PRIVACY POLICY FOR COLLECTION, MANAGEMENT, AND STORAGE OF PERSONAL INFORMATION

SAN DIEGO ASSOCIATION OF GOVERNMENTS

sandag.org/privacy

In compliance with the Americans with Disabilities Act of 1990 (ADA), this document is available in alternate formats by contacting the SANDAG ADA Coordinator, the Director of Diversity & Equity, at (619) 699-1900 or (619) 699-1904 (TTY).

Este documento está disponible en español en sandag.org/privacy

PRIVACY POLICY FOR COLLECTION, MANAGEMENT, AND STORAGE OF PERSONAL INFORMATION

SAN DIEGO ASSOCIATION OF GOVERNMENTS

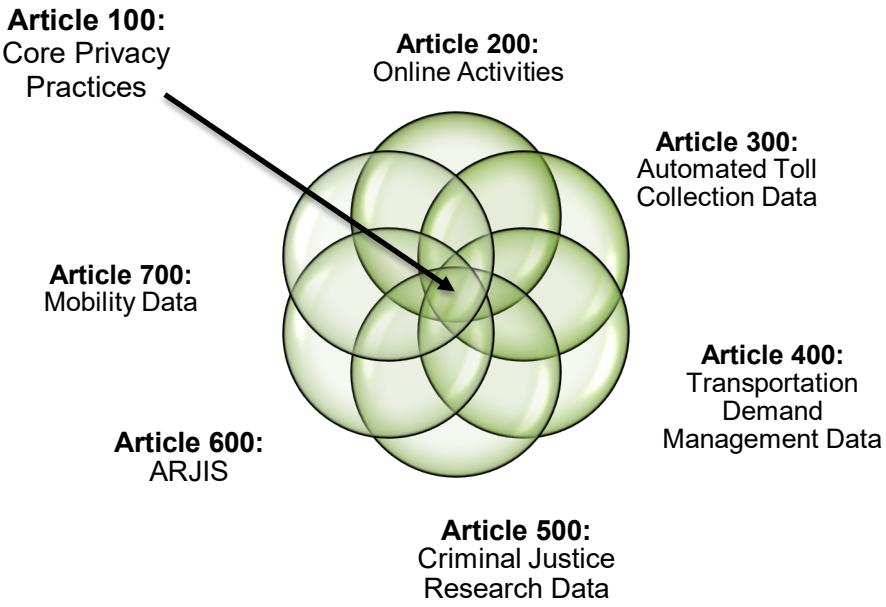
Key Points:

- We, the San Diego Association of Governments (SANDAG), collect data from your use of our online services and other programs.
- If you use our online services and programs, we may use your Personally Identifiable Information ("PII") to better administer these programs and services.
- This Privacy Policy describes the information we collect from you as part of your use of our online services and other programs and how that information will be used. This policy is detailed because we believe you should know as much as possible about our practices so that you can make informed decisions.
- The privacy of your PII is a serious matter; safeguarding and protection of PII is a high priority for SANDAG.
- We use best practices to safeguard your PII and make every effort to safeguard your information.
- This Privacy Policy is effective as of July 1, 2018. If we update this Privacy Policy, we will post the updates on our website.
- This Privacy Policy constitutes the entire agreement between you and SANDAG with respect to the collection, use, storage, and disclosure by SANDAG of Personally Identifiable and Aggregate Information obtained from the SANDAG online services or from participation in any other SANDAG programs.

If you have additional questions, you may email pio@sandag.org or call (619) 699-1900.

101. ORGANIZATION OF THE POLICY

SANDAG administers programs and services that require it to collect, use, and maintain the PII of members of the public. This document sets forth how we use your PII so that you can make informed decisions about participating in SANDAG programs and services. Article 100 sets forth the Core Privacy Practices that apply across all of SANDAG; Articles 200 through 700 contain more detailed practices that apply to particular types of data. This organization allows readers to easily locate practices that impact them based upon the services they utilize.



102. CONSTRUCTION IN THE EVENT OF A CONFLICT BETWEEN ARTICLES

Where provisions in Article 100 and any other Article might govern the same type of data, the later Article shall control.

103. AUTHORITIES

California Public Utilities Code §§ 132350.1(d); 132354(l), 132354(o); and 132360.3. Automated Regional Justice Information System (ARJIS) Joint Powers Agreement.

