

ADESE GAYRİMENKUL YATIRIM A.Ş.
OUMU BEACH HOUSE

PRIVACY AND PAYMENT SECURITY POLICY

ARTICLE 1: DATA PRIVACY COMMITMENT

Oumu Beach House, operating under ADESE GAYRİMENKUL YATIRIM A.Ş., adopts and implements all requisite technical and administrative (organizational) measures prescribed by the applicable legislation and in conformity with prevailing industry standards under its statutory duty of care, for the express purpose of safeguarding the confidentiality of personal and financial information disclosed by users via the website <https://oumubeachhouse.com/>.

Personal data pertaining to our customers shall under no circumstances be shared with, sold to, or permitted to be exploited for commercial purposes by any third party, save for statutory obligations set forth under the Law on the Protection of Personal Data No. 6698 (the "LPPD") and relevant legislation, circumstances necessary for the performance of a contract, and express customer authorizations / explicit consents.

ARTICLE 2: CREDIT CARD AND VIRTUAL POS PAYMENT SECURITY AND LIMITATION OF LIABILITY

2.1. Encryption Technology:

All data traffic pertaining to reservation payments processed via our website is secured and encrypted via industry-standard secure communication protocols (Secure Sockets Layer - SSL). From the precise moment credit card credentials are input, your data is transmitted in an encrypted format directly to the integrated technical systems of the relevant acquiring bank or licensed payment institution.

2.2. Direct Banking Integration:

Critical payment data pertaining to the Customer's credit card, debit card, and similar payment instruments—including PIN/passwords, CVV security codes, and primary account numbers (PAN)—shall under no circumstances be retained, held, or recorded within the servers, databases, or hotel data filing systems of <https://oumubeachhouse.com/>. All processes concerning information entry, authentication, and collection of payment take place entirely and directly between the Customer's web browser and the virtual POS interface of the relevant bank or licensed payment institution. In this context, the Operator bears no contractual, civil, or criminal liability whatsoever for any data breaches, cyberattacks, unauthorized intrusions, or systemic security vulnerabilities that may arise from banks, payment intermediaries, or the Customer's own terminal device or browser.

The Customer is under a strict personal obligation to maintain up-to-date antivirus/anti-malware software on their own device (computer, smartphone, etc.) and to preserve credential confidentiality. In the event that payment card credentials are duplicated or compromised through malicious software (such as keyloggers, Trojans, etc.) infiltrating the Customer's personal device, no liability shall be assumed by the Operator, given the absolute absence of any systemic fault or breach attributable to the Operator.

2.3. Mandatory 3D Secure Authentication Requirement:

The use of the 3D Secure (encrypted verification protocol) system is mandatory for all transactions executed via our website. Upon entering your card details and proceeding to the final checkout stage, you will be automatically redirected to your card-issuing bank's secure verification interface; the collection of payment will not be finalized unless you enter the one-time passcode (OTP) dispatched to your mobile

telephone via SMS or through your bank's mobile banking application. The unauthorized utilization of your card by third parties is thereby prevented. In the event of unauthorized transactions executed by third parties who have illicitly obtained the Customer's password, mobile device, or card credentials, all legal liability, claims, and causes of action shall be resolved exclusively between the relevant bank and the Customer, unless the fault of the Operator is conclusively established.

ARTICLE 3: SYSTEM SECURITY AND FORCE MAJEURE

The Operator implements state-of-the-art firewall architectures, logging systems, and cyber defense software within its sphere of control to protect its website servers against cyberattacks, unauthorized access, and data breaches. Nevertheless, notwithstanding the Operator's full implementation of all requisite cybersecurity measures; pursuant to the doctrine of the interruption of the causal nexus (break in the chain of causation) and the governing provisions on force majeure (specifically Articles 112, 115, and 136 of the Turkish Code of Obligations No. 6098), the Operator bears no contractual, civil, criminal, or strict liability for any damages or losses arising out of widespread cyberattacks compromising global or national telecommunications infrastructure, global zero-day vulnerabilities in third-party upstream servers, hardware-related force majeure events, or unforeseeable cyber incidents, save for instances of gross negligence (ağır kusur) or willful misconduct attributable to the Operator.