ONLINE PRIVACY POLICY

ExtensisHR, Extensis Group LLC; Extensis, Inc.; Extensis II, Inc.; Extensis III, Inc.; Extensis IV, Inc.; Extensis HRO, LLC; Extensis VI, LLC; Extensis VIII, Inc.; Extensis IX, LLC; and Extensis Holding, LLC ("ExtensisHR;" the "Company" or "we") has developed this privacy policy out of respect for the privacy of our customers, visitors to our website, job applicants, and independent contractors. This policy describes the personal information we collect, use, and disclose about individual consumers, applicants, and contractors who visit or interact with this website, visit any of our offices, stores, facilities, or locations, purchase or inquire about any of our products or services, contract with us to provide services, apply for a position of employment, or otherwise interact or do business with us.

Whenever you visit our website, we will collect some information from you automatically simply by you visiting and navigating through this site, and some voluntarily when you submit information using a form on the website, utilize the Live Chat feature on our website, enroll in or subscribe to our newsletter or marketing communications, request information, or use any of the other interactive portions of our website. Through this website, we will collect information that can identify you and/or your activity.

Additionally, whenever you communicate, interact, or do business with us, we will be collecting personal information from you or about you in the course of our interaction or dealings with you, whether online or at any of our physical locations or facilities, or whether you are contracted to perform services for us or apply for a position of employment.

This policy does **not** apply to our current and former employees and their family members, dependents, and beneficiaries. If you are a California resident (who is a current or former employee of the Company or a family member, dependent, or beneficiary of any of our current or former employees), you may request access to our Employee Privacy Policy by sending an email to PrivacyPolicy@ExtensisHR

PARTICIPATION IN DATA PRIVACY FRAMEWORK PROGRAM

ExtensisHR complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) as set forth by the U.S. Department of Commerce. ExtensisHR] has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union in reliance on the EU-U.S. DPF. If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit Data privacy framework website.

Consent to Share Personal Information When Using Chat Function

By using the Live Chat feature, you consent to our collection and analysis of all personal information provided. The Live Chat feature does not use any chatbot or artificial intelligence technology. Rather, each chat takes place with a live representative of the Company. We utilize a vendor called **Drift.com ("Chat Vendor")** to process, analyze, and store the contents of the chat on our behalf. The Chat Vendor "will not sell this data or share it besides the Company or another vendor engaged to assist in the services provided to the Company. The Chat Vendor will not use or disclose this data for any purpose other than providing services to the Company." For more information on how the Chat Vendor may use or disclose your personal information, please review their privacy policy https://www.drift.com/privacy-policy/. By using these forms and features, you direct the Company to disclose to and share with the Chat Vendor any personal information you provide.

Collection of Personal Information and Sensitive Personal Information

Based on your specific transactions and interactions with us or our website, we will or may collect, and we have in the last 12 months collected, the following categories of personal information about you. For each category of information, the categories of third parties and service providers to whom we have disclosed the information in

the last 12 months are detailed in the chart below. The examples provided for each category are not intended to be an exhaustive list or an indication of all specific pieces of information we collect from or about you in each category, but rather the examples are to provide you a meaningful understanding of the types of information that may be collected within each category.

Category	**Personal Identifiers**
Examples	Name, alias, social security number, date of birth, driver's license, or state identification card number, Company ID number.
Disclosed To in Last 12 Months	• Financial institutions • Government agencies • Promotional or other fulfilment vendors • Marketing support vendors and vendors that support managing or hosting the website and the Chat function on the website • Communication providers/vendors that facilitate, manage, and send/receive communications on our behalf via email, text/SMS, or phone. • Lead providers (referral sources) • Transaction support vendors (e.g., check guaranty, payment processors) • Data analytics vendors • Social media platforms • Recruiting firms, and/or staffing agencies • Talent acquisition management systems, and other vendors providing services for purposes of our human resources information system (HRIS) and management of job applicant data and recruiting process. • Consulting and investigation firms, including HR consultants, safety consultants, and workplace investigators. • Security and risk management vendors, including IT, cybersecurity, and privacy vendors and consultants. • Insurance carriers, administrators, and brokers • Corporate customers (meaning an entity, as opposed to a natural person, that purchases, leases, or finances any of our products or services) • Original equipment manufacturers (OEM) (suppliers and makers of the products we sell or lease to our customers) • Human Resource Vendors we engaged to process this data
Sold To or Shared With	Not sold for monetary or other valuable consideration, and not shared for cross-context behavioral advertising.
Retention Period	Duration of our relationship with you plus 4 years. If you are a job applicant and are hired by the Company, then name will be retained permanently, and the rest will be retained for duration of employment plus 6 years. If you are <u>not</u> hired, this data will be retained for 4 years from when position is filled or the date we receive your information, whichever is longer.