104. INFORMATION WE COLLECT, GENERALLY

SANDAG collects information to administer its programs and services. You provide some of this data directly such as when you create an account with SANDAG for access to a SANDAG program, when you submit a public records request[1], or when you contact us for support. We collect some data when you interact with our programs or services, such as our website or through social media. We also may obtain information about you from other government agencies or third-party partners, such as Google or Uber. SANDAG only collects information through lawful means. If you do not provide some necessary information, you may not be able to participate in certain programs or services. We only collect PII when we believe it is relevant and necessary to fulfill the SANDAG mission. The information we collect depends on the programs or services you use, and may include:

Contact information such as name, postal address, email address, and phone number; Demographic data such as date of birth and gender; Information about participation in our programs (e.g., location and travel pattern data); Account history with SANDAG; Account access information including user ID, password, responses to security questions, and security PIN; and Social Security number.

105. AUTOMATICALLY COLLECTED DATA

When you visit online services hosted by SANDAG, some information may be automatically collected, such as:

(a) The internet domain and Internet Protocol (IP) address from which you access our online services;

(b) The type of browser and operating system used to access our online services; and

(c) "Clickstream Data", which may include the date and time you access our online services; the pages you visit; and whether you linked to our online services from another website, including the address of that website.

These data, by themselves, do not collect or retain your name or other PII and are treated as Aggregate Information. SANDAG uses Aggregate Information to analyze and improve the effectiveness of our website, services, and programs. From time to time, we may undertake or commission statistical and other summary analyses of the general behavior and characteristics of customers participating in any of our services and programs and the characteristics of visitors to our site and may share Aggregate Information with third parties. Aggregate Information provided to third parties will not allow anyone to identify you or determine anything personal about you.

106. PERSONAL ACCOUNTS CREATED TO PARTICIPATE IN SANDAG PROGRAMS AND SERVICES

To access certain programs and services provided by SANDAG, individuals may be required to set up a personal account and provide PII. This information provided will only be used for the purpose intended and personal accounts may be closed at any time. Participation is voluntary.

[1] For more information on submitting public records requests under the California Public Records Act, please see SANDAG Board Policy No. 015, Records Management, and the SANDAG Public Records Request Guidelines.

107. SURVEYS

From time to time, SANDAG may conduct surveys. These may be conducted in person and then transcribed into a database or completed online. The collection of information through surveys is done for several reasons that include, but are not limited to, performance monitoring, federal reporting requirements, and marketing or planning SANDAG or other regional transportation services.

108. HOW WE USE THE INFORMATION WE COLLECT

SANDAG may use your PII to:

(a) Contact you about services you request;

(b) Contact you for marketing and/or public information purposes (you may opt out of marketing communications);

(c) Provide, bill, and collect for services you use;

(d) Respond to your questions and comments;

(e) Contact you in the event of a policy violation;

(f) Track and analyze travel patterns;

(g) Complete internal administrative, financial, and accounting functions;

(h) Administer your participation in surveys and research projects;

(i) Measure interest in services and programs;

(j) Evaluate, improve, or market SANDAG services;

(k) Identify or mitigate conflicts of interest;

(l) Comply with legal and regulatory requirements; and

(m) Verify your identity.

109. ROLE-BASED ACCESS CONTROLS

We implement role-based access controls to regulate access to PII based on the roles of individual users within SANDAG. Roles are defined according to job duties, authority, and responsibility, and SANDAG strives to limit access to PII to the minimum amount necessary to perform that role's function.

110. LIMITATIONS ON DISCLOSURES OF PERSONALLY IDENTIFIABLE INFORMATION

SANDAG only uses your PII when it is relevant and helps to fulfill the SANDAG mission. Unless otherwise expressly stated herein, we do not disclose your PII to third parties except as provided by Sections 111 through 115.

111. DISCLOSURES MADE WITH YOUR CONSENT

SANDAG may disseminate your PII when you provide written consent to do so.

112. DISCLOSURES PERMITTED BY LAW

SANDAG may disseminate PII about you without your consent when permitted by law or regulations and under the following circumstances:

(a) To refer accounts for collection;

(b) With an existing contract or agreement to protect shared PII with other transportation agencies or vendors working on behalf of SANDAG;

(c) To investigate unauthorized access to SANDAG computer systems or data;

(d) If SANDAG determines there are compelling circumstances regarding an individual's health or safety and the disclosure is not otherwise prohibited by law;

(e) To a law enforcement agency or regulator for investigatory or regulatory purposes;

(f) Anonymized Smartphone Media Access Control address; and

(g) Smartphone location.

113. DISCLOSURES REQUIRED BY LAW

SANDAG will disseminate PII about you: (a) when required by law; (b) pursuant to judicial process (such as a search warrant or administrative subpoena); or (c) when it receives a demand from a district attorney.

Certain information held by SANDAG may be subject to state public records laws. Dissemination of such information is governed by applicable California statutory provisions. Any dissemination of such information will be conducted in conformance with such laws.

