

**Privacy Policy for the Parking System for**

Master of Science

Information Technology

Bria Wright

University of Denver University College

April 16, 2025

Faculty: Nathan Braun MBA, BBA

Dean: Michael J. McGuire, MLS

Table of Contents

**Privacy Policy for the University Parking System ..... 3**

INTERNAL PRIVACY POLICY ..... 3

*The Parking System Application ..... 3*

*Data Collected ..... 4*

EXTERNAL PRIVACY POLICY ..... 5

*Information We Collect ..... 5*

*Why We Collect This Information ..... 6*

*Your Options and Controls ..... 6*

*Accessing and Updating Your Information ..... 7*

CONTACT US ..... 8

REFERENCES ..... 9

## **Privacy Policy for the University Parking System**

Effective Date: March 31, 2025

Last Updated: April 15, 2025

At the University of Denver, we are dedicated to safeguarding the privacy of all users of our Parking System Application. This Privacy Policy explains how we collect, use, store, and protect data through our internal procedures and user-facing terms. The policy ensures transparency, accountability, and security for all stakeholders who engage with the system. It includes both an internal policy for staff, developers, and administrators and an external policy for end-users such as students, faculty, staff, and visitors.

We are committed to protecting your personal information in accordance with the Colorado Privacy Act (CPA). By using the University Parking System, you agree to the terms outlined in this Privacy Policy.

### **INTERNAL PRIVACY POLICY**

This Section is intended for internal staff and developers in the University of Denver who work with the Parking System Application. It outlines the data handling processes, responsible access, and privacy implications of the information managed through the application.

#### *The Parking System Application*

The Parking System Application is a digital platform designed to manage university parking operations. It supports customer registration, vehicle registration, permit issuance, entry/exit scanning, and calculation of parking charges. The system facilitates operations considerations such as discounts for compact vehicles. The application supports both web and mobile platforms and integrates biometric verification for enhanced security.

### *Data Collected*

The Parking System Application collects the following categories of data:

- **Customer Data:** Name, address, email, phone number, and unique customer ID.
- **Vehicle Data:** License plate number, car type (e.g., compact, SUV), and a unique vehicle ID.
- **Permit Data:** Permit ID, permit type (single-car or multi-care), expiration date.
- **Parking Transactions:** Entry and exit times, lot location, fees, and timestamps.
- **Payment Information:** Total charges, payment status (paid/unpaid), and applicable discounts
- **Mobile Device Information:** Device type, Operating System, crash logs, app usage, and geolocation (user decides once or always and is able to change)
- **Biometric Data:** (if enabled): Fingerprint or facial recognition data used solely for authentication purposes on supported mobile devices.

Biometric data is never stored on our servers. Authentication occurs locally on the user's device, utilizing device-level security features (e.g., Apple Face ID, Android Biometrics API).

### *Privacy Implications*

The data collected may be considered personally identifiable information (PII) under relevant privacy laws, particularly the customer's name, contact information, and vehicle registration details. In some cases, the system may indirectly track user movement (via parking timestamps), which raises location privacy considerations.

No sensitive health data or financial payment instruments (e.g., credit card details or sensitive health information) are collected or stored by the Parking System Application. All

transactions are conducted through approved third-party systems or manually processed by university staff.

#### *Access Controls*

Access to data within the Application is role-based:

- **System Administrators** have full access to all data and system configurations for maintenance and auditing purposes.
- **Parking Office Staff** can view customer, vehicle, permit, and transaction data for processing registration, issuing permits, and managing disputes.
- **Developers and IT Support** may access anonymized or test data for development, debugging, and system improvement tasks.
- **No staff or system component** has access to biometric templates, as they remain confined to users' mobile devices.

Access is granted by role-based permissions, and all staff are trained in data protection best practices. Multi-factor authentication (MFA) is enforced across all administrator interfaces.

#### EXTERNAL PRIVACY POLICY

This Section of the policy is designed for users of the Parking System Application, including students, faculty, staff, and guests who register for parking services.

#### *Information We Collect*

We may collect the following data when you use our Parking System Application:

- **Personal Details:** Your name, address, phone number, email, student/faculty ID
- **Vehicle Data:** Your car's license plate number, make/model, and type and ID
- **Parking Transactions:** Location, duration, entry/exit times, and parking fees

- **Permit Details:** Permit ID, type, and expiration date
- **Mobile Device Data (if using the mobile app):**
  - Device type and operating system
  - Crash logs and usage statistics
  - Geolocation (only during active sessions)
- **Biometric Verification Data (if opted in):**
  - Fingerprint or face recognition to log in, this verification is handled by your device. We do not receive or store your biometric information.

#### *Why We Collect This Information*

We collect and use this information based on the Colorado Privacy Act (CPA):

- **Right to Access:** View what personal data we have collected about you.
- **Right to Correction:** Update or correct inaccurate information tied to your account.
- **Right to Deletion:** Request that we delete your personal data, subject to retention laws.
- **Right to Data Portability:** Receive a copy of your personal data in a usable format.
- **Right to Opt-Out:** You can opt out of the processing of personal or sensitive data (e.g., geolocation, biometrics).