Category	**Contact Information**
Examples	Home, postal or mailing address, email address, home phone number, cell phone number.
Disclosed To in Last 12 Months	• Financial institutions • Government agencies • Promotional or other fulfilment vendors • Marketing support vendors and vendors that support managing or hosting the website and the Chat function on the website.

	• Communication providers/vendors that facilitate, manage, and send/receive communications on our behalf via email, text/SMS, or phone. • Lead providers (referral sources) • Transaction support vendors (e.g., check guaranty, payment processors) • Data analytics vendors • Social media platforms • Recruiting firms, and/or staffing agencies • Talent acquisition management systems, and other vendors providing services for purposes of our human resources information system (HRIS) and management of job applicant data and recruiting process. • Consulting and investigation firms, including HR consultants, safety consultants, and workplace investigators. • Security and risk management vendors, including IT, cybersecurity, and privacy vendors and consultants. • Insurance carriers, administrators, and brokers • Corporate customers (meaning an entity, as opposed to a natural person, that purchases, leases, or finances any of our products or services) • Original equipment manufacturers (OEM) (suppliers and makers of Time and Labor products we sell or lease to our customers) • Human Resource Vendors we engaged to process this data
Sold To or Shared With	Not sold for monetary or other valuable consideration, and not shared for cross-context behavioral advertising.
Retention Period	Duration of our relationship with you plus 4 years. If you are a job applicant and are hired by the Company, then name will be retained permanently, and the rest will be retained for duration of employment plus 6 years. If you are <u>not</u> hired, this data will be retained for 4 years from when position is filled or the date we receive your information, whichever is longer.

Category	**Account Information**
Examples	Username and password for Company accounts and systems (including where a job applicant or candidate must create an account to apply for a job), and any required security or access code, password, security questions, or credentials allowing access to your Company accounts.
Disclosed To in Last 12 Months	Security and risk management vendors, including IT, cybersecurity, and privacy vendors and consultants.
Sold To or Shared With	Not sold for monetary or other valuable consideration, and not shared for cross-context behavioral advertising.
Retention Period	Username: permanent; Password or security code: while in use + 6 months or last 6-8 passwords used, whichever is longer

Category	**Protected Classifications**
Examples	Race, ethnicity, national origin, sex, gender, sexual orientation, gender identity, religious or philosophical beliefs, age, disability, medical or mental condition, military status, familial status, union membership.
Disclosed To in Last 12 Months	• Government Agencies • Talent acquisition management systems, and other vendors providing services for purposes of our human resources information system (HRIS) and management of job applicant data and recruiting process

	• Consulting and investigation firms, including HR consultants, safety, consultants, and workplace investigators. • Insurance carriers, administrators, and brokers • Corporate customers (meaning an entity, as opposed to a natural person, that purchases, leases, or finances any of our products or services) • Human Resource Vendors we engaged to process this data
Sold To or Shared With	Not sold for monetary or other valuable consideration, and not shared for cross-context behavioral advertising.
Retention Period	Duration of our relationship with you plus 4 years. This data is not collected from or about job applicants (unless required by law or government contract).

Category	**Commercial Transactional Data**
Examples	Information regarding products or services provided, purchasing history.
Disclosed To in Last 12 Months	• Promotional or other fulfilment vendors • Marketing support vendors and vendors that support managing or hosting the website and the Chat function on the website • Communication providers/vendors that facilitate, manage, and send/receive communications on our behalf via email, text/SMS, or phone. • Transaction support vendors (e.g., check guaranty, payment processors) • Consulting and investigation firms, including HR consultants, safety consultants, and workplace investigators • Security and risk management vendors, including IT, cybersecurity, and privacy vendors and consultants • Insurance carriers, administrators, and brokers • Corporate customers (meaning an entity, as opposed to a natural person, that purchases, leases, or finances any of our products or services) • Human Resource Vendors we engaged to process this data
Sold To or Shared With	Not sold for monetary or other valuable consideration, and not shared for cross-context behavioral advertising.
Retention Period	4 years after transaction, unless necessary to maintain for a longer period for product warranty, or OSHA / FDA / other regulatory compliance.