We reserve the right to impose reasonable charges for responding to access requests under the California Public Records Act. Fees for copies of records which are disclosed shall be assessed in accordance with the federal and state laws as well as with SANDAG Board Policy No. 015, Records Management.

In any case, we will seek to limit the scope of the disclosure and restrict such disclosures only to appropriate authorities and will disclose only such PII as is reasonably required to fulfill the purpose of the disclosure.

114. FRAUD DETECTION

We may utilize your PII in the performance of financial and accounting functions, including account settlement and enforcement, as well as disclosure of such information in good faith to appropriate authorities supporting such enforcement. To allow us to detect fraud and system errors, we may compare personal media use information to our own data.

115. NO PUBLIC DISCLOSURE OF SOCIAL SECURITY NUMBERS

Unless otherwise required by Section 113, SANDAG will not:

(a) publicly disclose Social Security numbers (SSNs);

(b) print an individual's SSN on any materials mailed to the individual; and

(c) sell or offer to sell any individual's SSN.

116. SHARING OF SCRUBBED DATA

Nothing in this policy limits the ability of SANDAG to use or maintain data that does not include or has been scrubbed of individually identifiable data elements.

117. RECORDS RETENTION

SANDAG retains records pursuant to a Records Retention Schedule maintained in accordance with the California Secretary of State Local Government Records Management Guidelines and Board Policy No. 015.

118. DESTRUCTION OF RECORDS AT END OF RETENTION PERIOD

Records containing PII are disposed of in a manner that does not disclose their content. Under the discretion of SANDAG and to the extent practicable, if an individual has requested to review their own records, records containing that person's PII will not be removed or destroyed before giving them an opportunity to access them.

119. PRIVACY PRACTICES AND POLICY AWARENESS

All employees are provided copies of SANDAG privacy and security policies and its Employee Handbook, which states that violating SANDAG policies regarding the appropriate use of PII and confidential information may result in disciplinary action up to termination.

120. AUDIT LOGS

The SANDAG data systems log events to provide better response to mitigate against negative influences such as cyber threats, security breaches, data corruption, or misuse of information.

121. SENIOR MANAGERS ARE RESPONSIBLE FOR THEIR DEPARTMENT'S DATA SYSTEMS

The responsibility for operating data systems is assigned to the head of each department or division that needs the information to perform its roles and responsibilities. As required by California Government Code § 6270.5, the SANDAG Catalog of Enterprise Systems sets forth which department or division is responsible for each system. These senior managers can advise individuals about what rights they may have to access records containing their PII and can be reached by contacting the main SANDAG office.

122. SAFEGUARDS, GENERALLY

We have put into place security systems designed to prevent unauthorized disclosure of PII that we collect or maintain and to deter and prevent would-be attackers and others from accessing this information.

We use standard security measures to minimize the threat that your PII will be lost, misused, altered, or unintentionally destroyed. We also use software programs to monitor network traffic in an effort to identify unauthorized attempts to upload or change information or otherwise cause damage.

These safeguards should not be construed in any way; however, as giving business, legal, or other advice, or warranting as fail-proof, the security of information provided by or submitted to SANDAG sites and information submitted through customer participation in our services, programs, or our website services. Because our sites do not encrypt incoming email, you should not send email containing information that you consider highly sensitive through SANDAG websites.

To protect information against unauthorized access and loss, SANDAG:

(a) Analyzes and manages potential data security risks;

(b) Monitors data system and network activity;

(c) Deploys and maintains firewalls and intrusion detection systems;

(d) Identifies which employees and vendors need to access PII to perform their duties;

(e) Limits employees' and vendors' access to PII to the minimum amount necessary to perform their duties including through the use of role-based access controls;

(f) Implements procedures for granting, supervising, and terminating employees' and vendors' access to PII;

(g) Disseminates privacy and security policies and trains employees and vendors about how to safeguard PII;

(h) Sets standards for creating, changing, and safeguarding passwords including changing default passwords and requiring unique passwords;

(i) Requires Multi-factor Authentication;

(j) Includes provisions in contracts with third parties to ensure they appropriately safeguard PII;

(k) Limits physical access to electronic data systems;

(l) Requires staff to use data security features on equipment used for SANDAG purposes;

(m) Requires research records containing PII or confidential information to be marked and stored in locked cabinets or offices;

(n) Documents security repairs and modifications;

(o) Implements procedures governing the receipt and removal of servers containing PII into and out of its facilities;

(p) Uses appropriate methods to dispose of PII and the media on which it is stored;

(q) Automatically terminates electronic sessions after a predetermined time of inactivity;

(r) Limits invalid log-in attempts;

(s) Uses appropriate encryption systems to protect sensitive information from being accessed or viewed by unauthorized users;

(t) Builds audit controls into information systems that record user activity; and

(u) Protects PII from improper alteration or destruction.

