



GPC Teammate and Applicant Privacy Notice

WE KEEP *THE WORLD*
MOVING



Overview

Your privacy is important to the Genuine Parts Company including but not limited to our operating divisions, subsidiaries, affiliates, and branches worldwide (collectively “GPC”, “we”, “us”, or “our”). We are proud to offer rewarding careers that combine a small company feel with a global scale, and we are committed to handling Teammate (employees, contractors, contingent or other personnel) and Applicant (prospective Teammate) personal data responsibly.

This notice and other notices provided to you at the time of collection explain how we collect your personal data, the types of personal data we process, why and how we use and share it, and your related rights.

Please note that this notice applies to your personal data handling as a Teammate or Applicant only. Our [Customer Privacy Notice](#) covers personal data we process about customers through other websites, applications, or services.

Personal Data We Collect and Use

How We Collect Your Personal Data

We collect personal data when you provide it directly to us like when you apply for a job with or accept employment with us, when we collect it automatically through our websites and information systems, and indirectly through our service providers like for background checks.

Why We Process Your Personal Data

We process your personal data for a variety of purposes including legitimate business purposes and to manage your employment or relationship with us. If you are a Teammate, we process your personal data and your emergency contacts’, dependents’ and beneficiaries’ personal data in order to manage your employment. If you are an Applicant, we process your personal data to communicate with you about careers at GPC, and to evaluate and manage your candidacy which may include interview scheduling, background screening, and on-boarding if you choose to accept our employment offer. If you are a Teammate or Applicant who needs access to GPC facilities or information systems, we also process your personal data to provide necessary access.

We may additionally process personal data based on your consent, like for background check verification, or, if you are an Applicant, to retain your profile longer than six months as described in the “Data Retention” section below. We also process personal data to comply with our applicable legal obligations - including to exercise or defend the legal rights of you, us or others; to meet requirements for tax, health and safety, anti-discrimination, whistleblowing, data subject rights, and similar laws, regulations, or law enforcement requests.

We limit processing of personal data considered sensitive or special category data under applicable laws to comply with legal requirements like employment laws and legal claims, conduct diversity and inclusion initiatives, provide health and insurance benefits, and to manage workplace attendance and absence.

Types of Personal Data We Process

We process personal data about you, which can include but is not limited to:

- **Name and contact details** - your full name, employee identification number, date of birth, email address, mailing address, phone number, and any similar details for beneficiary, dependent, and/or emergency contacts as applicable
- **Background information** – resume/CV qualification information like educational and work history; results of verifications where applicable to the job or position role including credit and criminal background checks, drug and alcohol screening, driving history, vehicle registration, vaccination status, and health certification
- **Demographic data** – date of birth, gender, and additional information considered sensitive or special categories of data under applicable laws like race, ethnicity, parental and military status, health, disability, sexual orientation, gender identity, transgender status, union membership, and religious, political, and philosophical beliefs
- **National identifiers** – government and taxpayer identification numbers like social security number, citizenship status, national ID, passport, residency number, work permit status, and driver's license
- **Teammate information** – job or position title, work location, performance history, complaint and investigation reports, achievements, and disciplinary actions
- **Financial information** – wage, salary, bonus, equity, bank account details, retirement account information, and other information required to provide services related to payroll, equity and incentive compensation, taxes, and benefits
- **Video, voice, and images** – video including workplace CCTV footage, voice, and photo for premises monitoring and to conduct our business operations
- **Biometric information** – fingerprints or other biometric information processed only as required for high-security situations, subject to additional terms as disclosed to you prior to collection
- **Workplace, device, information system, and content data** –location and other usage information associated with your use of GPC-owned equipment and information systems like devices, vehicles, and electronic communication systems; content of profiles, posts, and communications on intra-company websites, email, messaging, and phone systems

Please note that we presume your activity on GPC-owned communication systems and devices is work-related and may be monitored. We process this data in order to ensure organizational security, monitor appropriate use, comply with laws, and to support IT and other business operations.

Personal Data We Disclose

We disclose your personal data when we have a legitimate business need to operate our business, comply with legal obligations, and at your request or with your consent for the uses described above. When we share your personal data with third parties, we require them to handle your personal data in accordance with this privacy notice. We may disclose your personal data to the following types of recipients:

