



Personal Information Protection Policy

- Purpose:** SmartDrive Systems, Inc. ("SmartDrive") has adopted this policy to define requirements for the treatment of SmartDrive's employees' Personal Information, specifically how SmartDrive may collect and use information about our employees, job applicants, and candidates. While this policy is intended to describe the broadest range of SmartDrive's information processing activities globally, those processing activities may be more limited in some jurisdictions based on the restrictions of applicable laws. This notice is also adopted to comply with the California Consumer Privacy Act of 2018 (CCPA) and any terms defined in the CCPA have the same meaning when used in this notice.
- Background:** SmartDrive is a global company with its headquarters in the United States. To facilitate SmartDrive's global operations, SmartDrive may transfer and access Personal Information from around the world, including from other countries where it has operations. This means that Personal Information may be collected from, used, processed, and transferred to the United States and other countries or territories, and those countries or territories may not offer the same level of data protection as the country where you reside. Personal Information of employees located in the European Union are also governed by an additional privacy policy.
- Policy:** As a SmartDrive employee, third party contractor, job applicant, or candidate, you must expressly acknowledge that you have read, understand and agree to all terms of this Policy, as outlined below and as it may be modified by SmartDrive from time to time without prior notice. Where SmartDrive collects additional categories of personal information or uses the personal information we collected for materially different, unrelated, or incompatible purposes, SmartDrive will provide you notice.
- Management's commitment:** Management supports SmartDrive's Personal Information protection efforts to help its employees and third party contractors recognize and protect Personal Information. SmartDrive is committed to protecting the privacy and security of the Personal Information collected, processed, stored, and SmartDrive takes reasonable physical, electronic, and administrative measures to help protect the information from unauthorized or inappropriate access or use.
- Scope:** This policy applies to all employees, job applicants, and third party contractors. SmartDrive has separate privacy policies and terms of use that apply to the collection and use of Personal Information on its websites. Additionally, certain SmartDrive's products and services may have separate privacy policies and terms of use that apply to the collection and use of Personal Information. Any Personal Information collected by SmartDrive in connection with your use of its websites or products and services are not subject to this policy.
- Policy and Procedures Review:** The policy and related procedures will be reviewed every 12 months or as necessary.



7. **Personal Information:** SmartDrive collects and maintains different types of Personal Information about its employees, third party contractors, job applicants and candidates in accordance with applicable law. Some examples of Personal Information that SmartDrive may collect, also referred to as personal data, includes without limitation an individual's name, an individual's phone numbers, email address, mailing addresses, banking and other financial data, government identification numbers (e.g., social security numbers, tax payer ID's, driver's license, etc.), location data, an online identifier, date of birth, sexual orientation, gender, race, cultural or social identity, ethnicity, health and disability data, family-related data (e.g., marital status, personal and health-related data on family members, etc.), trade union data, national origin, and criminal records (referred herein as "Personal Information"). The terms Personal Information and personal data are used synonymously in this policy.

8. **Collection of Personal Information:** SmartDrive collects Personal Information directly from you in circumstances where you provide Personal Information (e.g., during the onboarding process, signing up for direct deposit, enrolling in benefits or services). This collection may include employee stock information. However, in some instances, the Personal Information that SmartDrive collects has been inferred about you based on other information you provide SmartDrive, through your interactions with SmartDrive, or from third parties. When SmartDrive collects your Personal Information from third parties, it is either because you have given SmartDrive express permission to do so, your permission was implied by your actions (e.g., your use of a third-party employee service made available to you by us), or because you provided explicit or implicit permission to the third party to provide the Personal Information to SmartDrive.

Where permitted or required by applicable law or regulatory requirements, SmartDrive may collect Personal Information about you without your knowledge or consent.

SmartDrive reserves the right to monitor the use of SmartDrive's premises, equipment, devices, computers, network, applications, software, and similar assets and resources. In the event such monitoring occurs, it may result in the collection of Personal Information about you. This monitoring may include the use of close circuit television (CCTV) cameras on and around SmartDrive's premises.

Additionally, SmartDrive may collect information required for SmartDrive to comply with laws, the requests and directions of law enforcement authorities or court orders (e.g., child support and debt payment information).

In particular, SmartDrive has collected the following categories of personal information from its employees, job applicants, or contractors within the last twelve (12) months:



Category	Examples ¹	Collected	Sources	Purpose	Third Parties Shared
A. Identifiers.	A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers.	YES	(a) Directly or indirectly from you (b) From third parties	(a) Performance of a contract (b) Necessary for our legitimate interests (c) Necessary to comply with a legal obligation	(a) Human resources information service providers (b) Financial investment service providers (c) Wellness program service providers to the extent that such a program is provided (d) Insurance providers and third party administrators (e) Training providers (f) Access control and security providers (g) Background check providers (h) Federal student aid and dependent care assistance providers (i) Voluntary legal assistance plan providers (j) Outside attorneys and law enforcement (k) Cellular mobile communications and internet connectivity providers

¹ Examples listed herein are illustrative of the types of personal information included in each category and may or may not be the specific types of personal information collected on an individual employee, contractor, or job applicant.



