When booking the Data Controller’s services, the Data Subject consents to the processing of the following personal data: name, surname, date of birth, personal identification number, ID document details, address, phone number, email, workplace details, loyalty program participation, gender, age, payment type, bank card details (number and expiry date) if paying by card, amount due, number of nights, car number, accommodation details, and other information related to purchased services.
- The Data Subject confirms the accuracy of the provided data and updates them if necessary.
- Personal data collected for guest accounting is stored for ten (10) years from the reservation date. Data necessary for debt management is retained until the debt is recovered, but no longer than ten (10) years. When personal data is no longer needed for processing purposes or the retention period expires, they are securely deleted unless required by law to be retained.
- In accordance with the Lithuanian Tourism Law, the Data Controller submits specific personal data to the State Data Agency through the National Tourism Information System.
- The Data Controller does not disclose personal data to unrelated third parties except in cases where:

✓ The Data Subject consents to data disclosure.
✓ It is necessary to provide services through Data Controller’s partners.
✓ It is required to protect the Data Controller’s legitimate interests (e.g., debt collection).
✓ It is mandated by authorized institutions in accordance with the laws of the Republic of Lithuania.

- The Data Controller may transfer personal data to Data Processors who provide services and process personal data on behalf of the Data Controller, ensuring compliance with security and confidentiality measures.

4.3. PROCESSING OF PERSONAL DATA FOR DIRECT MARKETING PURPOSES

- The Data Controller shares relevant updates about services, special offers, contests, and other valuable information with newsletter subscribers, in compliance with this Privacy Policy.
- Personal data is processed for direct marketing only with the explicit consent of the Data Subject. The following personal data may be processed for marketing purposes: name, surname, loyalty program participation, phone number, and email address.

- The Data Controller may collect statistics on the Data Subject's interactions with newsletters (e.g., whether the email was read, which links were clicked).
- The Data Subject's email address may be used for advertising via social networks, Google, and other platforms, tailoring ads to the target audience.
- Personal data may be used for profiling to provide customized solutions and offers. The Data Subject may withdraw their consent to automated processing, including profiling, at any time.
- Personal data is processed until the Data Subject withdraws their consent or for five (5) years from the date of consent. Before this period ends, the Data Controller may seek renewed consent from the Data Subject.
- The Data Subject has the right to withdraw their consent for direct marketing at any time without providing reasons by emailing HC108-FO@accor.com or calling +370 460 41199.
- Upon receiving a request to delete personal data, the Data Controller ceases processing it for marketing purposes within two (2) business days and deletes it.
- If the Data Controller sends marketing offers to existing clients, they ensure that clients have a clear, free, and easily exercised option to opt-out of such communications.

4.4. PROCESSING OF PERSONAL DATA FOR JOB APPLICATION PURPOSES

- The Data Controller processes voluntarily provided personal data of candidates to the extent they were submitted.
- Personal data is obtained directly from candidates and/or third-party sources, such as online platforms, and is not shared with third parties.
- Candidates' data is processed based on their consent, expressed by submitting their data, and the intention to take action, with the Candidate's consent through conclusive actions and/or a request before concluding a contract (Regulation Article 6(1)(a) and (b)).

4.5. PROCESSING OF PERSONAL DATA FOR CONTESTS, PROMOTIONS, AND COMPETITIONS

- The Data Controller processes personal data for contest or promotion participation only with the Data Subject's consent. The following data may be collected: name, surname, photos, phone number, and email.
- Data is obtained directly from contest participants and is not shared with third parties but may be publicly displayed on the Data Controller's website or social media accounts.
- Personal data is processed based on consent, expressed by submitting personal data (Regulation Article 6(1)(a)).
- Based on legitimate interest (Regulation Article 6(1)(f)).