- **Other Individuals and Teammates** – Your personal data like your GPC work profile, posts, and communications on intra-company websites are available to display to other Teammates. As applicable to certain GPC job roles like business representatives, we may make portions of your Teammate profile like work contact information available publicly or to our business customers.
- **Service Providers** – We engage these vendors to provide services on our behalf and at our direction including to manage taxes, travel, and expenses, health and safety, and to administer payroll, benefits, equity, and other incentive compensation. Benefits including medical insurance and retirement may require you to provide information directly to the service provider. We also share personal data with service providers who support our IT environment like cloud hosting, analytics, device management, remote access and information security or other technical services.
- **Regulatory Bodies and Law Enforcement Authorities** – We disclose personal data like national identifiers and demographic data to these entities in order to comply with applicable tax and healthcare laws and regulations. We may also disclose your personal data to law enforcement, courts of law, government agencies, and regulatory authorities to comply with legal requests like court orders or subpoenas. We may also disclose your personal data to these entities to meet our contractual obligations, or if we, in good faith, believe that disclosure is otherwise necessary or advisable to protect your, our, or others' rights, property, or safety; enforce our policies or contracts; collect amounts owed to us; or assist with an investigation or prosecution of suspected or actual illegal activity.
- **Entities Associated with Mergers, Acquisitions, and Other Business Transfers** – If we are involved in a merger, acquisition, financing due diligence, reorganization, asset purchase, bankruptcy, receivership, sale of company assets, transition of service or other business transfer, we may disclose your personal data as part of these processes as permitted and/or required by law and/or contract.
- **Affiliates and Subsidiaries** – We may disclose your personal data within our affiliates and subsidiaries for our internal business purposes.

Your Privacy Rights

In accordance with applicable law, you may have the right to:

- **Access and “port” your personal data**, including: (i) requesting confirmation of whether we are processing your personal information; (ii) obtaining access to or a copy of your personal information; (iii) receiving an electronic copy of personal information that you have provided to us, or ask us to send that information to another company (the “right of data portability”).
- **Request restriction of or object to our processing of your personal data**, including the right to: (i) withdraw your consent to processing, (ii) object to or restrict our uses of your Sensitive personal information for certain purposes, or (iii) opt out of profiling in furtherance of decisions that produce legal or similarly significant effects concerning you, if applicable, where each such requests are permitted by law.
- **Request correction of inaccurate or incomplete personal data**. In some cases, we may provide self-service tools that enable you to update your personal information, or we may refer you to the third-party who is the controller of your personal information who is able to make the correction.
- **Request deletion of personal data**, subject to certain exceptions prescribed by law.

You may submit an online request to exercise your rights [here](#) if you are in the US or Canada and [here](#) if you are in the EU, UK or Switzerland.

You have the right to not receive discriminatory treatment or be retaliated against for exercising any of these rights. If you would like to exercise any of these rights, please contact us as set forth below. We will evaluate and process such requests in accordance with applicable laws. To protect your privacy, GPC will take steps to verify your identity before fulfilling any valid request.

You may also authorize an agent to exercise the personal information rights described above. To authorize an agent, provide written authorization signed by you and your designated agent and Contact Us as set forth below for additional instructions.

International Data Transfers

We process personal data globally, including in but not limited to the United States. We use technical, organizational, and contractual measures to protect this personal data. When we make cross-border data transfers from the EEA, UK, or Switzerland to other countries, we consider applicable [adequacy decisions](#). As required, we implement the “[standard contractual clauses](#)” and the UK Addendum (“SCCs”) with data importers to provide an adequate level of protection.

Data Retention

We retain your personal data for as long as needed to fulfill the purposes described in this Privacy Notice. We consider various factors to determine the retention period relevant to you personal data as a Teammate or Applicant including volume and sensitivity, business need, and legal and regulatory obligations or guidance.

When an Applicant’s interview and review process ends, and does not result in job offer and acceptance, we retain the Applicant’s personal data for six months beyond the last interaction unless

retention is otherwise legally required. During the standard six month retention period we retain the personal data to consider the Applicant for other job openings and for legal/record keeping purposes. After the six month retention period ends, we will ask for your consent to retain your personal data for up to two years. If you do not consent, we will delete your profile. If you do consent to this extended period, we will consider you for future roles and may contact you for recruitment purposes. We will delete your profile after two years if we do not hear from you. You may email careers_pl@genpt.com to withdraw your consent at any time.

Security of Your Personal Data

We use technical, organizational, and contractual measures to protect the personal data that we store, transmit, or otherwise process against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. We regularly consider appropriate new security technology and methods as we maintain and develop our software and systems. Unfortunately, no online environment can be guaranteed to always be secure, and we cannot ensure or warrant the security of any information you provide to us. To the fullest extent permitted by applicable law, we do not accept liability for unintentional disclosure. If we learn of a data breach that is likely to affect the security of your personal information, we will notify you consistent with our legal obligations.

Third-Party Links and Applications

Our internal websites and applications may contain links to third-party websites or applications. Other public websites and applications not owned or operated by us may reference us or link to our sites or resources. Third-party services like these are not controlled by us. We do not control the privacy practices of these services and encourage you to read their privacy notices and consider the risk of using them.

