The Presidio Trust

Privacy Act of 1974; System of Records

AGENCY: The Presidio Trust.

ACTION: Notice of a new System of Records.

SUMMARY: Pursuant to the provisions of the Privacy Act of 1974, as amended, the Presidio Trust is issuing a public notice of its intent to establish a Parking Payment Compliance Program, system of records. INTERIOR PRESIDIO TRUST/Department of Planning and Compliance-XX, Passport Inc. Enforcement Software Solution.

DATES: This system of records is effective upon publication. New routine uses will be effective [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*].

ADDRESSES: You may send comments via email to the interim Privacy Officer, within Presidio Trust's Department of Administration, Luke Donohue, LDonohue@presidiotrust.gov. or via U.S. Mail 1750 Lincoln Blvd. San Francisco, CA, 94129.

FOR FURTHER INFORMATION CONTACT: Luke Donohue, interim Privacy Officer, Presidio Trust, 1750 Lincoln Blvd. San Francisco, CA, 94129, LDonohue@presidiotrust.gov.

SUPPLEMENTARY INFORMATION: The purpose of the Presidio Trust's Parking Payment Compliance Program is to encourage voluntary compliance with the parking payment regulations. Information collected includes a database of violations issued, appeals submitted, and records of correspondence. The system contains records which include first name, last name, cell phone number, email address, license plate number or VIN number, vehicle make/model, date/time of violation issuance, and photos taken of the vehicle by enforcement staff member when issuing the citation. Credit card information is separately held by the system but not shared with the Presidio Trust or its contractors. All information is collected and stored on the Passport Inc. Enforcement software.

The parking enforcement contractor utilizes the Passport Inc. Enforcement software when issuing violations in the field. The contractor enters the relevant fields, such as vehicle make and model, into the Passport system using a handheld device. Once the required information has been inputted, a notice of violation is printed and posted to the vehicle and a record of the violation is stored on the Passport system. The recipient of a violation is provided with instructions to pay their violation fee online. When the violation recipient pays their fee online, the Passport system collects their name and email address. If the recipient of a violation has not paid their violation fee within 10 days, a delinquent letter is sent to the vehicle's registered owner. The registered owner's mailing address is accessed from the California DMV database. If the recipient choses to appeal their violation, the recipient will provide their contact information, including their home address and phone number.

This information is retained for two-years, after which it is purged. As per Passport's Privacy Policy, California residents have the right to request, at no charge, deletion of their personal information that Passport has collected about them and to have such personal information deleted, except where an exemption applies.

System Name and Number: Parking Payment Compliance Program, Presidio Trust/Internal-2.

Security Classification: Unclassified.

System Location: Department of Planning & Compliance, 1750 Lincoln Blvd, San Francisco CA 94129. transportation@presidiotrust.gov.

System Manager(s): Department of Planning & Compliance, 1750 Lincoln Blvd, San Francisco CA 94129. transportation@presidiotrust.gov.

Authority for Maintenance of the System: Title I, Omnibus Parks Public Lands Act of 1996, Public Law 104-333 (https://www.govinfo.gov/link/plaw/104/public/333), 110 Stat. 4097.

Purpose(s) of the System: The primary purpose of the system is to encourage voluntary compliance with parking payment regulations by issuing notices and fees to non-compliant users.

Categories of Individuals Covered by the System: Records of violation are stored by license plate number. Vehicles that have been identified as not complying with the parking payment regulations and receive a violation are covered by this system. This includes Presidio Park Visitors, Presidio Trust Staff, and Presidio Park Residents and Commercial Tenants.

Categories of Records in the System: The system contains records of violations issued, which include first name, last name, cell phone number, email address, license plate number, vehicle make/model, date/time of violation issuance, and photos taken of the vehicle by enforcement staff member when issuing the citation. A record of appeals submitted is maintained and include written and photographic evidence submitted by the user. Records of correspondence are maintained and include delinquent notices sent to the registered owner and emails communicating the result of an appeal.
Mailed letters of correspondence include the register owner's mailing address. Credit card information is separately held by the system but not shared with the Presidio Trust or its contractors.

Record Source Categories: Records maintained by Passport are obtained from multiple sources. This includes records inputted by the enforcement staff member, mailing addresses from the California DMV database, and information provided by the recipient. These records are retained for two years unless otherwise requested by the individual. Paid violations and closed appeals may be deleted at the request of individual, open violations cannot be deleted at the request of the individual.

Routine Uses Of Records Maintained in The System, Including Categories of Users and Purposes of Such Uses: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside the Department of Interior as a routine use pursuant to 5 U.S.C. 552a(b)(3) may be made to:
(1) The appropriate Federal, State, local or foreign agency responsible for obtaining information relevant for investigating, prosecuting, enforcing, or implementing a statue, rule, regulation, or order when Presidio Trust becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation.
(2) The U.S. Department of Justice or in a proceeding before a court or adjudicative body when:

(a) The United States, the Presidio Trust, a component of the Presidio Trust, or, when represented by the government, an employee of the Presidio Trust is a party to litigation or anticipated litigation or has an interest in such litigation, and

(b) The Presidio Trust determines that the disclosure is relevant and necessary to the litigation and is compatible with the purpose for which the records were compiled.

