

Contents

General Principles for Processing of Personal Information 1

What Personal Information We Collect..... 2

How We Collect Personal Information 3

How We Use Information We Collect..... 4

Marketing Purposes 8

Who We Share Information With..... 8

Cross Border Data Transfer 10

Cookies and Similar Technology 11

Third Party Tracking and Online Advertising..... 11

Your Choices..... 12

Social Media Features 13

Security of Personal Information..... 13

Retention Period 13

Additional Provisions Children 14

Sensitive Information..... 14

Your Rights Regarding your Personal Information..... 14

Your Consent and Changes 15

Updates to This Privacy Statement 16

Contact Us 16

Local Specific Supplementing Notices 16

California Privacy Rights 16

Your Right To Object..... 18

International Data Transfers..... 18

Google Analytics 4 – Websites in the European Economic Area 19

Third Country Transfer 20

General Principles for Processing of Personal Information

This Privacy Statement is effective as of June 8, 2023. If you would like to review a previous version of this Privacy Statement, please contact us at Privacy@exitcertified.com.

The following is an explanation of how ExitCertified Corporation process (e.g.: collect, use, store, process, disclose and delete) your personal information.

ExitCertified recognizes the importance of privacy, security and data protection to our customers and partners worldwide.

This Privacy Statement informs you about our privacy practices and the choices you may make and the rights you may exercise in relation to your personal information that we collect about you when visiting or using ExitCertified websites, applications, and services (collectively, the “Services”). If you have questions or concerns regarding this Privacy Statement or our handling of your information collected under this Privacy Statement, contact Privacy@exitcertified.com.

What Personal Information We Collect

Personal information is information that directly identifies you or information otherwise defined as “personally identifiable” or “personal” under applicable law. This includes, but is not limited to:

- **Identity Data** first name, surname, last name, username or similar identifier, and title.
- **Business Contact Data** billing address, delivery address, (business) email address and (business) telephone numbers.
- **Personal Contact Data** home address
- **Financial Data** bank account, payment card details and credit history.
- **Transaction Data** details about payments to and from you and other details of products and services you have purchased from us.
- **Technical Data** internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access our websites.
- **Profile Data** your username and password, purchases or orders made by you, your role within your organization, interests, preferences, feedback and survey responses.
- **Usage Data** information about how you use our websites, products and services and how your device has interacted with our website, including the pages accessed and links clicked.
- **Preference Data** your preferences in receiving marketing from us and our third parties, your communication preferences, and dietary information.
- **Pictures/video or acoustical recordings** from live or virtual events or other video recordings (such as CCTV at our offices and warehouses).
- **Communication content** from your email, chat or otherwise written communication.

We also collect, use and share aggregated data such as statistical or demographic data for any purpose. Aggregated data may be derived from your personal information but is not considered personal information under applicable regulations as this data does not directly or indirectly reveal your identity. For example, we may aggregate your usage data to calculate the percentage of users accessing a specific website feature. However, if we combine or connect aggregated data with your personal information so that it can directly or indirectly identify you, we treat the combined data as personal information which will be used in accordance with this Privacy Statement.

How We Collect Personal Information

Directly From You. ExitCertified may collect personal information you provide directly to us via websites, mobile applications, email, EDI, by corresponding with us via telephone or post and other interactions. For example, we may collect personal information when you register with us as a customer, place an order for product or services, participate in promotional activities, use an application installed on a device, post on our Services, visit our premises or subscribe to notifications. When you visit our offices or warehouse, we may also obtain your personal information from the CCTV camera on the premises. Such video recordings are stored in line with local requirements. The purpose of the video recordings is the protection of our property, prevention and detection of criminal activity, legal enforcement and the protection of the health and safety of our employees and customers.

Automatically Collected from Your Use of our Services. ExitCertified may automatically collect personal information for business-related purposes, such as providing customer service, managing the Services we provide, complying with legal requirements, payment processing, and for marketing our products and Services.

When you visit our websites, we may automatically collect information about which of our websites you are visiting, your equipment, the browser you are using, as well as browsing actions and patterns including the pages accessed and links clicked. In some countries, including countries in the European Economic Area, this information may be considered personal information under applicable data privacy laws. Some of this information will be stored anonymously, and we will use it to improve our Services and to make our websites more user-friendly as well as for statistical purposes.

Some of this information may be collected using cookies and similar technology as further outlined in the section [Cookies and Similar Technology below](#). We may also receive technical data about you if you visit other websites employing our cookies.