Due to the nature of the internet communications and evolving technologies, we cannot provide, and disclaim, assurance that the information you provide to us will remain free from loss, misuse, or alteration by third parties who, despite our efforts, obtain unauthorized access.

SANDAG shall have no liability in tort, contract, or otherwise if unauthorized third parties unlawfully intercept or access transmissions or private communications to trace your PII or an external user illegally acquires your PII from the website.

123. RESPONDING TO SECURITY BREACHES

SANDAG will investigate incidents involving loss, theft, damage, misuse, or improper dissemination of information in accordance with its Incident Response Plan. SANDAG may disclose PII to individuals assisting with this investigation.

124. NOTIFICATION OF SECURITY BREACHES

If we detect an intrusion or other unauthorized access to or use of PII, we will act in accordance with California Civil Code 1798.29.

125. CHANGES TO BE POSTED

Any changes to this Policy will be posted on the SANDAG website.

126. CHOICES YOU CAN MAKE WITH REGARD TO YOUR DATA

For you to use certain SANDAG online services, or to participate in other programs, you may have to provide an email address. Should you want SANDAG to send you bulletins, updates, or other communications, you may need to grant us permission. You have the ability to decline to receive such information at any time. If you provide us with your email address, we may send you notifications, including information concerning your online services account or participation in other programs.

SANDAG will use your email address to send you the type of information for which you provided your email address. You also may "opt in" and affirmatively agree to receive additional email notifications from time to time or "unsubscribe" to stop email notifications. You may not, however, decline to receive important notices concerning the operation of our online services and other offline programs (such as updates to our Privacy Policy), or legal notices concerning your relationship to those services and programs. We will not distribute your email address or any contact information to any unrelated third party unless you expressly consent for us to do so, or it is required by law.

If you send us an email or letter with questions or comments, or if you provide your contact information when ordering goods or services from SANDAG, we may use your email address and other PII included in your correspondence in order to respond to you. If other users or third parties send us correspondence about your activities or postings on our online services or participation in other SANDAG programs, we may collect such information into a file specific to you. Upon the receipt of your written request, SANDAG will remove your name and address from its mailing list unless the information is used exclusively by SANDAG to contact you directly.

Article 200
Online Activities

201. SCOPE OF THIS ARTICLE

This article sets forth the SANDAG privacy practices surrounding its collection, use, and maintenance of information gathered from administering its websites or from communicating on a social networking website.

202. HOW WE COLLECT PERSONALLY IDENTIFIABLE INFORMATION FROM ONLINE ACTIVITIES

(a) SANDAG may collect PII about you when you:

1. Register on a website administered by SANDAG;
2. Subscribe to our newsletter;
3. Comment on one of our social media webpages;
4. Participate in a media campaign or sweepstakes; or
5. Send an email to SANDAG.

(b) Other users or third parties may send us correspondence about your activities or postings on our online services or participation in SANDAG programs. If this occurs, we may collect that information into a file specific to you.

(c) SANDAG does not use social media websites to maintain or disseminate the PII of any individual.

203. SOCIAL SECURITY NUMBERS

SANDAG does not collect SSNs over the internet.

204. IP ADDRESSES

SANDAG may collect and maintain IP addresses of visitors and users of SANDAG websites.

205. THIRD-PARTY LINKS ON SANDAG WEBSITES

SANDAG online services may contain links to other sites ("Linked Sites"). Linked Sites are not under SANDAG control and SANDAG is not responsible for their content or privacy practices. The inclusion of a link does not imply endorsement by SANDAG of the site or any association with its operators.

206. HOW WE USE THE INFORMATION WE COLLECT FROM ONLINE ACTIVITIES

In addition to the uses set forth in Section 108, we may use your PII to:

(a) Provide services to you and develop new services;

(b) Perform statistical, demographic, and marketing analyses;

(c) Determine how users interact with our services or assess the success of a campaign or event;

(d) Email you our newsletter[2];

(e) Notify you of the results of a contest or other promotion; and

(f) Investigate fraud or a violation of our Terms of Use.

207. DELETION

SANDAG will delete electronically collected PII that you have previously submitted while participating in SANDAG programs if you request it, it is feasible, and doing so is consistent with SANDAG records retention policies and procedures and does not impair the ability of SANDAG to provide, bill, and collect for services you use.

208. BACKUP DATA

Backups shall be performed regularly to ensure SANDAG is able to recover data and business processes in a timely manner in the event of an incident or disaster, and backups are retained off-site for disaster recovery purposes.

209. ACCESSING YOUR PERSONALLY IDENTIFIABLE INFORMATION

(a) You can request to review, change, update, or delete PII that you previously submitted while participating in SANDAG online programs. SANDAG will take reasonable steps to verify your identity before granting access to your PII.