We do not sell or share your information with marketers or third-party advertisers. We will respond within 45 days, as required by the CPA.

#### *Your Options and Controls*

You have full control over your data:

- **Biometric Login:** Completely optional. You can enable/disable it anytime in your phone's security settings.

- **Mobile Location Access:** You can revoke location permissions in your device settings.  
Note that this may limit app functionality during entry/exit scanning.
- **Edit Your Profile:** You can request corrections to your name, vehicle, or contact details by contacting the Parking Office.
- **Account Deletion:** You may cancel your account and request the removal of your personal information, subject to university data retention policies.

#### *Accessing and Updating Your Information*

You may:

- View your current permits and associated vehicles.
- Review your parking history and charges.
- Modify your contact details or vehicle records.
- Enable or disable biometric login options.

These actions can be done through the mobile or web interface. For full data removal requests, contact the Parking Office directly.

#### *Data Security*

We work following FERPA and local laws. We protect your data through multiple layers of security:

- **Encryption:** All communication is encrypted in transit and at rest
- **Access Controls:** Role-based permissions and MFA are used internally
- **Local Biometric Security:** Your fingerprint or face ID never leaves your device
- **Geolocation Limits:** Location data is used temporarily and discarded after your parking session ends

- **Regular Audits:** We conduct internal checks to ensure privacy compliance

*In Case of a Data Breach*

If your data is compromised:

- We will notify affected users within 30 days as required under Colorado Revised Statute § 6-1-716.
- We will also report the breach to the Colorado Attorney General, if applicable.
- We will investigate and remedy the breach immediately
- Support will be available to assist you in recovering access or updating compromised information

For biometric data, since it is never stored by the Parking System Application, there is no risk of compromise from our systems.

CONTACT US

If you have questions or concerns about this policy or your data:

- Parking Office
  - Department Address: University of Denver, 2199 S. University Blvd, Colorado, 80208
  - Email: Steven.Veloff@du.edu
  - Phone: 303-871-2706
  - Permits & Enforcement: T2 Systems, Inc



## REFERENCES

“Blocked.” 2024. Privacyengine.io. September 9, 2024.

<https://www.privacyengine.io/blog/colorado-privacy-act/>.

CDC. 2024. “Family Educational Rights and Privacy Act (FERPA).” Public Health Law. May 13,

2024. <https://www.cdc.gov/phlp/php/resources/family-educational-rights-and-privacy-act-ferpa.html>.

Darke, Sean F., Phillip Short, Clay Cosse, Dante Stella, Jake Parker, and Colby Williams. 2023. “A

Reference Guide to State Laws on Biometric Information and Related Legislative Trends

Guide to U.S. Biometric Privacy Laws.” [https://www.irisid.com/wp-](https://www.irisid.com/wp-content/uploads/2023/11/SIA-Guide-US-Biometric-Privacy-Laws-web-FINAL-c.pdf)

[content/uploads/2023/11/SIA-Guide-US-Biometric-Privacy-Laws-web-FINAL-c.pdf](https://www.irisid.com/wp-content/uploads/2023/11/SIA-Guide-US-Biometric-Privacy-Laws-web-FINAL-c.pdf).

Frankenfield, Jake. 2023. “How Personally Identifiable Information (PII) Works.” Investopedia.

November 2, 2023. <https://www.investopedia.com/terms/p/personally-identifiable-information-pii.asp>.

Kosinski, Matthew. 2024. “Multi-Factor Authentication.” Ibm.com. January 4, 2024.

<https://www.ibm.com/think/topics/multi-factor-authentication>.

Kunz, Immanuel . 2024. “Privacy by Design: Integrating Privacy into the Software Development

Life Cycle – Cybersecurity-Blog.” Fraunhofer.de. June 4, 2024.

<https://www.cybersecurity.blog.aisec.fraunhofer.de/en/privacy-by-design-integrating-privacy-into-the-software-development-life-cycle/>.

“Parking & Mobility Services | University of Denver.” 2025. University of Denver. 2025.

<https://www.du.edu/parking>.

“University Parking Solutions - T2 Systems.” 2025. T2 Systems. March 6, 2025.

<https://www.t2systems.com/higher-education/>.

Wu, Stephen. n.d. “Six-Step Process of Implementing an Effective Security and Privacy Program

- Artificial Intelligence and Robotics Law - Silicon Valley Law Group.” Artificial

Intelligence and Robotics Law. [https://www.airoboticslaw.com/blog/six-step-process-](https://www.airoboticslaw.com/blog/six-step-process-implementing-security-privacy-program)

[implementing-security-privacy-program](https://www.airoboticslaw.com/blog/six-step-process-implementing-security-privacy-program).