



Privacy and Security Policy

Siskin Enterprises, Inc, PermaPlate Company LLC and PermaPlate Film, LLC (“PermaPlate,” “we” or “us,”) has created the following Privacy and Security Policy (“Privacy Policy”) to inform you about your limited consumer personal private information (“PPI”) of the following:

- * what type of limited PPI we collect;
- * when we collect it;
- * how and why we collect it,
- * how we use it;
- * how we protect it,
- * how and when we share it;
- * what choices you have regarding our collection and use of this limited PPI; and
- * compliance with other laws e.g., Canada and California.

Besides the retail purchase of our products thru an authorized dealer and agent, this Privacy and Security Policy applies to these sites <http://www.siskinent.com>, <http://www.permaplate.com>, and <http://www.permaplatefilms.com> (“Sites”). PermaPlate is the controller of your limited PPI provided to, collected by or for, or processed with your use of the Sites and the retail purchase of our products. Entering the Sites constitutes your acceptance and agreement to the terms in this Privacy and Security Policy. If you do not agree with these terms Privacy and Security Policy, please do not enter the Sites.

WHAT PERSONAL PRIVATE INFORMATION (“PPI”) WE COLLECT

- **Types of limited PPI We Collect**
 - Your name
 - Your address
 - Your e-mail address

- Your phone number
 - Information about your vehicle (make, model, year, color, VIN etc.)
 - Date our Product was applied and the price paid
 - Details about your warranty and any warranty claims
- **We Collect your PPI When**
 - You purchase our products and or services from an authorized dealer.
 - You connect with us regarding customer service via our customer service center.
 - You visit the Sites or participate in interactive features of the Sites or mobile applications.
 - You sign up for mobile messages, or social media notifications from us.
 - You respond to one of our surveys, or participate in a focus group.
 - You provide us with comments, suggestions, or other input.

HOW AND WHY WE COLLECT PPI

- **Technologies Used**

We may use cookies and or other technologies to receive and store certain types of information. This information includes Internet Protocol (IP) addresses, browser information, Internet Service Provider (ISP), operating system, date/time stamp and other data conveyance methods including facsimile, pdf, jpeg and other electronic files. This information helps us provide timely customer service in the event of our claims administration of your warranty or service contract. To provide the best customer experience possible, we also use this information for reporting and analysis purposes, such as how you are timely responding to your claim and our performance required for any follow-up services.

- **Information you give us directly.**

When you sign up for, or purchase, a product or service from an authorized dealer or agent you provide limited PPI, like your name, mailing address, email address, telephone number, and information to us so we can provide you with the product or service you are purchasing, e.g., a warranty or service contract. Also, you give us information verbally by phone or in writing by email or letter, particularly when you file a claim.

- **Information we receive from companies that help us provide you with products and services.**

We receive information from third parties we engage to examine your vehicle and report back to us regarding your warranty or service contact claim. This may include a body or repair shop and or a professional technician required to perform repairs at our expense in relation to claims you make with us.

- **User Experience Information**

To improve customer service and to assist you in resolving any issues surrounding your claim, we use tools to monitor certain user experience information, including, but not limited to, login information, IP address, data regarding pages visited, and specific actions taken on pages visited.

- **Information from Other Sources**

We may also obtain your limited PPI from business partners and associates under the consent you have provided them. This may improve our ability to resolve any claims and surrounding issues in a timely and professional manner.

- **Public Forums**

Any information you submit in a public forum (e.g., a blog, chat room, or social network) can be read, collected, or used by us and other participants, and could personalize your experience. You are responsible for the information you submit in these instances.

- **Mobile Privacy**

We offer mobile applications (“apps”) that allow you to receive claims administration services and other information from us. All information collected by us via our mobile application is protected by this Privacy and Security Policy. Although you do not have to provide your location information to us to use our mobile applications, our services require a zip code to function. If you have questions about location and notification privacy, please contact your mobile service provider or the manufacturer of your device to learn how to adjust your settings.

HOW WE USE THE INFORMATION WE COLLECT

- **Product and Service Fulfillment**
 - Fulfill and manage purchases, orders, payments, returns/exchanges, or requests for information, or to otherwise serve you.
 - Provide any requested services.
- **Internal Operations**
 - Improve the effectiveness of the Sites, mobile experience, and marketing efforts.
 - Perform other needed business activities as described elsewhere in this policy.
- **Fraud Prevention**
 - To prevent fraudulent transactions, monitor against theft and otherwise protect our customers and our business.
- **Legal Compliance**
 - To assist law enforcement and respond to subpoenas.