Category	**Biometric Data**
Examples	Fingerprints, facial recognition, handprint.
Disclosed To in Last 12 Months	Not disclosed other than to Original equipment manufacturers OEM (suppliers and makers of the Time and Labor products we sell or lease to our customers) , the vendor we engaged to process this data.
Sold To or Shared With	Not sold for monetary or other valuable consideration, and not shared for cross-context behavioral advertising.
Retention Period	While in use for identity verification, plus 1 year. Not collected from job applicants.

Category	**Credit/Financing Application Data**
Examples	Information collected through credit or financing applications, including employment history, company name, role, salary, dates of employment, bank accounts, income sources.
Disclosed To in Last 12 Months	• Financial institutions • Government agencies

	• Talent acquisition management systems, and other vendors providing services for purposes of our human resources information system (HRIS) and management of job applicant and recruiting process • Consulting and investigation firms, including HR consultants, safety consultants, and workplace investigators • Security and risk management vendors, including IT, cybersecurity, and privacy vendors and consultants • Insurance carriers, administrators, and brokers • Corporate customers (meaning an entity, as opposed to a natural person, that purchases, leases, or finances any of our products or services) • Human Resource Vendors we engaged to process this data
Sold To or Shared With	Not sold for monetary or other valuable consideration, and not shared for cross-context behavioral advertising.
Retention Period	4 years.

Category	**Internet Network and Computer Activity**
Examples	Date and time of your website visit; webpages visited; links clicked on the website; browser ID; browser type; device ID; operating system; form information downloaded; domain name from which our site was accessed; search history; cookies; internet or other electronic network activity information related to usage of Company networks, servers, intranet, or shared drives, as well as Company-owned computers and electronic devices, including system and file access logs, security clearance level, browsing history, search history, and usage history.
Disclosed To in Last 12 Months	• • Marketing support vendors and vendors that support managing or hosting the website and the Chat function on the website • Leader providers (referral sources) • Social media platforms • Security and risk management vendors, including IT, cybersecurity, and privacy vendors and consultants
Sold To or Shared With	Not sold for monetary or other valuable consideration, and not shared for cross-context behavioral advertising.
Retention Period	3 years

Category	**Mobile Device Data**
Examples	Information collected when you navigate, access, or use any of our websites via mobile device, including device type, software type; data identifying your device if you access our business networks and systems, including cell phone make, model, and serial number, cell phone number, and cell phone provider.
Disclosed To in Last 12 Months	• Promotional or other fulfilment vendors
Sold To or Shared With	Not sold for monetary or other valuable consideration, and not shared for cross-context behavioral advertising.
Retention Period	3 years

Category	Visual, Audio, or Video Recordings –
Examples	Your image when recorded or captured in surveillance camera footage or pictures of you taken on our premises or at our events or that you share with us; video and audio recordings of calls and virtual meetings as disclosed to you at the time of the call.
Disclosed To in Last 12 Months	•Communication providers/vendors •Security and risk management vendors, including IT, cybersecurity, and privacy vendors and consultants
Sold To or Shared With	Not sold for monetary or other valuable consideration, and not shared for cross-context behavioral advertising.
Retention Period	Duration of our relationship with you plus 4 years.

Category	Pre-Hire Information / Pre-Contract Information
Examples	Information gathered on job applicants and independent contractors as part of background screening, reference checks, pre-hire/contract drug test results, information gathered as part of vendor evaluation and other assessments of your qualifications to provide services to the Company, information recorded in job interview notes, information contained in candidate evaluation records and assessments, information in work product samples you provided, and voluntary disclosures by you.
Disclosed To in Last 12 Months	• Recruiting firms, and/or staffing agencies • Talent acquisition management systems, and other vendors providing services for purposes of our human resources information system (HRIS) and management of job applicant data and recruiting process
Sold To or Shared With	Not sold for monetary or other valuable consideration, and not shared for cross-context behavioral advertising.
Retention Period	Independent Contractors: Duration of our relationship with you plus 4 years. Job Applicants: If hired, this data will be retained for duration of employment plus 6 years. If not hired, it will be retained for 4 years from when position is filled or the date we receive your information, whichever is longer.