(b) Individuals that registered for online accounts can access and update certain PII about them by logging into their accounts.

---

[2] Subscribers can opt out of SANDAG newsletters at any time by clicking the "Unsubscribe" link that is present at the bottom of each newsletter.

210. CALIFORNIA DO-NOT-TRACK DISCLOSURES

SANDAG does not automatically collect PII over time and across third-party websites or online services. Moreover, a website visitor must provide informed consent by reading instructions and filling out a form to provide PII on the SANDAG websites. Accordingly, “do not track” mechanisms to prevent automatic collection of PII do not apply to SANDAG websites.

211. OUR USE OF COOKIES

Cookies by themselves do not collect or retain your name or other PII. SANDAG uses cookies to:

(a) Assist us in providing our services to you;

(b) Allow you to navigate through online services without having to repeatedly re-enter your password;

(c) Track and analyze activity through our online services; and

(d) Introduce services to you on our websites.

212. YOU CAN CHOOSE WHETHER TO ACCEPT COOKIES

Internet browsers typically allow you to decide whether to accept cookies, reject cookies, or to have your browser notify you each time a cookie is offered. You also can delete cookies from your hard drive. If your browser does not accept cookies from our online services, some features of our online services may be impaired.

213. NO THIRD-PARTY USE OF OUR COOKIES

Third parties cannot use the cookies SANDAG utilizes on its online services.

Article 300
Automated Toll Collection Data

301. SCOPE OF THIS ARTICLE

This Article sets forth the SANDAG privacy practices surrounding its collection, use, and maintenance of information gathered by its operation of automated toll collection equipment.

302. DATA WE COLLECT BY OPERATING TOLL ROADS

SANDAG may collect the following information from individuals who use the toll roads it operates:

(a) License plate information, including plate type, number, and state;

(b) Vehicle information, including make, model, year, and color;

(c) Travel pattern data, including where and when transponders enter and exit tolled lanes, per-mile rate, number of miles, and trip charge; and

(d) Payment information, including credit card or bank account number, credit card type, expiration date, name on card, billing address, and security number.

303. HOW WE USE THE INFORMATION WE COLLECT FROM OPERATING TOLL ROADS

SANDAG may use the PII collected through the operations of its toll roads to:

(a) Further account settlement or enforcement activities;

(b) Market toll-related products or services to nonsubscribers in toll evasion notices;

(c) Comply with interoperability specifications and standards; and

(d) Locate a driver when that driver fails to pay a toll.

304. LIMITATIONS ON USING THE DATA TO MARKET SERVICES

SANDAG will not use a nonsubscriber's FasTrak® PII to market products or services to that nonsubscriber.

305. DISCLOSURES OF TOLL DATA AUTHORIZED BY LAW

Absent a search warrant, SANDAG may provide PII to a peace officer only when the officer is conducting a criminal or traffic collision investigation and certifies in writing to SANDAG that he has good cause to believe that the delay in getting the search warrant would result in:

(a) Danger to an individual's physical safety;

(b) A flight from prosecution;

(c) A loss of evidence;

(d) The intimidation of potential witnesses;

(e) Serious jeopardy to an investigation; or

(f) Undue delay of a trial.

306. RETENTION OF FASTRAK ACCOUNT INFORMATION

SANDAG deletes FasTrak subscribers':

(a) Basic Account Information (e.g., name, credit card number, billing address, and vehicle information) within four and 1/2 years of the date the account is terminated with no amounts due to SANDAG; and

(b) Non-Basic Account Information (e.g., tolls assessed and paid, travel pattern data) four and 1/2 years after the bill related to the information has been paid and all toll violations have been resolved.

307. DELETION

SANDAG will delete electronically collected PII that you have previously submitted while participating in SANDAG programs if you request it, it is feasible, and doing so is consistent with SANDAG records retention policies and procedures and does not impair the ability of SANDAG to provide, bill, and collect for services you use or used.

308. BACKUP DATA

Backups shall be performed regularly to ensure SANDAG is able to recover data and business processes in a timely manner in the event of an incident or disaster, and backups are retained off-site for disaster recovery purposes.

309. ACCESSING YOUR PERSONALLY IDENTIFIABLE INFORMATION

(a) You can request to review, change, update, or delete PII that you previously submitted while participating in SANDAG toll programs. SANDAG will take reasonable steps to verify your identity before granting access to your PII.

(b) Individuals who registered for online FasTrak accounts can access and update certain PII about them by logging into their accounts.