Category	Examples ¹	Collected	Sources	Purpose	Third Parties Shared
					(l) Information Technology help desk providers
B. Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)).	<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> <p>Some personal information included in this category may overlap with other categories.</p>	YES	<p>(a) Directly or indirectly from you</p> <p>(b) From third parties</p>	<p>(a) Performance of a contract</p> <p>(b) Necessary for our legitimate interests</p> <p>(c) Necessary to comply with a legal obligation</p>	<p>(a) Human resources information service providers</p> <p>(b) Financial investment service providers</p> <p>(c) Wellness program service providers to the extent that such a program is provided</p> <p>(d) Insurance providers</p> <p>(e) Outside attorneys and law enforcement</p> <p>(f) Potential investors/debt providers</p>
C. Protected classification characteristics under California or federal law.	<p>Age (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual</p>	YES	<p>(a) Directly or indirectly from you</p> <p>(b) From third parties</p>	<p>(a) Performance of a contract</p> <p>(b) Necessary for our legitimate interests</p> <p>(c) Necessary to comply with a legal obligation</p>	<p>(a) Human resources information service providers</p> <p>(b) Financial investment service providers</p> <p>(c) Wellness program service providers, to the extent that such a program is provided</p> <p>(d) Insurance providers</p>

Category	Examples ¹	Collected	Sources	Purpose	Third Parties Shared
	orientation, veteran or military status, genetic information (including familial genetic information).				
D. Commercial information.	Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.	NO			
E. Biometric information.	Genetic, physiological, behavioral, and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as, fingerprints, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data.	NO			
F. Internet or other similar network activity.	Browsing history, search history, information on a consumer's interaction with a website, application, or advertisement.	YES	(a) Directly or indirectly from you	(a) Performance of a contract (b) Necessary for our legitimate interests (c) Necessary to comply with a legal obligation	(a) Analytics and business intelligence vendors (b) Security service providers



Category	Examples ¹	Collected	Sources	Purpose	Third Parties Shared
G. Geolocation data.	Physical location or movements.	YES	(a) Directly or indirectly from you	(a) Necessary for our legitimate interests	
H. Sensory data.	Audio, electronic, visual, thermal, olfactory, or similar information.	YES	(a) Directly or indirectly from you	(a) Performance of a contract (b) Necessary for our legitimate interests (c) Necessary to comply with a legal obligation	(a) Security and access service providers
I. Professional or employment-related information.	Current or past job history or performance evaluations.	YES	(a) Directly or indirectly from you (b) From third parties	(a) Performance of a contract (b) Necessary for our legitimate interests (c) Necessary to comply with a legal obligation	(a) Human resources information service providers (b) Potential investors/debt providers
J. Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99)).	Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records.	YES	(a) Directly or indirectly from you (b) From third parties	(a) Necessary for our legitimate interests	(a) Human resources information service providers
K. Inferences drawn from other personal information.	Profile reflecting a person's preferences, characteristics, psychological trends, predispositions,	NO			



Category	Examples ¹	Collected	Sources	Purpose	Third Parties Shared
	behavior, attitudes, intelligence, abilities, and aptitudes.				

9. Use of Personal Information: SmartDrive may use Personal Information as follows to:

- identify you personally
- communicate with you
- comply with human resource requirements
- comply with government regulations
- provide employee benefits (e.g., compensation, health, insurance, etc.)
- provide wellness programs (to the extent that SmartDrive provides such programs)
- protect the safety and security of SmartDrive’s workforce, guests, property, and assets (including controlling and facilitating access to and monitoring activity on and in SmartDrive’s premises and activity using SmartDrive’s computers, devices, networks, communications and other assets and resources).
- carry out any additional purposes of which SmartDrive advises you or as otherwise set forth in the CCPA.
- carry out other purposes as part of SmartDrive’ business activities when reasonably required and necessary for our legitimate interests, including, for example:
 - track commissions and incentives for employees, annual performance evaluations, employment compensation, providing access control and safety for employees while on SmartDrive premises, expense reimbursement, phone and web conferencing, secure destruction of paper and electronic media, and support systems to streamline business operations.

10. Disclosure of Personal Information to Third Parties: SmartDrive will not disclose, sell or otherwise distribute Personal Information to any third party without your prior permission except under the following circumstances:

- Where you request SmartDrive or provide your consent to SmartDrive.
- In order to carry out the uses of Personal Information described in this Policy.
- When using or collaborating with third parties in the operation of SmartDrive’s business, including in connection with providing many of the benefits and services SmartDrive offers SmartDrive employees (e.g., human resources information systems, financial investment service providers, background check providers, employment authorization (E-Verify) service providers, on the job training providers, job applicant tracking providers, workers compensation providers, medical provider network for workers’ compensation, federal student aid and dependent care assistance providers, voluntary legal assistance plan providers, wellness program service providers (to the extent that such services are provided), insurance providers, outside attorneys and law enforcement, access control and security providers, cellular mobile communications and internet connectivity providers). When SmartDrive shares Personal Information with third parties, SmartDrive requires that they only use or disclose such Personal Information only as



necessary to provide the requested services to SmartDrive and in a manner consistent with the use and disclosure provisions of this policy and applicable law.