Category	Employment and Education History
Examples	Information contained in job applicants' resumes regarding educational history, information in transcripts or records of degrees, vocational certifications obtained, and information regarding prior job experience, positions held, and when permitted by applicable law your salary history or expectations.
Disclosed To in Last 12 Months	• Financial Institutions • Communication providers/ vendors • Lead providers • Social Media Platforms • Recruiting firms, and/or staffing agencies • Consumer reporting agencies or credit reporting agencies • Talent acquisition management systems, and other vendors providing services for purposes of our human resources information system (HRIS) and management of job applicant data and recruiting process • Consulting and investigation firms, including HR consultants, safety consultants, and workplace investigators • Security and risk management vendors, including IT, cybersecurity, and privacy vendors and consultants • Corporate customers

	• Human Resource Vendors we engaged to process this data
Sold To or Shared With	Not sold for monetary or other valuable consideration, and not shared for cross-context behavioral advertising.
Retention Period	If hired, this data will be retained for duration of employment plus 6 years. If not hired, it will be retained for 4 years from when position is filled or the date we receive your information, whichever is longer.

Category	**Professional Related Information**
Examples	Information on independent contractors contained in tax forms/1099 forms, safety records, licensing and certification records, and performance records, and information related to services provided by independent contractors, including in statements of work.
Disclosed To in Last 12 Months	• Financial institutions • Recruiting firms, and/or staffing agencies • Talent acquisition management systems, and other vendors providing services for purposes of our human resources information system (HRIS) and management of job applicant data and recruiting process
Sold To or Shared With	Not sold for monetary or other valuable consideration, and not shared for cross-context behavioral advertising.
Retention Period	Duration of our relationship with you plus 4 years.

Category	**Financial Information – Independent Contractors**
Examples	Information contained in invoices billed to the Company and in records of payments made to independent contractors by the Company, or other financial account information.
Disclosed To in Last 12 Months	• Financial institutions
Sold To or Shared With	Not sold for monetary or other valuable consideration, and not shared for cross-context behavioral advertising.
Retention Period	Duration of our relationship with you plus 4 years.

Category	**Facility & Systems Access Information –**
Examples	Information identifying you, if you accessed our secure company facilities, systems, networks, computers, and equipment, and at what times, using keys, badges, fobs, login credentials, or other security access method.
Disclosed To in Last 12 Months	Security and risk management vendors, including IT, cybersecurity, and privacy vendors and consultants
Sold To or Shared With	Not sold for monetary or other valuable consideration, and not shared for cross-context behavioral advertising.
Retention Period	3 years

Of the above categories of Personal Information, the following are categories of Sensitive Personal Information the Company may collect from or about consumers, independent contractors, or job applicants:

1. Personal Identifiers (social security number, driver's license or state identification card number, passport number)

2. Account Information (your Company account log-in, in combination with any required security or access code, password, or credentials allowing access to the account)
3. Protected Classifications (racial or ethnic origin, religious or philosophical beliefs, union membership, or sexual orientation)
4. Biometric Information (used for the purpose of uniquely identifying you)

Personal information ***does not*** include:

- Publicly available information from government records.
- Information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer, independent contractor, or applicant, or from widely distributed media.
- Information made available by a person to whom the consumer, independent contractor, or applicant has disclosed the information if the consumer, independent contractor, or applicant has not restricted the information to a specific audience.
- Deidentified or aggregated information.

We may collect your personal information from the following sources:

- You the consumer, independent contractor, or job applicant, when you visit the website and voluntarily submit information through forms on the website or social media, when you visit any of our stores or physical locations, when you purchase or inquire about any of our products or services, when you utilize the Chat feature on the website, when you enter into a contract to perform services for us, or when you apply for a position of employment
- Our employees, contractors, vendors, suppliers, guests, visitors, other consumers, and customers based on your interactions with them (if any)
- We utilize cookies to automatically collect information about our website visitors
- Surveillance cameras at our physical locations
- Lead generators and referral sources
- Credit and consumer reporting agencies
- HR support vendors
- Social media platforms
- Career sites or platforms like LinkedIn, Indeed, and JazzHR
- Company-issued computers, electronic devices, and vehicles
- Company systems, networks, software applications, and databases you log into or use
- Company systems, networks, software applications, and databases you log into or use in the course of applying for a position with the Company, interacting with our website, or otherwise interacting with us in any other capacity, including from vendors the Company engages to manage or host such systems, networks, applications or databases
- Personal references and former employers (if you are a job applicant)
- Schools, universities, or other educational institutions which you attended (if you are a job applicant)
- From friends, family, or colleagues who choose to email you job postings that they think you may be interested in from our application platform or careers page
- Third party customer databases