Collecting this information enables us to better understand the visitors who come to our website, where they come from, and what content on our website is of interest to them. We use this information for our internal analytics purposes and to improve the quality and relevance of our website to our visitors.

Publicly available. ExitCertified may collect personal information from publicly available sources, including, but not limited to, public internet websites and databases, public or government sources, and news media.

Third Parties. We may obtain personal information from third parties that have obtained or collected information about you and that have the right to provide that personal information to us.

Business Partners. We may receive information about you from others within your organization, or from our business partners we work with to provide our products and services. For example, we may obtain information about you from the resellers that purchase offerings available from us and provide such offerings to you or your organization.

Third Party Information Provider. ExitCertified may contract with third parties who provide information to businesses to verify certain information about you or obtain information about you, for example analytics providers, advertising networks and marketing companies, search information

providers, credit reference, fraud prevention, anti-money laundering or government agencies, providers of technical, payment and delivery services, data brokers or aggregators. We may use the personal information received from a third party in accordance with the terms established between ExitCertified and the third party.

How We Use Information We Collect

We collect personal information from and about you for a variety of purposes. For example, we use personal information to fulfill your requests, process your transactions and provide our Services to you; to communicate with you; for marketing and advertising purposes; to monitor, improve, and develop our products and Services; and to protect the security and integrity of our business, comply with legal requirements and obligations; for our business and operational purposes; and as otherwise permitted or required by law.

The table below sets forth the reasons why we process your personal information, the associated legal basis we rely on to legally process your personal information, and the categories of personal information (identified in Section 4 “Personal Information we collect from you”).

In regions where legitimate interest is not supported as legal basis for processing, we typically rely on your consent and agreement to the processing as described in this Privacy Statement unless our legal basis for the processing is compliance with a legal obligation or performance of a contract/transactional relationship.

Processing Purpose	Type of data	Legal basis for processing including basis of legitimate interest
To manage our relationship with you as a business partner including to register you as a new customer, to determine credit limits, contracting and enforcing our terms and conditions and other principles as well as this Privacy Statement, notifying you about changes to our terms or other operational (non-marketing) information required by law or otherwise operationally necessary	Identity, Contact, Financial, Transaction, Profile, Preference	Performance of a contract with you Legal obligation Legitimate Interest (to safeguard the legal and financial position of ExitCertified and successful operations, for example, product recall notices, or relevant information relating to your orders)
To process our transactions including to process and delivering your orders, to provide our Services, to verify completeness and accuracy of your /or your customers address data, to manage payments, fees and charges, to collect and recover account receivables as well as RMA management	Identity, Contact, Financial; Transaction, Profile, Preference	Performance of a contract with you Legitimate Interest (necessary to ensure the quality of our Services, and the successful operations and processing of the transaction and to pursue our legal rights)

For the establishment, exercise or defense of legal claims	Identity, Contact, Financial; Transaction, Profile, Pictures/video or acoustical recordings	Legitimate Interest (to safeguard and pursue the legal and financial position of ExitCertified)
To provide general customer services, including to maintain and support your customer account, to collect and manage your preferences regarding i.e., marketing communication and / or cookies, to communicate with you by phone or email	Identity, Contact, Financial, Transaction, Technical, Profile,	Performance of a contract Legal obligation Legitimate Interest (necessary to ensure the quality and improvement of our Services, successful operations and processing of transactions)
To respond to customer service inquiries, to respond to refund requests and complaints, to discuss issues relating to your account or the website, and to provide customer support.	Preference	
To register, maintain and refer to you as contact and, in your role, acting for the business partner you are working for	Identity, Contact, Profile, Preference	Necessary for our and our business partner's legitimate interests to help, maintain and manage the business relationship with our business partners and to provide general customer services
To plan, administer and protect our business and websites (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)	Identity Contact Technical	Legal obligation Necessary for our legitimate interests (for running our business safely, provision of administration and IT services, network security, to prevent fraud and other illegal activities and in the context of a business reorganization or group restructuring exercise)
To conduct research, contests, surveys and sweepstakes	Identity Contact Profile Usage Preference Technical	Performance of a contract with you Consent Necessary for our legitimate interests (to study how customers use our products/services, to develop them and grow our business)
To de-personalize data for statistical and analytical purposes	Identity Contact Profile Usage Preference Transaction Technical	Legitimate interest (to grow our business, to develop business strategies and generate new business opportunities)