4.6. PROCESSING OF PERSONAL DATA FOR THE PURPOSES OF STAFF AND CLIENT SAFETY, PROPERTY PROTECTION, PREVENTION OF LEGAL VIOLATIONS, AND IDENTIFICATION OF OFFENDERS (VIDEO SURVEILLANCE)

- Individuals within the Data Controller's premises are captured within the video surveillance area (including hotel interior and exterior premises, the restaurant, outdoor terrace, and parking lot). The video cameras record images of individuals and vehicles, as well as the date, time, and location of the recordings.
- Video surveillance is conducted for the purposes of protecting individuals and property, preventing legal violations, identifying offenders, and investigating legal infractions. Video surveillance is not conducted in areas designated for private use, such as restrooms, showers, changing rooms, or hotel rooms.
- Video surveillance data is stored for two (2) weeks, after which it is automatically deleted.
- Video data may be transferred only to law enforcement authorities in accordance with the legal provisions of the Republic of Lithuania.
- Video surveillance data may also be provided to insurance companies in the event of an insured incident.
- Notice of video surveillance in specific areas is provided through clearly visible informational signs.
- Personal data collected through video surveillance is processed based on the Data Controller's legitimate interest (Regulation Article 6(1)(f)).

4.7. PROCESSING OF PERSONAL DATA FOR OTHER PURPOSES

The Data Controller may process the Data Subject's personal data for other purposes if the Data Subject has provided consent or if the processing is based on other legally established criteria for lawful data processing.

5. PERSONAL DATA STORAGE

- Personal data is protected from loss, unauthorized use, and modification through organizational and technical measures. The data controller takes appropriate steps to protect the information, but no website, online transaction, computer system, or wireless communication is completely secure.
- The data controller applies different retention periods for personal data, following legal requirements and considering the purposes of data processing.

- Personal data may be stored for a longer period than specified in this Policy when: there are reasonable suspicions of illegal activity under investigation; personal data is necessary for resolving disputes or complaints; for backup copies and other purposes related to the operation/maintenance of information systems; when personal data is used as evidence in civil, administrative, or criminal cases; or when other special legal grounds, conditions, or cases provided by laws arise.
- Once the retention periods have expired, unless extended, or when the grounds for storage are no longer valid, personal data is destroyed in such a way that it cannot be reconstructed.

Personal data retention periods:

Purpose of Personal Data Processing	Retention Period
Personal data of clients – for the provision of services	10 years from the day of using Hotel services.
Processing of candidates' personal data for recruitment purposes	4 months after the Candidate is hired. A longer retention of the Candidate's resume and other data requires the Candidate's consent. Data of candidates not hired will be destroyed within 4 months of receipt.
Processing of personal data of data subjects for video surveillance purposes	2 weeks
Processing of personal data of data subjects for organizing games, promotions, contests	1 year from the day the contest is completed
Processing of personal data of data subjects for direct marketing purposes	5 years from the day of consent unless the Data subject wishes to extend this period.

6. RIGHTS OF THE DATA SUBJECT

The data subject whose data is processed by the Data Controller has the following rights:

- The right to know (be informed) about the processing of their personal data (right to know).
- The right to access their data and understand how it is being processed (right of access); to exercise this right, the individual must provide an identity document to the Data Processor or contact through electronic communication tools that allow proper identification of the person. The personal data of the data subject will be provided free of charge once per calendar year. If personal data, video footage, or other data is provided for the second time in a year, the data subject will be informed about the applicable fees (for example, for the receipt of data on a CD, DVD, or other media containing the video footage, document preparation, etc.), as well as the procedure for payment.
- The right to request the correction or, depending on the purpose of personal data processing, completion of incomplete personal data (right to rectification).
- The right to request the deletion or suspension of personal data processing (excluding storage) (right to erasure and the right to be forgotten); this provision does not apply when data retention is mandatory under the law.
- The right to request that the data controller restrict the processing of personal data under one of the legitimate grounds (right to restriction).
- The right to file a complaint with the State Data Protection Inspectorate of the Republic of Lithuania or to the Data Controller via email at HC108-FO@accor.com.
- The right to withdraw any given consent for processing their personal data (if the personal data is processed based on consent).
- The right to object to the processing of their personal data for direct marketing purposes. The data subject may submit a request in writing to the Data Controller via email at HC108-FO@accor.com, informing them that their personal data should no longer be processed for direct marketing purposes, without specifying the reasons for the objection.
- The right to submit any request or instruction related to the processing of personal data to the Data Controller in writing in one of the following ways: in person, by mail to Vanagupe g. 31, LT-00173 Palanga, or by email at HC108-FO@accor.com. The Data Controller will respond to the request or instruction within one month from the date of the request and will either take the action requested or refuse to do so. If necessary, this period may be extended by an additional two months, depending on the complexity and number of requests. In this case, the Data Controller will inform the data subject of the extension within one month of receiving the request, along with the reasons for the delay.
- The Data Controller may refuse to allow data subjects to exercise the above rights, except for the objection to direct marketing, in cases where, under the law, it is necessary to ensure the prevention, investigation, or detection of crimes, breaches of professional or ethical conduct, or to protect the rights and freedoms of the Data Subject, the Data Controller, or other individuals.