We may disclose, sell, or share your personal information to/with the following categories of service providers, contractors, or third parties:

- Financial institutions
- Government agencies
- Promotional or other fulfilment vendors

- Marketing support vendors and vendors that support managing or hosting the website and the Chat function on the website
- Communication providers/vendors that facilitate, manage, and send/receive communications on our behalf via email, text/SMS, or phone.
- Lead providers (referral sources)
- Transaction support vendors (e.g., check guaranty, payment processors)
- Data analytics vendors
- Social media platforms
- Consumer reporting agencies or credit reporting agencies
- Recruiting firms, and/or staffing agencies
- Talent acquisition management systems, and other vendors providing services for purposes of our human resources information system (HRIS) and management of job applicant data and recruiting process
- Consulting and investigation firms, including HR consultants, safety consultants, and workplace investigators
- Security and risk management vendors, including IT, cybersecurity, and privacy vendors and consultants
- Insurance carriers, administrators, and brokers
- Corporate customers (meaning an entity, as opposed to a natural person, that purchases, leases, or finances any of our products or services)
- Original equipment manufacturers (OEM) (suppliers and makers of the products we sell or lease to our customers)

We may collect and disclose your personal information for any of the following business purposes:

1. To fulfill or meet the purpose for which you provided the information.
2. To process and submit financing applications, including to apply for credit, or credit pre-qualification.
3. To process, complete, and maintain records on transactions.
4. To provide warranty coverage on products and services.
5. To retain your selection for Text opt in/opt out to ensure customers who opted out are not sent any text messages.
6. To provide and communicate recall notifications to customers.
7. To schedule, manage and keep track of customer appointments.
8. To complete appraisals.
9. To maintain records of when customers decline a service or sale.
10. To respond to consumer inquiries, including requests for information, customer support online, Chat on the website, phone calls, and in-store inquiries.
11. To provide interest-based and targeted advertising.
12. To contact you by email, telephone calls, mail, SMS, or other equivalent forms of communication regarding updates or informative communications related to the functionalities, services, or other information you requested or asked the Company to provide to you.
13. To improve user experience on our website.
14. To understand the demographics of our website visitors.
15. To detect security incidents.
16. To debug, identify, and repair errors that impair existing intended functionality of our website.
17. To protect against malicious or illegal activity and prosecute those responsible.
18. To verify and respond to consumer requests.
19. To prevent identity theft.
20. **JOB APPLICANT PURPOSES:**

a. To fulfill or meet the purpose for which you provided the information. For example, if you share your name and contact information to apply for a job with the Company, we will use that Personal Information in connection with your candidacy for employment.
b. To comply with local, state, and federal law and regulations requiring employers to maintain certain records, as well as local, state, and federal law, regulations, ordinances, guidelines, and orders relating to infectious diseases, pandemics, outbreaks, and public health emergencies, including applicable reporting requirements.
c. To evaluate your job application and candidacy for employment.
d. To obtain and verify background check and references.
e. To communicate with you regarding your candidacy for employment.
f. To permit you to create a job applicant profile, which you can use for filling out future applications if you do not get the job you are apply for.
g. To keep your application on file even if you did not get the job applied for, in case there is another position for which we want to consider you as a candidate even if you do not formally apply.
h. To evaluate and improve our recruiting methods and strategies.
i. To engage in lawful monitoring of job applicant activities and communications when they are on Company premises, or utilizing Company internet and WiFi connections, computers, networks, devices, software applications or systems.
j. To engage in corporate transactions requiring review or disclosure of job applicant records subject to non-disclosure agreements, such as for evaluating potential mergers and acquisitions of the Company.
k. To evaluate, assess, and manage the Company's business relationship with vendors, service providers, and contractors that provide services to the Company related to recruiting or processing of data from or about job applicants.
l. To improve job applicant experience on Company computers, networks, devices, software applications or systems, and to debug, identify, and repair errors that impair existing intended functionality of our systems.
m. To reduce the risk of spreading infectious diseases in or through the workplace.