- SmartDrive may buy or sell businesses and other assets. In such transactions, employees' information is generally one of the transferred business assets and SmartDrive reserves the right to include your Personal Information as an asset in any such transfer. Also, in the event that SmartDrive, or substantially all of SmartDrive's assets, is acquired, your Personal Information may be one of the transferred assets.
- Where required by law, by order or requirement of a court, administrative agency, or government tribunal, which includes in response to a lawful request by public authorities, including to meet national security or law enforcement requirements or in response to legal process.
- If SmartDrive determines it is necessary or desirable to comply with the law or to protect or defend SmartDrive's rights or property.
- As necessary to protect the rights, privacy, safety, or property of an identifiable person or group or to detect, prevent or otherwise address fraud, security or technical issues, or to protect against harm to the rights, property or safety of SmartDrive, SmartDrive's customers, applicants, candidates, employees, third party contractors, or the public, or as otherwise required by law.
- Where the Personal Information is public.
- To seek advice from SmartDrive's attorneys and other professional advisers.
- To professional advisers (e.g., bankers, attorneys, accountants) and potential buyers and vendors in connection with the disposal or acquisition by use of a business or assets.
- Like most international businesses, SmartDrive has centralized certain aspects of SmartDrive's business operations, including for example, financial, human resources, and information technology administration. This may result in the transfer of Personal Information from one country to another and amongst SmartDrive's various subsidiaries and affiliates. It should be noted that this may or may not include countries where the level of privacy protection and the legal rights of individuals are not considered commensurate with standards of protection in jurisdictions having comprehensive data protection laws, such as the countries of the European Union and Canada.

11. **Access, Correction and Retention of Personal Information:** To access or correct your Personal Information that SmartDrive has collected, please refer to the appropriate steps in the appropriate section related to the Access to Personnel Files and Payroll Records in the SmartDrive Employee Handbook.

Except as otherwise permitted or required by applicable law or regulatory requirements, SmartDrive will retain your Personal Information only for as long as SmartDrive believes it is necessary to fulfill the purposes for which the Personal Information was collected, including for the purpose of meeting any legal, accounting or other reporting requirements or obligations.

12. **Security of Personal Information:** SmartDrive employs reasonable security measures and technologies, including without limitation, password protection, encryption, physical locks, video cameras for employee and physical asset safety, dangerous website blocking, etc. to ensure the confidentiality of Personal Information. If you are authorized to have access to the



Personal Information of others, it is important that you take the appropriate measures to protect this Personal Information. Paper and other hard copies containing Personal Information should be secured in a locked location when not in use. Computers and other access points should be secured when not in use by logging out or locking. Passwords and user ID's should be guarded and not shared. When no longer necessary for business purposes, paper and hard copies should be immediately destroyed using paper shredders or other approved devices. Do not leave copies in unsecured locations waiting to be shredded or otherwise destroyed. Do not make or distribute unauthorized copies of documents and other tangible medium containing Personal Information. Electronic files containing Personal Information should only be stored on secured company computers and not copied or otherwise communicated to unauthorized individuals within or outside of SmartDrive. Refer to SmartDrive Employee Handbook for more information about your responsibilities to protect confidential information, including your and others' Personal Information.

13. **Resolving Concerns:** If you have questions or concerns regarding this policy or the handling of your Personal Information, please contact accommodations@smartdrive.net. Alternatively, you may also anonymously report violations of policy or law using SmartDrive's third-party managed anonymous reporting hotline:

- USA: 1-800-721-0527
- UK: 0-808-189-1457
- China: 400-1-400-120-9176
- India: 000-800-100-4416

14. **Policy changes:** This policy is reviewed periodically to ensure it accurately captures all types of data collected or any additional or different processing of such data. SmartDrive may, therefore, change this policy at any time. When we make changes to this policy, we will provide you with a copy of the updated notice and/or also post the updated notice in Paycom and/or the SmartDrive intranet and update the Version History.

References and Related Documents:

California Consumer Privacy Act of 2018

15. Version History

Version	Description	Name	Date
1.0	Initial document summarizing current policy	Barrett Welch	03/23/2017
2.0	Add Personal Information protection control requirements to clarify responsibilities	Alex Branisteanu Jason Peretz	6/18/2018
3.0	Add requirements pursuant to the CCPA	Alex Branisteanu Barrett Welch	12/13/2019