Effective Date, Changes to Our Privacy Notice and Practices

When we update this Privacy Notice, we will revise the “Last Updated” date. If we make any material changes, we will make reasonable efforts to inform you, consistent with the significance of the changes we make.

Contact Us

For present and former Teammates, the controller of your personal data is the GPC entity that is or was your employer or the entity to which you provided contract services. For Applicants, the party responsible for (i.e., the controller of) your personal information is the GPC entity to which you have applied for a role. If you have any questions about our privacy practices or this Privacy Notice, you may submit an online request [here](#) or use the contact information below:

If located in the United States:

Email: gpc_privacy@genpt.com

Postal Mail: Genuine Parts Company, Attention: Legal Department- Privacy, 2999 Wildwood Parkway, Atlanta, GA 30339.

If located in Canada:

Email: data.privacy@uapinc.com

Postal Mail: UAP Incorporated, Attention: Legal Department- Privacy, 7025 Ontario Street East, Montreal, Quebec H1N 2B3.

If located in EEA, UK, or Switzerland:

Email: compliance@allianceautomotive.eu

Postal Mail: Legal Department- Privacy, 90 Chancery Lane, London WC2A 1EU

Region-specific Disclosures

California Notice

If you are an Employee or Applicant residing in California, then this notice applies to you. The California Privacy Rights Act provides you with specific rights regarding your personal information. This notice explains your rights and how to exercise them. We will not discriminate against you for exercising them.

You or your authorized agent may exercise your California privacy rights by submitting an online request [here](#) or through the additional methods described in the “Contact Us” section above. You have the right to request:

1. Notice of and access to the categories of personal information we collect about you within the past 12 months, the categories of sources of personal information we collect about you, our purpose for collecting them, the categories of third parties to whom we disclosed specific categories of personal information, and specific pieces of personal information we disclosed about you.
2. Deletion of your personal information
3. Correction of inaccurate personal information about you

We do not “sell” or “share” your personal information for cross context behavioral advertising. We otherwise disclose personal information as described in the table below:

Category of Personal information Collected	Category of Third Parties to which Information is disclosed
Identifiers A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number or other similar identifier	<ul style="list-style-type: none">• Service Providers• Government entities• GPC affiliates• Benefits Providers

<p>Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e))</p> <p>A name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information.</p>	<ul style="list-style-type: none"> • Service Providers • GPC affiliates • Benefits Providers
<p>Sensitive personal information</p> <p>A social security, driver's license, state identification card, or passport number, an account log-in, financial account, debit card or credit card number in combination with any required security or access code, password, or credentials allowing access to an account, biometric information, precise geolocation, racial or ethnic origin, religious or philosophical beliefs, or union membership, contents of a Teammate's mail, email, and text messages unless the business is the intended recipient of the communication, or genetic information.</p>	<ul style="list-style-type: none"> • Service Providers • Government entities • GPC affiliates • Benefits Providers
<p>Protected classification characteristics under California or federal law</p> <p>Age (40 years or older), race, color, ancestry, national origin, citizenship, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status, genetic information (including familial genetic information).</p>	<ul style="list-style-type: none"> • Government entities • GPC affiliates • Benefit Providers
<p>Geolocation data</p> <p>Physical location or movements (of Company-owned vehicles or devices)</p>	<ul style="list-style-type: none"> • Service Providers • GPC affiliates
<p>Professional or employment-related information</p> <p>Current or past job history or performance evaluations.</p>	<ul style="list-style-type: none"> • GPC affiliates

We describe the purposes for personal information collection and categories of sources from which we collect it in the "Personal Data We Collect and Use" section above. We disclose your personal information as described in the "Personal Data We Disclose" section. The "Data Retention" section above explains the criteria we use to determine how long to retain your personal information.

European Economic Area, United Kingdom, and Switzerland

For present and former Teammates, the controller of your personal data is the GPC entity that is or was your employer or the entity to which you provided contract services. For Applicants, the party responsible for (i.e., the controller of) your personal data is the GPC entity to which you have applied for a role.

If you are working in or residing in these locations, you may have certain rights under applicable laws like the EU and UK General Data Protection Regulation and similar local laws, including your rights to request:

1. Access to and a copy of your personal data;
2. Correction of inaccurate personal data;
3. Erasure or deletion of personal data that is no longer needed for its original purpose of collection and does not need to be retained for other legitimate purposes;
4. Restrict or object to the processing of your personal data; and
5. Transfer of your personal data to another company.

We handle cross-border data transfers as described in our “International Data Transfers” section above, and our legal bases and purposes for processing your personal data are described in the “Personal Data We Collect and Use” and “Personal Data We Disclose” sections above.

If you have any questions about our privacy practices or this Privacy Notice, you may contact us by using the information in the Contact Us section above. We endeavor to answer your privacy questions, however, you also have the right to complain to your relevant data protection authority.