Article 400
Transportation Demand Management (TDM) Data

401. SCOPE OF THIS ARTICLE

This article sets forth the SANDAG privacy practices surrounding its collection, use, and maintenance of PII collected from your use of TDM Programs. TDM programs include the SANDAG iCommute Program and related surveys.

402. TRANSPORTATION DEMAND MANAGEMENT INFORMATION WE COLLECT

SANDAG may collect your:

(a) Contact information, such as email address and phone number;

(b) Start and destination addresses;

(c) Employer;

(d) Work schedule;

(e) Usual mode and cost of transportation; and

(f) Travel Preferences, such as preferred mode of travel or time of travel.

403. HOW WE USE THE TRANSPORTATION DEMAND MANAGEMENT INFORMATION WE COLLECT

SANDAG may use PII about you to:

(a) Match you with other people traveling in the same direction should you request assistance;

(b) Match you with access to resources, such as secure bicycle parking, to aid you in your journey to and from work; and

(c) Help stranded commuters to get home in cases of emergency.

404. RETENTION OF TRANSPORTATION DEMAND MANAGEMENT RECORDS

We maintain TDM records for up to ten years.

405. DELETION

SANDAG will delete electronically collected PII that you have previously submitted while participating in SANDAG TDM programs if you request it, it is feasible, and doing so is consistent with SANDAG records retention policies and procedures and does not impair the ability of SANDAG to provide, bill, and collect for services you use.

406. BACKUP DATA

Backups shall be performed regularly to ensure SANDAG is able to recover data and business processes in a timely manner in the event of an incident or disaster, and backups are retained off-site for disaster recovery purposes.

407. ACCESSING YOUR PERSONALLY IDENTIFIABLE INFORMATION

You can request to review, change, update, or delete PII that you previously submitted while participating in SANDAG TDM programs. SANDAG will take reasonable steps to verify your identity before granting access to your PII.

Article 500
Criminal Justice Research Data

501. SCOPE OF THIS ARTICLE

This article sets forth SANDAG privacy practices surrounding its collection, use, and maintenance of PII by the SANDAG Criminal Justice Research Division ("Division") and is intended to protect the privacy and confidentiality of research subjects.

502. CRIMINAL JUSTICE RESEARCH DATA WE COLLECT

SANDAG collects a broad range of PII depending upon the social issue being studied, including, but not limited to, the data types listed below. Please note that when SANDAG collects individual-level information, no one involved in the research study is participating without their knowledge or consent.

(a) FBI Uniform Crime Reporting Data;

(b) California Law Enforcement Telecommunications System (CLETS);

(c) Sexual Orientation;

(d) Marital Status;

(e) Family Information;

(f) Citizenship;

(g) Police Reports;

(h) Criminal Offender Record Information (CORI);

(i) Employment Status and History;

(j) Health Information;

(k) Education Records;

(l) Veteran Status;

(m) Census Bureau Data; and

(n) Ethnic Origin/Race.

503. HOW WE USE CRIMINAL JUSTICE RESEARCH DATA

SANDAG may use your information to:

(a) Analyze crime trends and jurisdictional crime patterns;

(b) Review responses to crime in the region;

(c) Examine crime reduction and prevention strategies; and

(d) Assess the effectiveness and efficiency of crime-control programs.

504. ARREST INFORMATION

SANDAG will not disclose to any unauthorized person CORI pertaining to an arrest, detention, or proceeding not resulting in a conviction.

505. INSTITUTIONAL REVIEW BOARD PROTECTION

(a) The Criminal Justice Research Division ("Division") utilizes Institutional Review Board protections for research involving human subjects and complies with U.S. Department of Justice confidentiality requirements to help ensure that data subjects' PII is not inappropriately used or disseminated.

(b) The Division uses several methods to keep data confidential, such as name-stripping, substituting codes for participant identifiers, storing data in locked cabinets, and encrypting electronic data.

(c) The Division has discretion to select which privacy methods it will use based upon the nature of the information collected and potential risks to participants from a breach of confidentiality.

(d) The Division requires data subjects to complete an informed consent form when it collects data directly from individuals. The consent form discusses the nature of the research being conducted and states that the individual is not required to participate and can stop participating at any time.

506. DISSEMINATION OF CRIMINAL JUSTICE RESEARCH DATA

(a) The Division disseminates project findings to the public; those findings do not contain PII of any data subjects.

(b) The Division does not transfer data in identifiable form outside of SANDAG.

507. RETENTION OF CRIMINAL JUSTICE RESEARCH RECORDS

The Division data subjects' PII is destroyed per the Records Retention Schedule.

508. BACKUP DATA

Backups shall be performed regularly to ensure SANDAG is able to recover data and business processes in a timely manner in the event of an incident or disaster, and backups are retained off-site for disaster recovery purposes.