HOW WE PROTECT THE INFORMATION WE COLLECT

- **Security Methods**
 - We maintain leading technical, administrative, physical, electronic and procedural safeguards at our international headquarters in Salt Lake City, Utah to protect the confidentiality and security of PPI transmitted to us. Your limited PPI may only be accessed by persons within our organization, or our third party service providers, or business partners and associates (“Companies”), who require such access to carry out the purposes stated in this policy, your desired business intent. To guard this information, our Sites use Transport Layer Security (TLS), version 2.0, SSL and Transparent Data Encryption (TDE) where we collect PPI. TLS encrypts your PPI so only we can decode the information.
- **E-mail Security**
 - E-mail may not be encrypted and is not considered a secure means of transmitting PPI. “Phishing” is a scam designed to steal your information. If you receive an e-mail that looks like it is from us asking you for certain information, such as a credit card, do not respond. Though we might ask you your name, or possibly a VIN #, we will never request your password, credit card information or other or additional PPI through e-mail. We also use a 3rd party security provider with Targeted Threat Protection and URL Defense and AI Learning.
- **Additional Security**
 - We suggest all our customers to take measures to help protect your PPI, including:
 - Install the latest security updates and anti-virus software on your computer to help prevent malware and viruses.
 - Reset your e-mail account passwords frequently, at least every 90 days.
 - Use complex passwords or passphrases
 - Do not use the same password on more than one website.
 - Do not share your password with others.
 - Sign out/log off website sessions so your session is closed and cannot be accessed by another user on the same computer, especially when using a public computer or terminal.

HOW WE SHARE THE INFORMATION WE COLLECT

- **General Policy**
 - We do not sell or rent, nor have we ever sold or rented, PPI to third parties; except, we may share your limited PPI with third parties.
 - **Service Providers**
 - We may need to share your PPI with our service providers, business partners, and associates (“Companies”) to ensure the proper registration of your Warranty or Service Contract, to administer any claims, to process requests for cancellations, and general financial management, control and collection. We share only necessary PPI to achieve the purposes required. These Companies may not use the information we share with them for any other purpose.
 - **Legal Requirements**

- We may disclose your PPI you provide to us when disclosure is appropriate to comply with the law, including to meet national security or law enforcement requirements; to enforce or apply terms and conditions and other agreements; or to protect the rights, property or safety of our company, our customers or others.
- **When You Direct Us**
 - At your direction or request, we may share your PPI.
- **Business Transfers**
 - If some or all of our business assets are sold or transferred, we generally would transfer the corresponding PPI regarding our customers. We also may retain a copy of that PPI.
- **International Data Transfers**
 - If we are deemed to transfer PPI cross-border, we rely on the following legal bases to transfer your PPI under legally-provided mechanisms to lawfully transfer data across borders:
 - Consent (where you have given consent);
 - Contract (where processing is necessary for performing an obligation we have to you as Administrator of the warranty or Service Contract you purchased); and
 - Legitimate interests (as outlined in this Privacy Policy)

WHAT CHOICES DO YOU HAVE?

Canadian Customers - Access and Rectification

You may request access to your PPI and to request a correction to it if you believe it is inaccurate. If you have submitted PPI to us and would like access to it, or if you would like it removed or corrected, please contact us using the contact information below. We will use reasonable efforts to comply with your request. However, sometimes, we may not be able to allow you to access PPI, for example if it contains personal information of other persons, or for legal reasons. In such cases, we will provide you with a reasonable explanation of why it is not possible to grant access to your PPI.

California Consumer Privacy Act – for California Consumers

This PRIVACY NOTICE FOR CALIFORNIA RESIDENTS supplements the information in the Privacy Statement of Siskin/Permaplate and our affiliates (collectively, “we,” “us,” or “our”) and applies solely to residents of California (“consumers” or “you”). We have adopted this specific notice to comply with the California Consumer Privacy Act of 2018, its rules and regulations, *et seq* (“CCPA”) and other California privacy laws. Any terms defined in the CCPA have the same meaning when used in this notice.