21. **INDPENDENT CONTRACTOR AND BUSINESS-TO-BUSINESS PURPOSES:**
a. To fulfill or meet the purpose for which you provided the information.
b. To comply with state and federal law and regulations requiring businesses to maintain certain records (accident or safety records, and tax records/1099 forms).
c. To engage the services of independent contractors and compensate them for services.
d. To evaluate, make, and communicate decisions regarding an independent contractor, including decisions to hire and/or terminate.
e. To grant independent contractors access to secure Company facilities, systems, networks, computers, and equipment, and maintain information on who accessed such facilities, systems, networks, computers, and equipment, and what they did therein or thereon.
f. To implement, monitor, and manage electronic security measures on independent contractor devices that are used to access Company networks and systems.
g. To evaluate, assess, and manage the Company's business relationship with vendors, service providers, and contractors that provide services to the Company.
h. To improve user experience on Company computers, networks, devices, software applications or systems, and to debug, identify, and repair errors that impair existing intended functionality of our systems.
i. To reduce the risk of spreading infectious diseases in or through the workplace.

22. **INFECTIOUS DISEASE PURPOSES (pandemic, outbreak, public health emergency, etc.):**
a. To reduce the risk of spreading infectious diseases in or through the workplace.
b. To protect job applicants, independent contractors, and other consumers from exposure to infectious diseases (e.g., COVID-19).

c. To comply with local, state, and federal law, regulations, ordinances, guidelines, and orders relating to infectious diseases, pandemics, outbreaks, and public health emergencies, including applicable reporting requirements.
d. To facilitate and coordinate pandemic-related initiatives and activities (whether Company-sponsored or through the U.S. Center for Disease Control and Prevention, other federal, state and local governmental authorities, and/or public and private entities or establishments, including vaccination initiatives).
e. To identify potential symptoms linked to infectious diseases, pandemics, and outbreaks (including through temperature checks, antibody testing, or symptom questionnaire).
f. To permit contact tracing relating to any potential exposure to infectious diseases.
g. To communicate with job applicants, independent contractors, and other consumers regarding potential exposure to infectious diseases (e.g., COVID-19) and properly warn others who have had close contact with an infected or symptomatic individual so that they may take precautionary measures, help prevent further spread of the virus, and obtain treatment, if necessary.

We do NOT and will not sell your personal information in exchange for monetary or other valuable consideration. We do not share your personal information for cross-context behavioral advertising.

We do not and will not use or disclose your sensitive personal information for purposes other than the following:

1. To perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services.
2. To detect security incidents that compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted personal information.
3. To resist malicious, deceptive, fraudulent, or illegal actions directed at the business and to prosecute those responsible for those actions.
4. To ensure the physical safety of natural persons.
5. For short-term, transient use.
6. To perform services on behalf of the Company.
7. To verify or maintain the quality or safety of a product, service or device that is owned, manufactured, manufactured for, or controlled by the Company, and to improve, upgrade, or enhance the service or device that is owned, manufactured by, manufactured for, or controlled by the Company.
8. For purposes that do not involve inferring characteristics about consumers, contractors, and job applicants.

Retention of Personal Information

We will retain each category of Personal Information in accordance with our established data retention schedule as indicated above. Some of the retention periods in the retention schedule above are measured from a particular point in time that has not occurred yet, such as the end of employment or end of a relationship (whether business, contractual, or transactional) plus a certain number of years. Where no particular event is defined in the retention schedule as the point from which the retention period is measured, we will measure the retention period from either: (1) the date the record or data was collected, created, or last modified; (2) the date of the particular transaction to which the record or data pertains; or (3) another triggering event that is determined to be reasonable and appropriate based on the nature of the data and the legal/business needs for its continued use.

In deciding how long to retain each category of personal information that we collect, we consider many criteria, including, but not limited to: the business purposes for which the Personal Information was collected; relevant federal, state and local recordkeeping laws; applicable statutes of limitations for claims to which the information may be relevant; and legal preservation of evidence obligations.

We apply our data retention procedures on an annual basis to determine if the business purposes for collecting the personal information, and legal reasons for retaining the personal information, have both expired. If so, we will purge the information in a secure manner.