509. SECURITY

Criminal justice information collected by the Division is maintained on SANDAG servers and is protected by the same security safeguards set forth at Section 122. The Division supplements those safeguards by:

(a) Requiring that staff pass background checks, complete the CORI/CLETS training, and agree in writing to comply with confidentiality requirements before accessing criminal justice data;

(b) Taking disciplinary action against personnel who inappropriately access criminal justice data;

(c) Maintaining its own written security procedures;

(d) Providing a copy of its security procedures to research staff;

(e) Requiring electronic files containing PII to be saved on secure servers or in “Restricted Data” folders in an encrypted format;

(f) Requiring electronic media and hard copies of documents containing PII to be kept in a locked file cabinet in the Division’s lab when not being used;

(g) Requiring staff to lock or log out of their computers before leaving them unattended;

(h) Deleting PII saved temporarily on computer hard drives;

(i) Requiring staff to coordinate with a project manager before copying data;

(j) Prohibiting staff from leaving PII unattended;

(k) Prohibiting staff from taking PII home; and

(l) Prohibiting staff from discussing the contents of files containing confidential information with anyone other than research staff.

Article 600
ARJIS

601. AUTOMATED LICENSE PLATE READER DATA

The ARJIS Acceptable Use Policy for the Regional License Plate Reader System is adopted as Section 601 of this Policy.

602. FACIAL RECOGNITION DATA

The ARJIS Acceptable Use Policy for Facial Recognition is adopted as Section 602 of this Policy.

Article 700
Mobility Data

701. SCOPE OF THIS ARTICLE

This Article sets forth SANDAG privacy practices surrounding its collection, use, and maintenance of mobility data collected by the SANDAG Mobility Data Clearinghouse (MDC).

702. MOBILITY DATA WE COLLECT

SANDAG collects information from the operators of micromobility fleet vehicles in the San Diego region for the purposes stated herein. Such information includes, but may not be limited to:

(a) Trip start and end times (including overall trip duration);

(b) Trip route information (including a series of latitude and longitude points collected at regular intervals by micromobility vehicles and overall trip distance);

(c) Universally unique identifier (UUID) of the micromobility vehicle used in a particular trip (including operator information); and

(d) Status and location of parked vehicles.

Mobility data stored in the MDC is not independently personally identifying. Nevertheless, due to the remote risk that the data could be linked to individual riders (re-identified) if combined with other datasets, SANDAG treats raw mobility data as PII for purposes of determining the level of protection to be afforded to such data. Neither SANDAG nor authorized MDC users (see Section 703) are permitted to re-identify or attempt to re-identify mobility data contained in the MDC.

Mobility data is collected primarily through implementation of the Mobility Data Specification (MDS), an open source set of Application Programming Interfaces (APIs) focused on dockless e-scooters, bicycles, mopeds, and carshare. The data is generated by micromobility vehicles through Global Positioning System (GPS) and Global Navigation Satellite System (GNSS) sensors attached to the vehicles by micromobility fleet operators and transmitted to SANDAG via MDS. SANDAG does not collect mobility data directly from individual riders or their personal devices.

703. DISSEMINATION OF MOBILITY DATA

Authorized MDC users have role-based access to the raw mobility data stored within the MDC and are bound by data processing terms and acceptable use policies in connection with such access. SANDAG does not disseminate raw mobility data beyond authorized users unless required by law, such as in response to a search warrant.

Datasets derived from raw mobility data (e.g., by further aggregating the raw mobility data or combining it with other SANDAG geographic information system (GIS) data) are treated as Aggregate Information. Aggregate Information may be shared with third parties. Aggregate Information provided to third parties will not allow anyone to identify you or determine anything personal about you.

704. HOW MOBILITY DATA IS USED

SANDAG and authorized MDC users may use mobility data to:

(a) Analyze trends regarding use of micromobility vehicles;

(b) Inform micromobility policy decisions;

(c) Regulate micromobility operations;

(d) Support capital improvements;

(e) Assess and update the regional travel demand model; and

(f) Identify opportunities for improving the transportation system.

705. SECURITY

Mobility data stored in the MDC is protected by the same security safeguards set forth at Section 122.

706. BACKUP DATA

Backups shall be performed regularly to ensure SANDAG is able to recover data and business processes in a timely manner in the event of an incident or disaster, and backups are retained off-site for disaster recovery purposes.

707. RETENTION OF MOBILITY DATA

Raw mobility data is destroyed per the Records Retention Schedule. Aggregate Information derived from raw mobility data may be retained indefinitely for the purposes described herein.

708. ACCESS AND DELETION

Because mobility data is not collected or stored in a manner that is linked to or allows SANDAG to associate it with a particular individual, individuals cannot request to review, change, update, or delete mobility data specific to them. Please note that mobility data is not used to make individualized decisions nor is raw mobility data generally available to the public.