Information We Collect

We collect information that identifies, relates to, describes, references, can be associated with, or could reasonably be linked, directly or indirectly, with a particular consumer (“personal information”). We have collected these categories of personal information from consumers within the last twelve (12) months:

Category	Examples
A. Identifiers.	A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, or other similar identifiers.
B. Personal information categories in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)).	A name, signature, address, telephone number. Some personal information in this category may overlap with other categories.
C. Commercial information.	Personal property, products or services purchased, obtained, or considered, or other purchasing.

Personal information does not include:

- Publicly available information from government records
- De-identified or aggregated consumer information.
- Information excluded from the CCPA's scope, like:
 - Health or medical information covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the California Confidentiality of Medical Information Act (CMIA) or clinical trial data;
 - Personal information covered by certain sector-specific privacy laws, including the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA) or California Financial Information Privacy Act (FIPA), and the Driver's Privacy Protection Act of 1994.

We obtain the categories of personal information listed above from the following sources:

- **Information you give us directly.** When you sign up for, or purchase, a product or service from us, we'll ask you for personal information, like your name, mailing address, email address, telephone number, and information to provide you with the product or service you are purchasing, or when we receive information from you verbally by phone or in writing by email or letter, including when you file a claim.

- **Information you give us indirectly.** When you complete warranty registration forms, service contract forms, or other PermaPlate forms provided by car, marine, RV and power sports dealers, we receive the information you have provided.
- **Information we receive from companies that help us provide you with products and services.** We receive information from third parties we hire to examine your vehicle and report back to us in relation to warranty or service contact claims you might make and from repair shops that perform repairs at our expense in relation to claims you have made with us.
- **Information we receive from our business partners and associates.** We receive information from business partners and associates under the consent you have provided them.

Use of Personal Information

We may use or disclose the personal information we collect for one or more of the following business purposes:

- Process and administer the limited warranty associated with our appearance protection product;
- Process and administer your service contract;
- Provide the products and services you request (fulfillment of requests for additional consumer kits, warranty transfers to subsequent owners, etc.), or to otherwise operate our business;
- Evaluate the effectiveness of our customer responsiveness and improve our products and services (complaint management system);
- Respond to your questions or inquiries;
- Carry out other purposes disclosed to you and to which you have consented; and comply with legal or regulatory requirements (For example, we are required by law in several states to retain a registration record for each warranty issued with a protection product purchase for the term of the warranty, and for a specified time thereafter).
- As described to you when collecting your personal information or as otherwise set forth in the CCPA.
- To evaluate or conduct a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of our assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which personal information held by us is among the assets transferred.

We will not collect additional personal information or use the personal information we collected for materially different, unrelated, or incompatible purposes without providing you notice.

Sharing Personal Information

We may disclose your personal information to a third party for a business purpose. When we disclose personal information for a business purpose, we enter a contract that describes the purpose and requires the recipient to both keep that personal information confidential and not use it for any purpose except performing the contract.

In the preceding 12 months, we have disclosed these categories of personal information for a business purpose:

Category A: Identifiers.

Category B: California Customer Records personal information categories.
Category C: Commercial Information.

We disclose your personal information for a business purpose to these categories of third parties, to our affiliates, to third party service providers or third parties to whom you or your agents authorize us to disclose your personal information with products or services we provide to

In the preceding twelve (12) months, we have sold no personal information.

Your Rights and Choices

The CCPA provides consumers (California residents) with specific rights regarding their personal information. This section describes your CCPA rights and explains how to exercise those rights.

Access to Specific Information and Data Portability Rights

You may request that we disclose certain information to you about our collection and use of your personal information over the past 12 months. Once we receive and confirm your verifiable consumer request, we will disclose to you:

- The personal information and sources of the personal information we collected about you.
- Our business or commercial purpose for collecting that personal information and the third parties with whom we share that personal information.
- The specific pieces of personal information we collected about you (also called a data portability request).
 - If we disclosed your personal information for a business purpose, the disclosures for a business purpose, identifying the personal information categories that each category of recipient obtained.

Deletion Request Rights

You may request that we delete any of your personal information we collected from you and retained, subject to certain exceptions. Once we receive and confirm your verifiable consumer request, we will delete (and direct our service providers to delete) your personal information from our records, unless an exception applies.