Third Party Vendors

We may use other companies and individuals to perform certain functions on our behalf. Examples include administering e-mail services and running special promotions. Such parties only have access to the personal information needed to perform these functions and may not use or store the information for any other purpose. Subscribers or site visitors will never receive unsolicited e-mail messages from vendors working on our behalf.

Accountability of Onward Transfer Principle

In the context of an onward transfer, ExtensisHR has responsibility for the processing of personal information it receives under the DPF Principles and subsequently transfers to a third party acting as an agent on its behalf. ExtensisHR shall remain liable under the DPF Principles if its agent processes such personal information in a manner inconsistent with the DPF Principles, unless the ExtensisHR proves that it is not responsible for the event giving rise to the damage.

Business Transfers

In the event we sell or transfer a particular portion of our business assets, information of consumers, contractors and applicants may be one of the business assets transferred as part of the transaction. If substantially all of our assets are acquired, information of consumers, contractors and applicants may be transferred as part of the acquisition.

Compliance with Law and Safety

We may disclose specific personal and/or sensitive personal information based on a good faith belief that such disclosure is necessary to comply with or conform to the law or that such disclosure is necessary to protect our employees or the public.

Use of Cookies, Pixels, and Other Tracking Technologies

Cookies are small files that a website may transfer to a user's computer that reside there for either the duration of the browsing session (session cookies) or on a permanent, until deleted, basis (persistent cookies) that may be used to identify a user, a user's machine, or a user's behavior. We make use of cookies under the following circumstances and for the following reasons:

- Provide you with services available through the website and to enable you to use some of its features
- Authenticate users and prevent fraudulent use of user accounts
- Identify if users have accepted the use of cookies on the website
- Compile data about website traffic and how users use the website to offer a better website experience
- Understand and save visitor preferences for future visits, such as remembering your login details or language preference, to provide you with a more personal experience, or to avoid you having to re-enter your preferences every time you use the website

- Track your browsing habits to enable us to show advertising which is more likely to be of interest to you, including advertising by third parties on our website

You may delete cookies from your web browser at any time or block cookies on your equipment, but this may affect the functioning of or even block the website. You can prevent saving of cookies (disable and delete them) by changing your browser settings accordingly at any time. It is possible that some functions will not be available on our website when use of cookies is deactivated. Check the settings of your browser. Below you can find some guidance:

- Safari
- Opera
- Internet Explorer
- Google Chrome
- Mozilla

Do Not Track (DNT) is a privacy preference that users can set if they do not want web services to collect information about their online activity. We do not respond to DNT signals.

External Links

Our website contains links to other sites. We are not responsible for the privacy practices or the content of such websites. To help ensure the protection of your privacy, we recommend that you review the Privacy Policy of any site you visit via a link from our website.

Passwords

The personal data record created through your registration with our website can only be accessed with the unique password associated with that record. To protect the integrity of the information contained in this record, you should not disclose or otherwise reveal your password to third parties.

Children Under the Age of 16

We do not knowingly sell or share the personal information of consumers under 16 years of age.

However, we do not sell or share personal information collected from children at least 13 years of age and less than 16 years of age without receiving a request to opt-in to the selling or sharing of personal information from such children.

When we receive a request to opt-in to the selling or sharing of personal information from a child at least 13 years of age and less than 16 years of age, we will inform the child of their ongoing right to opt-out of the selling or sharing of their personal information at any point in the future and the process for doing so as provided for by the Notice of Right to Opt-Out of Selling and Sharing.

How We Protect the Information that We Collect

The protection of the information that we collect about visitors to our websites is of the utmost importance to us and we take every reasonable measure to ensure that protection, including:

- We keep automatically collected data and voluntarily collected data separate at all times.

- We use internal encryption on all data stores that house voluntarily captured data.

- We use commercially reasonable tools and techniques to protect against unauthorized access to our systems.

- We restrict access to private information to those who need such access in the course of their duties for us.

International Visitors

We do not target, market to, or offer our products or services to consumers outside of the United States. You agree not to submit your personally identifiable information through the website if you reside outside the United States.