(3) To a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual.
(4) To appropriate agencies, entities, and persons when:

(a) The Presidio Trust suspects or has confirmed that there has been a breach of the system of records

(b) The Presidio Trust has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, The Presidio Trust (including its information systems, programs, and operations), the Federal Government, or national security.

(c) The disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with The Presidio Trusts efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

(5) To another Federal agency or Federal entity, when the Presidio Trust determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in:

(a) Responding to a suspected or confirmed breach.

(b) Preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national or national security, resulting from a suspected or confirmed breach.

(6) To Contractors when the contractor is working on a contract, service, job, or other activity for the Agency and who have a need to have access to the information in performance of their duties or activities for the Agency. Recipients will be required to comply with the requirements of the Privacy Act of 1974 as provided in 5 U.S.C. 552a(m).

Policies and Practices for Storage of Records: These records are stored online within the Passport backend management system, Operator Management or "OpsMan". All functions and features are password protected. The physical security of the Passport Inc. data center is managed by Amazon AWS data centers and physical access to the Passport office is restricted using employee ID badges.

Passport has a completely separate cardholder data environment that is subject to PCI compliance were all credit card data is processed and stored. Credit card numbers are encrypted with AES-256 with a rotating encryption key. All information is stored in an isolated card storage database per best practices. Passport completes assessments every year to ensure the effectiveness of its controls. This includes SOC 1 Type 2, SOC 2 Type 2, and a PCI DSS.

Policies and Practices for Retrieval of Records: The Passport records system may only be accessed by the Presidio Trust's Transportation and the parking enforcement. Each individual staff member receives a unique account. The login requires a multi-factor authentication.

The Passport system keeps an audit trail of all actions within. This records the action performed, date, and user. The system will also record reports run, searches performed (With search parameters) from a CSR perspective as well. Passport gives the Presidio Trust full discretion as to how to manage its system and can limit access by the individual user or their role within the Presidio Trust's administration.

Policies and Practices for Retention and Disposal of Records: Violation and appeal records are kept for two years or until requested by the individual. Records are purged from the Passport system and no records are stored outside the Passport system, either electronically or printed.

Administrative, Technical, and Physical Safeguards: Passport's cybersecurity program aligns with the NIST Cybersecurity Framework, and Passport is SOC 2 compliant and PCI DSS Level 1 merchant and service provider certified. Passport's defensive line is monitored 24/7, 365 days a year by trained professionals. Passport complies with all applicable laws and regulations concerning privacy and data protection including the California Consumer Privacy Act (CCPA) and the EU General Data Protection Regulation (GDPR). Passport utilizes intrusion detection systems, virtual private network (VPN), and public key infrastructure (PKI) certificates.

Record Access Procedures: An individual requesting access to their records should send a written inquiry to the applicable System Manager or the Privacy Act Officer identified above. A Privacy Act request must meet the requirements of 36 CFR 1008 (https://www.ecfr.gov/current/title-36/chapter- X/part-1008). The request must include a general description of the records sought and the requester's full name, current address, and sufficient identifying information such as date of birth or other information required for verification of the requestor's identity. The request must be signed and dated and be either notarized or submitted under penalty of perjury in accordance with 28 U.S.C. 1746.

Requests submitted by mail must be clearly marked "PRIVACY ACT REQUEST FOR ACCESS" on both the envelope and letter. A request to access records must meet the requirements of 36 CFR 1008 and 36 CFR 1008.13 (https://www.ecfr.gov/current/title-36/section-1008.13)-.14, .16-.17.

Contesting Record Procedures: An individual requesting amendment of their records should send a written request to the applicable System Manager or the Privacy Act Officer as identified above. DOI instructions for submitting a request for amendment of records are available on the DOI Privacy Act Requests website at https://www.doi.gov/privacy/privacy-act-requests. The request must clearly identify the records for which amendment is being sought, the reasons for requesting the amendment, and the proposed amendment to the record. The request must include the requester's full name, current address, and sufficient identifying information such as date of birth or other information required for verification of the requestor's identity. The request must be signed and dated and be either notarized or submitted under penalty of perjury in accordance with 28 U.S.C. 1746. Requests submitted by mail must be clearly marked "PRIVACY ACT REQUEST FOR AMENDMENT" on both the envelope and letter. A request to contest or amend records must meet the requirements of 36 CFR 1008 and 36 CFR 1008.18 (https://www.ecfr.gov/current/title-36/section-1008.18)-.19, .22, .24.

Notification Procedures: An individual requesting notification of the existence of records about them should send a written inquiry to the applicable System Manager as or the Privacy Act Officer identified above. A Privacy Act request must meet the requirements of 36 CFR 1008 (https://www.ecfr.gov/current/title-36/chapter-X/part-1008). The request must include a general description of the records and the requester's full name, current address, and sufficient identifying information such as date of birth or other information required for verification of the requestor'sidentity. The request must be signed and dated and be either notarized or submitted under penalty of perjury in accordance with 28 U.S.C. 1746. Requests submitted by mail must be clearly marked "PRIVACY ACT INQUIRY" on both the envelope and letter.

Exemptions Promulgated for the System: None.

HISTORY: None.

Luke Donohue,
Director of Administration.

[FR Doc. 2024-04006 Filed: 2/26/2024 8:45 am; Publication Date: 2/27/2024]