<p>In order to measure the effectiveness of our advertising and to better understand your and your organization’s purchasing focus, interests, expertise, your role in your organization and general areas of business interests of your organization, we aggregate, match and/or compare data from different data sources using data analytics and applying artificial intelligence</p>	<p>Identity Contact Technical Transaction Profile Usage Preference</p>	<p>Legitimate interest (to grow our business, to develop a successful marketing strategy and effective advertising that is customized to the individual interests of the recipients who have consented / not opted out to receive marketing communication)</p>
<p>To deliver relevant website content and advertisements to you and measure or understand the effectiveness of the advertising we serve to you</p>	<p>Identity Contact Profile Usage Preference Technical</p>	<p>Consent Necessary for our legitimate interests (to study how customers use our products/services, to develop them, to grow our business and to inform our marketing strategy)</p>
<p>To facilitate, manage, personalize and improve your online experience, our products and services and our marketing customer relation by using data analytics</p>	<p>Technical Usage</p>	<p>Consent if required for setting cookies or using third party analytics as to our cookie information Necessary for our legitimate interests (to define types of customers for our products and services, to keep our website updated and relevant, to develop our business and to inform our marketing strategy)</p>
<p>To provide services in connection with marketing campaigns to you including events, webinars and whitepapers</p>	<p>Identity Contact Profile Usage Preference Pictures/Video</p>	<p>Consent with respect to event videos or pictures or direct marketing Performance of a contract Necessary for our legitimate interests (to grow our business)</p>
<p>To enable third party direct marketing communications, for example, from our vendor partners</p>	<p>Identity Contact Profile Usage Preference</p>	<p>Consent</p>
<p>To help advertisers and publishers serve and manage ads on the website or on third-party sites, and to tailor ads based on your interests and browsing histories.</p>	<p>Identity Contact Profile Usage Preference</p>	<p>Please see the section on Cookies and Other Website Usage Information for additional information related to such advertising and your related controls.</p>
<p>For marketing, promotion and advertising purposes</p>	<p>Identity Contact Technical Profile</p>	<p>Consent Legitimate interest (to grow our business)</p>

<p>To discover any criminal activity or alleged criminal activity through fraud monitoring and suspicious transaction monitoring.</p>	<p>Identity Contact Transaction Technical Usage Profile Financial</p>	<p>Necessary for our legitimate interests (for the purposes of preventing or detecting unlawful acts)</p>
<p>To comply with our contractual or legal obligations to share data with credit reference, fraud prevention agencies and law enforcement agencies and screen against denied party lists.</p>	<p>Identity Contact Transaction Technical Financial</p>	<p>Legal obligation Necessary for our legitimate interests (to protect our business by preventing financial crime and to comply with legal obligations of ExitCertified organization not directly applying to the ExitCertified affiliate)</p>
<p>To comply with our internal requirements or contractual obligations, specially to verify transactional compliance, for example in the context of marketing funding, incentives, end user specific price promotions</p>	<p>Identity Contact Transaction Usage Profile Financial</p>	<p>Legal obligation Necessary for our legitimate interests (to protect our business by preventing financial crime and grey market activities)</p>
<p>To discover any criminal activity or alleged criminal activity through fraud monitoring and suspicious transaction monitoring including denied party list screening, monitoring or recording of emails and text messages, social media messages and other communications (including under specific circumstances telephone calls) in relation to your dealings with us.</p>	<p>Identity Contact Transaction Technical Usage Profile Financial</p>	<p>Legal obligation Necessary for our legitimate interests (for preventing or detecting unlawful and inappropriate acts and securing ExitCertified legal position, to protect the security of our communications systems and procedures, and to comply with legal obligations applying to ExitCertified as an organization)</p>
<p>To assess the quality of our customer services and to provide staff training</p>	<p>Identity Contact Transaction Usage Profile</p>	<p>Consent Legitimate Interest (To maintain and improve our Services)</p>
<p>Comply with a legal obligation or respond to lawful requests by public authorities (including national security or law enforcement requirements)</p>	<p>Identity Contact Transaction Technical Usage Profile Financial</p>	<p>Legal obligation Legitimate interest (if the legal obligations applies to the ExitCertified organization but not to the relevant ExitCertified affiliates)</p>

To expand and operate our business operations, such as mergers and acquisitions, reorganizations, or other disposition of all or part of our business, assets or stock, factoring of receivables.	Identity Contact Transaction Technical Profile Financial	Legitimate interest (to develop and grow our organization)
To control and manage our facilities and premises, including video recordings	Identity Contact Pictures/video	Legitimate interest (the protection of our property, prevention and detection of criminal activity and the protection of the health and safety of our employees and customers)

Marketing Purposes

We may use, combine, and enhance your information (especially identity, contact, technical, usage and profile data) from different data sources and apply certain business intelligence to better understand your role, your preferences and form a view on which offers and opportunities we think may be of interest for you in your professional function. This is done by evaluating data to identify patterns in usage and purchasing behavior. We may use certain algorithms in this regard which by means of automated decision provide you with marketing information being relevant to you in the context of your organization, provided you haven't opted out to receive this information.