Rights Under the CCPA and CPRA

This section of the Privacy Policy applies only to California residents who are natural persons. If you are a California resident, you have the following rights pursuant to the California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA):

1. Right to Know. The right to request, up to 2 times in a 12-month period, that we identify to you (1) the categories of personal information we have collected about you going back to January 1, 2022, unless doing so would be impossible or involve disproportionate effort, or unless you request a specific time period, (2) the categories of sources from which the personal information was collected, (3) the business or commercial purpose for collecting, selling, or sharing this information (6) the categories of personal information that we have disclosed about you for a business purpose and the categories of persons to whom it was disclosed for a business purpose;

2. Right to Access. The right to request, up to 2 times in a 12-month period, that we disclose to you, free of charge, the specific pieces of personal information we have collected about you going back to January 1, 2022, unless doing so would be impossible or involve disproportionate effort, or unless you request a specific time period;

3. Right to Delete. The right to request, up to 2 times in a 12-month period, that we delete personal information that we collected from you, subject to certain exceptions;

4. Right to Correct. The right to request that we correct inaccurate personal information (to the extent such an inaccuracy exists) that we maintain about you;

5. The right to designate an authorized agent to submit one of the above requests on your behalf. See below for how you can designate an authorized agent; and

6. The right to not be discriminated or retaliated against for exercising any of the above rights, including an applicant's and independent contractor's right not to be retaliated against for exercising the above rights.

How We Will Verify That it is Really You Submitting the Request

If you are a California resident, when you submit a Right to Know, Right to Access, Right to Delete, or Right to Correct request through one of the methods provided above, we will ask you to provide some information in order to verify your identity and respond to your request. Specifically, we will ask you to verify information that can be used to link your identity to particular records in our possession, which depends on the nature of your relationship and interaction with us.

Responding to Your Right to Know, Right to Access, Right to Delete, and Right to Correct Requests

Upon receiving a verifiable request from a California resident, we will confirm receipt of the request no later than 10 business days after receiving it. We endeavor to respond to a verifiable request within 45 calendar

days of its receipt. If we require more time (up to an additional 45 calendar days, or 90 calendar days total from the date we receive your request), we will inform you of the reason and extension period in writing. We will deliver our written response by mail or electronically, at your option. The response we provide will also explain the reasons we cannot comply with a request, if applicable.

We do not charge a fee to process or respond to your verifiable 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.

For a request to correct inaccurate personal information, we will accept, review, and consider any documentation that you provide, and we may require that you provide documentation to rebut our own documentation that the personal information is accurate. You should make a good-faith effort to provide us with all necessarily information at the time that you make the request to correct. We may deny a request to correct if we have a good-faith, reasonable, and documented belief that a request to correct is fraudulent or abusive. If we deny your request to correct, we shall inform you of our decision not to comply and provide an explanation as to why we cannot comply with a request, if applicable. **If You Have an Authorized Agent:**

If you are a California resident, you can authorize someone else as an authorized agent who can submit a request on your behalf. To do so, you must either: (a) execute a valid, verifiable, and notarized power of attorney; or (b) provide other written, signed authorization that we can then verify. When we receive a request submitted on your behalf by an authorized agent who does not have a power of attorney, that person will be asked to provide written proof that they have your permission to act on your behalf, and we will also contact you and ask you for information to verify your own identity directly with us and not through your authorized agent. We may deny a request from an authorized agent if the agent does not provide your signed permission demonstrating that they have been authorized by you to act on your behalf.

Other California Privacy Rights

The California Civil Code permits California residents with whom we have an established business relationship to request that we provide you with a list of certain categories of personal information that we have disclosed to third parties for their direct marketing purposes during the preceding calendar year. To make such a request, please send an email]PrivacyPolicy@extensishr.com, or write to us at the address listed below. Please mention that you are making a “California Shine the Light” inquiry.

Consent to Terms and Conditions

By using this website, you consent to all terms and conditions expressed in this Privacy Policy.

Changes to Our Privacy Policy

As our services evolve and we perceive the need or desirability of using information collected in other ways, we may from time to time amend this Privacy Policy. We encourage you to check our website frequently to see the current Privacy Policy in effect and any changes that may have been made to them. If we make material changes to this Privacy Policy, we will post the revised Privacy Policy and the revised effective date on this website. Please check back here periodically or contact us at the address listed at the end of this Privacy Policy.

Consumers With Disabilities

This policy is in a form that is accessible to consumers with disabilities.

Questions About the Policy

This website is owned and operated by ExtensisHR If you have any questions about this Privacy Policy, please contact us at PrivacyPolicy@extensishr.com or call 888-473-6398

This policy was last updated July 9, 2024.