Article 800
Other Provisions

801. DISCLAIMER NOTICE

SANDAG makes no claims, promises, or guarantees about the accuracy, currency, completeness, or adequacy of the contents of SANDAG online services and expressly disclaims liability for errors and omissions in its contents. In the event of a conflict between this Privacy Policy and the Public Records Act or other law governing the maintenance or disclosure of records, the Public Records Act or other applicable law will control. No warranty of any kind, implied, express, or statutory, including, but not limited to, the warranties of non-infringement of third-party rights, title, merchantability, fitness for a particular purpose, and freedom from computer virus, is given with respect to SANDAG online services or its links to other internet resources. Although we have put in place security systems (as described in this Policy) that are designed to prevent unauthorized disclosure of your PII, due to the nature of internet technologies we cannot provide firm assurances as to the security of this information, and expressly disclaim any such obligation.

802. INDEMNIFICATION

You agree to indemnify and hold SANDAG, its officials, officers, employees, sponsors, partners, and agents harmless from any claims, actions, costs (including legal costs), or losses by any third party due to or arising out of your use of or conduct in relation to these online services.

803. SEVERABILITY

The SANDAG online services are controlled and overseen by SANDAG from its location in San Diego, California. This Policy shall be construed in accordance with the laws of the State of California, without regard to any conflict of law provisions. Any dispute arising under this Policy shall be resolved exclusively by the state or federal courts sitting in San Diego, California.

804. CONTACT US

We welcome your feedback, questions concerns, or suggestions regarding our Privacy Policy. You may contact us in the following ways:

- Telephone

  1-15 Express Lanes: (888) 889-1515
  South Bay Expressway (SR 125): (619) 661-7070
  iCommute: Call 511 and say “iCommute”
  General SANDAG: (619) 699-1900

- Email

  SANDAG: webmaster@sandag.org
  iCommute: iCommute@sandag.org
  I-15 Express Lanes: customerservice@sandag.org
  South Bay Expressway (SR 125 Toll Road): customerservice@sadag.org
  511: 511sd.com/sd511/ContactUs.aspx

- Mail

  San Diego Association of Governments
  Office of General Counsel
  401 B Street, Suite 800
  San Diego, CA 92101

Definitions

Aggregate Information is information that does not identify you and may include statistical information concerning use of SANDAG programs and services or the pages on our site that users visit most frequently.

Basic Account Information refers to FasTrak accounts and includes the subscriber's name, credit or debit card number, billing address, and vehicle information.

Clickstream Data is information concerning the sequence of mouse clicks made by a website user, the pages viewed by users, the amount of time users spend on a certain page, and other similar information. Clickstream Data can be thought of as a "trail" that users make while navigating through a website or other online services.

Cookies are text files that websites use to: (a) recognize repeat visitors; (b) facilitate a visitor's use of the site; and (c) compile aggregate data to improve the site.

Data Subject means the individual identified by the Personally Identifiable Information at issue.

Disclosure or **Dissemination** is the release, transfer, provision of access to, or disclosure in any other manner of PII outside the entity holding the information.

FasTrak means the automated toll-collection system used throughout California and locally administered by SANDAG.

Internet Protocol (IP) Address is an address associated with your computer's connection to the internet.

Need to Know means that the intended recipient of the data needs to access the information to effectively perform his or her duties and responsibilities to SANDAG.

Network Administrator is a person authorized by an employer or organization to manage programs or benefits administered by SANDAG for the benefit of employees who voluntarily participate in Transportation Demand Management programs.

Non-Basic Account Information refers to FasTrak accounts and includes the tolls assessed and paid and travel pattern data associated with a subscriber's transponder or license plate number.

Online Services include our websites, mobile applications, personal accounts hosted on a SANDAG website or mobile application, and other internet-based services.

Personally Identifiable Information (PII) is any information about an individual maintained by an agency, including: (a) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records; and (b) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Social Media Website is a website or application that allows users to create and share content or to participate in social networking. Examples include Facebook, Twitter, YouTube, Instagram, and LinkedIn.

Users are visitors who register their identity with a website through the website registration process or through a Facebook or Open ID interface.

Unrelated Third Parties means anyone who is not involved in providing SANDAG services, running a SANDAG affiliated website, or fulfilling requests you make concerning such websites or SANDAG systems.

Visitors are users who visit a website but do not register or provide PII to the website.

We, **Us**, and **Our** mean SANDAG and its programs, projects, and services.

You and **Your** refer to any person: (a) who accesses this site; (b) who participates in a website services program; or (c) whose PII is provided to SANDAG.

Revised August 2022