7. THIRD-PARTY WEBSITES, SERVICES, AND PRODUCTS ON THE DATA CONTROLLER'S WEBSITE

The Data Controller's website may contain third-party advertising panels, links to their websites and services, which the Data Controller does not control, such as a link to the Data Controller's Facebook or Instagram profile. The Data Controller is not responsible for the security and privacy of information collected by third parties. The data subject should read the privacy policies applicable to third-party websites and services they use. If the data subject submits their data via Facebook or Instagram, the Data Controller understands that the data subject agrees that the provided contact phone number and email address can be used to contact them and send service offers.

8. USE OF COOKIES

When visiting the Data Controller's website, the aim is to provide content and features that are tailored to the needs of the visitor. For this, cookies are needed – small pieces of information automatically created while browsing the website and stored on the visitor's computer or other device. They help the Data Controller recognize the visitor as a previous website visitor, save browsing history, and adapt the content accordingly. Cookies also help ensure smooth website operation, monitor the duration and frequency of website visits, and collect statistical information about the number of website visitors.

How to manage and delete cookies. When using a browser to access content, you can configure your browser to accept all cookies, reject all cookies, or notify you when a cookie is sent. Each browser is different, so information on how to change cookie settings can be found in the browser's help menu. The operating system of a specific device may also have additional cookie controls. If you do not want information to be collected via cookies, you can use a simple procedure available in most browsers that allows you to reject the use of cookies. To learn more about how to manage cookies, you can visit http://www.allaboutcookies.org/manage-cookies/. Please note that in some cases, deleting cookies may slow down your browsing speed, limit the functionality of certain website features, or block access to the website.

The Data Controller uses various types of cookies and similar technologies on the website, each of which has a specific function:

Cookie Name	Description	Created On	Expiration Time
_ga, _gid	Tracking cookies from Google Analytics. The cookie collects information about user behavior on the website and is used to store statistical information.	Upon first page entry.	2 years, 24 hours
_gat	Google Analytics cookie used to regulate the query speed.	Upon page entry.	1 minute
random-cookie	WordPress system cookie.	Upon first page entry.	Until the session ends
__atuvc	Social sharing statistics from Addthis.com.	Upon page entry.	1 year
__atuvs	Social sharing statistics from Addthis.com.	Upon page entry.	1 year
_fbp	Facebook advertising statistics.	Upon page entry.	3 months
_ecl	Used to determine if the cookie notice has been displayed.	Upon page entry.	1 year
pll_language	Used to store the user's selected language.	Upon first page entry.	1 year
vngPrAd	Manages running banner ads.	Upon first page entry.	1 day

9. FINAL PROVISIONS

- The legal relationships related to this Policy are governed by the laws of the Republic of Lithuania.
- The Data Controller is not responsible for any damage, including damage caused by disruptions in the use of the Website, data loss or corruption resulting from the actions or inactions of the individual or third parties acting with the individual's knowledge, errors, deliberate harm, or any other improper use of the Website.
- Any amendments or changes to the Privacy Policy will take effect from the day they are published on the Website.
- If, after the amendment or change to the Policy, the Data Subject continues to use the Website and/or the services provided by the Data Controller, it is considered that the Data Subject does not object to such amendments and/or changes.
- For issues related to personal data processing, please contact via email at HC108-FO@accor.com.
- The Privacy Policy is effective from 07.12.2021.