If you are a user from the United States, ExitCertified may use your personal information for direct marketing purposes. You may unsubscribe from marketing emails by following the unsubscribe instructions contained in such emails, or you may contact us at Privacy@exitcertified.com if you do not want your personal information to be used for these purposes.

If you are a user from outside of the United States, you will receive marketing communications from us if you have requested information from us, if you have set your preferences accordingly, if you purchased goods or services from us, or if you provided us with your details when you entered a competition or registered for a promotion and, in each case, you have not opted out of receiving that marketing.

Who We Share Information With

We share your personal information with your consent or as necessary to complete any transaction or provide any product or service you have requested or authorized. We also share personal information with third- party vendors, resellers and distributors, third-party service providers, affiliates, and business units, with insurers, financial institutes, banks, consultants or law firms, when required by law or to respond to legal process, to protect our customers, to protect lives, to maintain the security of our services, for enforcement and defense of claims and to protect the rights or property of ExitCertified.

We may disclose your Personal Information as follows:

Vendors. ExitCertified may share Personal information about you with the third-party vendors that make offerings available through us. For example, we may share your personal information with a

third-party vendor if you purchase or access a service through us, or a ExitCertified reseller, and that vendor requires verification of a purchase to register that service. We may also share your personal information with a third-party vendor if that vendor co-sponsors a marketing activity with us to verify your participation in the marketing activity.

Resellers. ExitCertified may share your personal information with the resellers that purchase offerings from us. For example, we may share your personal information if you purchase or access an offering through a reseller, and that reseller leveraged our reseller tools and services.

Third-party Service Providers. ExitCertified may provide your personal information to third-parties that provide services, including but not limited to customer service, payment processing, email and messaging support, hosting, management, maintenance, information analysis, offering fulfillment or delivery, or other services we may receive on an outsourced basis. When we outsource data processing activities to a Third-Party Service Provider processing data on our behalf we follow a supplier due diligence protocol, and data processing by the supplier will be governed by documented terms. We will endeavor to require that these third parties use your personal information only as necessary for such reasons and protect your personal information consistent with this Privacy Statement and applicable law.

Affiliates and Business Units. ExitCertified may share your personal information with our affiliates, regardless of whether these entities share the ExitCertified brand. We may also share your personal information with other business units that also offer products or services under the ExitCertified brand or one of our other brands. Our affiliates and business units will use your personal information we share with them in a manner consistent with this Privacy Statement.

Other Users. ExitCertified may share your personal information with other users when you elect to interact with those users (or request that we communicate with them on your behalf) through the website. This may include facilitating communications with other users or enabling posting of personal information to areas of the website accessible by other users. You should be aware that any personal information (or other information) you provide in these areas may be read, collected, and used by others who access them.

Law Enforcement and Safety. ExitCertified may share your personal information with any competent law enforcement, regulatory, government agency, court, other governmental officials, or other third-party where we believe disclosure is necessary (i) as a matter of applicable law or regulation, (ii) to exercise, establish or defend our legal rights, or (iii) to protect your vital interests or those of any other person.

Sale or Acquisition of Assets. If ExitCertified transfers ownership or control of any portion of ExitCertified to an actual or potential buyer, whether in the context of an acquisition, merger, reorganization, or other disposition of all or any portion of our business, assets, or stock (including in connection with any bankruptcy or similar proceedings including financing or granting related security interest), we may transfer your personal information to that actual or potential buyer, provided that the use of your personal information by that third-party remains subject to applicable law.

Others. We may share your personal information with any other person with your consent to the disclosure.

We may also share aggregated, anonymized data with third parties for other purposes. Such information does not identify you individually, but may include usage, viewing and technical information we collected through your use of our website. If we are required under applicable law to treat such information as personal information, then we will only disclose it as described above. Our agents, vendors, consultants, marketing service providers, and other service providers including other ExitCertified companies may receive, or be given access to your information, including personal information and usage information, in connection with their work on our behalf.