We may deny your deletion request if retaining the information is necessary for us or our service providers to:

1. Complete the transaction for which we collected the personal information, provide a good or service you requested, take actions reasonably anticipated within the context of our ongoing business relationship with you, or otherwise perform our contract with you;
2. Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activity;
3. Debug products to identify and repair errors that impair existing intended business purposes;
4. Exercise free speech, ensure the right of another consumer to exercise their free speech rights, or exercise another right provided for by the CCPA;
5. Comply with the California Electronic Communications Privacy Act (Cal. Penal Code 1546 seq.);

6. Enable solely internal uses reasonably aligned with consumer expectations based on your relationship with PermaPlate;
7. Comply with a legal obligation we have; and
8. Make other internal and lawful uses of that information compatible with the context in which you provided your personal information.

Exercising Access, Data Portability, and Deletion Rights

To exercise the access, data portability, and deletion rights described above, please submit a verifiable consumer request to us by either:

- **Calling us at 800-___-___.**
- **Emailing us at _____@_____.com.**

Only you or a person registered with the California Secretary of State you authorize to act on your behalf, may make a verifiable consumer request related to your personal information. You may also make a verifiable consumer request on behalf of your minor child.

You may only make a verifiable consumer request for access or data portability twice within a 12-month period. The verifiable consumer request must:

- Provide sufficient information that allows us to reasonably verify you are the person about whom we collected personal information or an authorized representative.
- Describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it.

We cannot respond to your request or provide you with personal information if we cannot verify your identity or authority to make the request and confirm the personal information relates to you. Making a verifiable consumer request does not require you to create an account with us. We will only use personal information provided in a verifiable consumer request to verify the requestor's identity or authority to make the request.

Response Timing and Format

We strive to reply to a verifiable consumer request within 45 days of its receipt. If we require more time (up to 90 days), we will inform you of the reason and extension period in writing. If you have an account with us, we will deliver our written response to that account. If you do not have an account with us, we will deliver our written response by mail or electronically, at your option. Any disclosures we provide will only cover the 12-month period preceding the verifiable consumer request's receipt. The response we provide will also explain the reasons we cannot comply with a request, if applicable. For data portability requests, we will select a format to provide your personal information readily useable and should allow you to transmit the information from one entity to another entity without hindrance.

We do not charge a fee to process or respond to your verifiable consumer request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we

will tell you why we made that decision and provide you with a cost estimate before completing your request.

Non-Discrimination

We will not discriminate against you for exercising any of your CCPA rights. Unless permitted by the CCPA, we will not deny you goods or services, charge you different prices or rates for goods or services, including through granting discounts or other benefits, or imposing penalties, or provide you a different level or quality of goods or services.

HOW DO YOU ACCESS AND UPDATE THE INFORMATION

- To keep your information accurate and complete, you can access or update some of your information in these ways:
 - Contact us with your current contact information and the information you would like to access. We will provide you the information requested if reasonably available, or will describe more fully the information we typically collect.
 - Depending on your location, you may also have certain additional rights regarding your personal information such as (i) the right to obtain a copy of your personal data you provided to us; (ii) the ability to change or correct your personal data through your account settings; (iii) the right to have us delete or limit our use of your personal information, except information we must retain, by contacting us.

INTERNATIONAL CUSTOMER PRIVACY

- PermaPlate is subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC).
- For most non-US transactions, we have partnered with third party companies (“Vendors”) that we have selected to help us facilitate international transactions. We work closely with these Vendors to ensure that your transaction is handled with care and all the information you provide is secure.
- Any information you provide us is controlled and processed by Siskin/PermaPlate.

PRIVACY POLICY REVISIONS

By accessing the Site or interacting with us, you consent to our use of information collected or submitted as described in this Privacy Policy. We reserve the right to change or modify this Privacy Policy at any time and in our sole discretion, and we will post the new Privacy Policy on our website at www._____.com on the date it becomes effective. You agree to the new Privacy Policy by your continued access to and/or use of our site and/or your continued use of our products and/or services after any such changes. Please periodically review this privacy policy so you know what personal information we collect, how we use it, and with whom we may share it. We may change or add to this Privacy Policy, so we encourage you to review it periodically.

Siskin Enterprises, Inc., PermaPlate Company, LLC and PermaPlate Film LLC.
Legal and Compliance Department
P.O. Box 58
Salt Lake City, Utah 84110

This Security and Privacy Policy was last updated on April 7, 2020.