



Yes, you can.®

INVACARE CORPORATION

California Consumer Privacy Act **Employee Disclosure**

January 1, 2020

Invacare Corporation (“Company”) respects the privacy of our employees as an essential part of our privacy program. We are committed to the proper handling of the personal information collected or processed in connection with your employment relationship with us as required by the California Consumer Privacy Act of 2018 (“CCPA”). This disclosure describes categories of personal information we collect and the purposes for which we process that information in accordance with the CCPA, which defines personal information generally as information that identifies, relates to, describes or is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly to a particular individual or household. Personal information does not include publicly available information, which is defined under CCPA to mean information lawfully made available from federal, state, or local government records.

We collect, receive, maintain and/or share personal information with third party service providers to carry-out certain processes related your employment, such as paying you and providing you with benefits. The categories and the purposes described below for use of personal information reflects data processed by our third party service providers.

	Examples Only (not all information is collected in each category)	Collected
Category A.	Identifiers, such as name, contact information, online identifiers and Social Security numbers and other government-issued ID numbers	YES
Category B.	Personal information, as defined in the California consumer records law, such as name, contact information, insurance policy number, education, employment, employment history financial information, medical information and health information ¹	YES
Category C.	Characteristics of protected classifications under California or federal law, ² such as sex, age, race, disability, citizenship, immigration status and marital status	YES
Category D.	Commercial information, such as transaction information, purchase history and financial details	NO

¹ This includes 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.

² This include sex, age (40 and over), race, color, disability, marital status, citizenship, immigration status, military/veteran status, domestic violence victim status, and request for leave.

Category E.	Biometric information, such as facial recognition and fingerprints	YES ³
Category F.	Internet or network activity information, such as browsing history and interactions with our website, applications or systems	YES
Category G.	Geolocation data, such as device location	YES ⁴
Category H. ⁴	Audio, electronic, visual, and similar information, such as images and audio, video or call recordings created in connection with our business activities;	YES
Category I.	Professional or employment-related information, such as work history and prior employer, human resources data and data necessary for benefits and related administrative services	YES
Category J.	Education information subject to the federal Family Educational Rights and Privacy Act, such as student records	YES
Category K.	Inferences drawn from any of the Personal Information listed above to create a profile or summary above, for example, an individual's preferences, abilities, aptitudes and characteristics	NO

Personal information is collected for the following purposes:

1. To comply with state and federal law and regulations;
2. To process payroll;
3. To track time and attendance;
4. To manage workers' compensation claims;
5. To administer and maintain benefits, including group health insurance;
6. To administer and maintain retirement service;
7. To manage employee performance of their job duties, including promotions, discipline, and/or termination;
8. To conduct workplace investigations;
9. To evaluate job applicants and candidates for employment;
10. To obtain and verify background checks;
11. To grant and monitor employees' access to secure company facilities;
12. To implement, monitor, and manage electronic security measures on devices that are used to access networks and systems (e.g., incident management);
13. To engage in corporate transactions requiring review of employee records, such as for evaluating potential mergers and acquisitions of the Company;
14. To maintain commercial insurance policies and coverages, including for workers' compensation and other liability insurance;
15. To anonymize and/or aggregate data to perform workforce analytics, data analytics, and benchmarking;
16. To perform call monitoring and surveillance (e.g., CCTV); and
17. To provide, validate, or communicate services offered by our third party service providers (e.g., ADP for payroll purposes), directly to individuals.

³ Our third party service provider, ADP, uses biometric time clocks to verify employees identity when clocking in or out, by scanning a portion of the employee's finger or hand. The clocks do not collect or store an image of the employee's finger or hand; rather, they create and store encrypted mathematical representation of a portion of the finger or hand.

⁴ Only for Sales Associates that utilize the Motus mobile application.

If you have any questions about the collection and processing of your Personal Information or about the security of your Personal Information, please contact privacy@invacare.com or Human Resources.