Credit reference and legal compliance checks. The personal information that we have collected from you when setting up an account may be shared with credit reference, anti-bribery, anti-money laundering and fraud prevention agencies who use it to prevent fraud, anti-bribery and money laundering and to verify your identity.

We may access and use information from credit reference agencies and other third parties when you open your account and periodically to:

- manage and take decisions about your account, including assessing your creditworthiness.
- prevent criminal activity, fraud, and money laundering.
- check your identity and verify the accuracy of the information you provide to us; and
- trace debtors and recover debts.

We will continue to share information with credit reference agencies about how you manage your account, including any default in making payments, while you have a relationship with us. This information will be made available to other organizations so that they can make decisions about you.

If false or inaccurate information is provided and/or fraud is identified or suspected, details will be passed to fraud prevention agencies, law enforcement agencies and other organizations may access and use this information.

If we, or a fraud prevention agency, determine that you pose a fraud or money laundering risk, we may refuse to provide services to you.

A record of any fraud or money laundering risk will be retained by the fraud prevention agencies and may result in others refusing to provide services or financing to you. Fraud prevention agencies can hold your information for different periods of time.

When credit reference and fraud prevention agencies process your information, they do so based upon their own legal basis which may include a legitimate interest in preventing fraud and money laundering, and to verify identity, to protect their business and to comply with laws that apply to them.

Cross Border Data Transfer

ExitCertified is headquartered in the United States, with customers throughout the world. As such, your personal information may be transferred to and processed in regions other than the region you are resident in and/or the region where the data was originally collected. These regions may not ensure a level of protection for personal information equivalent to the laws applied in your region. We implement appropriate measures for the transfer in compliance with applicable law to ensure an adequate level of data protection of personal information.

Cookies and Similar Technology

We, and our third-party partners, may automatically collect certain types of usage information when you visit our Services, read our emails, or otherwise engage with us. We typically collect this information through a variety of tracking technologies, including cookies, flash objects, web beacons and similar technology (collectively, “tracking technologies”). For example, we collect information about your device and its software, such as your IP address, browser type, date and time stamp, a unique ID that allows us to uniquely identify your browser, mobile device or your user account, and other such information. Depending on your browser or device settings, we may collect your location data, including GPS coordinates or we may approximate your device’s location based on other information, such as an IP address. We also collect information about the way you use our Services, for example, the site from which you came and the site to which you are going when you leave our Services, the pages you visit, the links you click, how frequently you access the Services, whether you open emails or click the links contained in emails, whether you access the Services from multiple devices, and other actions you take on the Services.

We may collect analytics data, or use third-party analytics tools such as Google Analytics, to help us measure traffic and usage trends for the Service and to understand more about the demographics of our users. You can learn more about Google’s practices at <http://www.google.com/policies/privacy/partners> and view its currently available opt-out options at <https://tools.google.com/dlpage/gaoptout>. Although we do our best to honor the privacy preferences of our users, we are unable to respond to Do Not Track signals set by your browser at this time.

We use or may use the data collected through tracking technologies to: (a) remember information so that you will not have to re-enter it during your visit or the next time you visit our Services; (b) provide custom, personalized content and information, including targeted content and advertising; (c) recognize and contact you across multiple devices; (d) provide and monitor the effectiveness of our Services; (e) monitor aggregate metrics such as total number of visitors, traffic, usage, and demographic patterns on our Services; (f) diagnose or fix technology problems; and (g) otherwise to plan for and enhance our Services.

If you would prefer not to accept cookies, most browsers will allow you to: (i) change your browser settings to notify you when you receive a cookie, which lets you choose whether to accept it; (ii) disable existing cookies; or (iii) set your browser to automatically reject cookies. Please note that doing so may negatively impact your experience using the Services, as some features of our Services may not work properly. Depending on your mobile device and operating system, you may not be able to delete or block all cookies, you may not be able to block non-cookie technologies or the changes to your settings may have no effect. You may also set your e-mail options to prevent the automatic downloading of images that may contain technologies that would allow us to know whether you have accessed our e- mail and performed certain functions with it.

We and our third-party partners may also use cookies and tracking technologies for advertising purposes. For more information about tracking technologies, please see “Third-Party Tracking and Online Advertising” below.

Third Party Tracking and Online Advertising

Interest Based Advertising. We participate in interest-based advertising and use third-party advertising companies to serve you targeted advertisements based on your browsing history. We may share, or we may permit third-party online advertising networks, social media companies and other third-party services, to collect, information about your use of our Services over time so that they may play or display ads on our Services, on other devices you may use, and on other websites, apps, or Services.

These third parties may collect information such as click stream information, browser type, time, and date you visited the Services, mobile device identifiers, your use of third-party applications, and/or precise geolocation data and other information. We and our third-party partners use this information to make the advertisements you see online more relevant to your interests, as well as to provide advertising-related Services such as reporting, attribution, analytics, and market research.

Your Choices

Cookies and Flash cookies. Most browsers allow you to adjust your browser settings to: (i) notify you when you receive a cookie, which lets you choose whether to accept it; (ii) disable existing cookies; or (iii) set your browser to automatically reject cookies. Blocking or deleting cookies may negatively impact your experience using the Services, as some features and services on our Services may not work properly. Deleting cookies does not delete Local Storage Objects (LSOs) such as Flash objects and HTML5. To manage Flash cookie settings and preferences, you must use the settings manager on Adobe’s website or by clicking [here](#). If you choose to delete Flash objects from our Service, then you may not be able to access and use all or part of the Service or benefit from the information and Service offered.

Interest-based advertising. To learn about interest-based advertising and how you may be able to opt- out of some of this advertising, you may wish to visit the Network Advertising Initiative’s online resources, at <http://www.networkadvertising.org/choices>, and/or the DAA’s resources at www.aboutads.info/choices. Please note that opting-out of receiving interest-based advertising through the NAI’s and DAA’s online resources will only opt-out a user from receiving interest-based ads on that specific browser or device, but the user may still receive interest-based ads on his or her other devices. You must perform the opt-out on each browser or device you use. Some of these opt-outs may not be effective unless your browser is set to accept cookies. If you delete cookies, change your browser settings, switch browsers or computers, or use another operating system, you will need to opt- out again.

Mobile advertising. You may also be able to limit interest-based advertising through the settings on your mobile device by selecting “limit ad tracking” (iOS) or “opt-out of interest-based ads” (Android). You may also be able to opt-out of some but not all interest-based ads served by mobile ad networks by visiting <http://youradchoices.com/appchoices> and downloading the mobile AppChoices app.

Social Media Advertising. We may display targeted advertising to you through social media platforms, such as Facebook, LinkedIn and others. These companies have interest-based advertising programs that allow us to direct advertisements to users who have shown interest in our services while those users are on the social media platform, or to groups of other users who share similar traits, such as commercial interests and demographics. These advertisements are governed by the privacy policies

of the social media companies that provide them and you can control your advertising preferences directly on those platforms.

Google Analytics and Advertising. We use Google Analytics to recognize you and link the devices you use when you visit our services on your browser or mobile device, login to a user account on our services, or otherwise engage with us. Google Analytics allows us to better understand how our users interact with our services and to tailor our advertisements and content to you. We may also utilize certain forms of display advertising and other advanced features through Google Analytics, such as Remarketing with Google Analytics and Demographic and Interest Reporting. These features enable us to use first-party cookies (such as the Google Analytics cookie) and third-party cookies (such as the Doubleclick advertising cookie) or other third-party cookies together to inform, optimize, and display ads based on your past visits to the Services. For information on how Google Analytics collects and processes data, as well as how you can control information sent to Google, review Google's site "How Google uses data when you use our partners' sites or apps" located at www.google.com/policies/privacy/partners/. You can learn about Google Analytics' currently available opt-outs, including the Google Analytics Browser Ad-On, here: <https://tools.google.com/dlpage/gaoptout/>. You may control your advertising preferences or opt-out of certain Google advertising products by visiting the Google Ads Preferences Manager, currently available at <https://google.com/ads/preferences> or by visiting NAI's online resources at <http://www.networkadvertising.org/choices>.

Social Media Features

ExitCertified provides social media features that enable you to share information with your social networks and to interact with ExitCertified on various social media sites. These providers may recognize you and collect information about your visit to our Services, and they may set a cookie or employ other tracking technologies. Your interactions with those features are governed by the privacy notices of those companies. We encourage you to review the privacy notices and settings on the social media sites you use to interact to make sure you understand the information that may be collected, used, and shared by those sites. You may disable these features at any time.

Security of Personal Information

We seek to comply with legal requirements and use reasonable measures to help protect information about you from loss, theft, misuse and unauthorized access, disclosure, alteration and destruction. If required by applicable law, ExitCertified will notify you in the event we become aware of a security breach involving your personal information stored by or for us.

Retention Period

We retain your personal information for the period necessary to fulfill the purposes outlined in this Privacy Statement or otherwise upon collection of your personal information, unless a longer retention period is required or allowed by law or to otherwise fulfill a legal obligation.

To determine the appropriate retention period for personal information, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorized use or disclosure of your personal data, the purposes for which we process your personal data and whether

we can achieve those purposes through other means, and the applicable legal requirements.

When we no longer have a legitimate business need to process your personal information, we will either delete or anonymize it, if this is not possible (for example, because your personal information has been stored in backup archives), then we will securely store your personal information and isolate it from any further processing until deletion is possible.

Additional Provisions Children

We do not knowingly collect information from children as defined by local law, and do not target our websites to children.

Compliance with Local Laws

This Privacy Statement is meant to guide ExitCertified with respect to personal information collected from or about you. While this Privacy Statement applies to personal information generally, the local laws, rules and regulations of jurisdictions that are applicable to ExitCertified (“Local Laws”) may require standards that are stricter than this Privacy Statement, and in such event, ExitCertified will comply with applicable Local Laws. Specific privacy notices may be adopted to address the specific privacy requirements of particular jurisdictions.

Sensitive Information

“Sensitive Personal Data” may include personal data from which we can determine or infer an individual’s racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, membership in a trade union or professional association, physical or mental health or condition, biometric or genetic data, sexual life or judicial data (including information concerning the commission or alleged commission of a criminal offence), financial account information or government issued identification numbers. Unless we specifically request or invite you to provide sensitive personal information to us as defined by applicable law, we ask that you not send us such information. In cases where we may request or invite you to provide sensitive personal information, we will only process sensitive personal information you provide with your express consent. We only process Sensitive Personal Data if and to the extent permitted by applicable law and subject to the specific national legal requirements applicable to you (which may be for example, explicit notification of processing, reasons of general interest and/ or explicit consent).

Your Rights Regarding your Personal Information

Access to Personal Information. In accordance with the applicable data privacy law, you may be entitled to request certain information about the personal information we have stored about you; to request certain access to, correction, deletion, portability or blocking of such data, and to request restriction of processing or to object to the processing. For this purpose, please click contact Privacy@exitcertified.com with the subject line ‘access to Personal information request’.

If you need to update or change your personal information, you may log into your account or you may contact us at Privacy@exitcertified.com.

ExitCertified reserves the right to decline requests to access or delete personal information if and to the extent disclosure or deletion of the information requested is not required, for example because we may keep the personal information to achieve a legitimate purpose or to protect our rights or not permitted by applicable law.

To guard against fraudulent requests for access, ExitCertified reserves the right to verify your identity by requiring sufficient information to allow it to confirm the identity of the party making the request before granting access or making corrections.

You will not have to pay a fee to access your personal data or to exercise any of the other rights. However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive or where we are legally permitted to do so. Alternatively, we may refuse to comply with your request in these circumstances.

The Right To Object. In accordance with the applicable privacy law, especially in the European Union, you may have the right to object to the processing of your Personal Information if we process your personal information based on a legitimate interest, including the processing for the purposes of direct marketing. The objection can be filed via email or by any other means towards the respective ExitCertified Affiliate or at the e-mail address: Privacy@exitcertified.com. In case you object to the processing for direct marketing purposes, the personal information shall no longer be processed unless our legitimate reasons for the processing outweighs your rights and freedoms.

Your Consent and Changes

You have a right to withdraw your consent with processing of your personal information (if given) at any time at the e-mail address: Privacy@exitcertified.com. Please note that the withdrawal of your consent does not affect the lawfulness of the processing based on your consent given before its withdrawal. The withdrawal of your consent also does not affect the processing of your personal information which is being done by us on another legal basis than your consent (e.g. in particular if the processing is necessary for the performance of a contract, fulfilment of a legal obligation or due to other reasons stated in the valid legal regulation).

Lodge A Complaint. If you have any objections or complaints with the way we process your personal information, you may - as applicable - have the right to lodge a complaint with the competent data protection authority or other governmental entity. We would, however, appreciate the opportunity to discuss your concerns before you approach the authorities so please contact us at Privacy@exitcertified.com.

Compliance

If you believe that your personal information has been processed or disclosed in violation of this Privacy Statement, raise your concerns by contacting us at Privacy@exitcertified.com.

Questions

If you have any questions or concerns about this Privacy Statement, the privacy practices of

ExitCertified, our collection or use of your personal information, or you wish to access your personal information, please contact us. If we need or are required to contact you concerning any issue or event that involves this Privacy Statement, then we will do so using the email address, telephone number, or physical mailing address we have on file for you.

Updates to This Privacy Statement

We will update this Privacy Statement from time to time. When we make changes to this Privacy Statement, we will change the effective date in the "Introduction" section of this Privacy Statement. If we make material changes to this Privacy Statement, we will notify you by prominent posting on this website or our online services, or through other appropriate communication channels. All changes shall be effective from the date of publication unless otherwise provided.

Contact Us

If you have any questions or requests in connection with this Privacy Statement or other privacy-related matters, please send an email to Privacy@exitcertified.com.

Alternatively, inquiries may be addressed to: ExitCertified Corporation
Attn: Legal Department
450 Sansome St #600,
San Francisco, CA 94111,
United States

Local Specific Supplementing Notices

These Local specific Notices supplement the ExitCertified Privacy Statement and provide additional information about personal data processing as required by the applicable data protection law and its implementing rules and regulations. In case of any inconsistencies between the ExitCertified Privacy Statement and the below local specific notices, the local specific notices prevail.

California Privacy Rights

This section applies to you if you are a resident of the state of California. California law requires us to disclose certain information regarding the categories of personal information we collect. For purposes of this section, "personal information" has the meaning provided by the California Consumer Privacy Act (the "CCPA") and does not include information that is publicly available, that is deidentified or aggregated such that it is not capable of being associated with you, or that is excluded from the CCPA's scope, such as personal information covered by certain sector-specific privacy laws, such as the HIPAA, the FCRA, GLBA or the Driver's Privacy Protection Act of 1994. This section does not apply to personal information we collect when we are acting as a "service provider" to process information in accordance with a contract with our business customers. To learn more about the types of personal information we collect and the purposes for which we collect this information, please refer to the sections of the Privacy Statement titled "**What Personal Information We Collect**" and "**How We Use Information We Collect.**"

Also, to learn about our retention practices please refer to the section in the Privacy Statement titled **“Record Retention”**.

Disclosure of personal information. We share personal information with third parties for business purposes or we may sell your personal information to third parties, subject to your right to opt out of those sales (see Your California Rights and Choices below). The categories of third parties to whom we sell or disclose your personal information for a business purpose include: (i) other ExitCertified companies; our service providers, vendors and advisors; (iii) business partners with whom we work to provide our services; (iv) supply chain partners; (iv) ad networks and advertising partners; (v) analytics providers and ; (vi) social networks. In the previous 12 months, we have disclosed all categories of personal information we collect (explained in the chart above) to third parties for a business purpose.

We do not “sell” personal information such as your name, email address and mailing address for direct marketing purposes. As is common practice among companies that operate online, we do allow certain third-party advertising networks, social media companies and other third-party businesses to collect information directly from your browser or device through cookies or similar tracking technology when you visit or interact with our website, use our apps or otherwise engage with us online. For example, they may collect Internet/Network information, such as a cookie or device ID, browsing history and website usage, Geolocation Data, and Inferences generated from your browsing history and interactions with our service as well as other sites and services. These third parties use this personal information to serve relevant ads on our site, on other websites or mobile apps, or on other devices you may use, or to personalize content and perform other advertising-related services such as reporting, attribution, analytics and market research. These third-party businesses may use such information for their own purposes in accordance with their own privacy statements, which may include reselling this information to additional third parties, including other advertising networks. To learn more, please see **“Third-Party Tracking and Online Advertising”** section of our Privacy Statement.

Your California Rights and Choices. As a California resident, you may be able to request to exercise the following rights:

- The Right to Know any or all of the following information relating to your personal information we have collected and disclosed in the last 12 months, upon verification of your identity:
 - The specific pieces of personal information we have collected about you;
 - The categories of personal information we have collected about you;
 - The categories of sources of the personal information;
 - The categories of personal information that we have disclosed to third parties for a business purpose, and the categories of recipients to whom this information was disclosed;
 - The categories of personal information we have sold and the categories of third parties to whom the information was sold; and
 - The business or commercial purposes for collecting or selling the personal information.
- The Right to Request Deletion of personal information we have collected from you, subject to certain exceptions.
- The Right to Opt Out of Personal Information Sales to third parties now or in the future.

You also have the right to be free of discrimination for exercising these rights. However, please note that if the exercise of these rights limits our ability to process personal information (such as in the case of a deletion request), we may no longer be able to provide you our products and services or engage with you in the same manner.

California Consumer Rights Requests. You may submit a request to exercise your California Consumer Rights, including a request to opt out of personal information sales, through one of the mechanisms described below. We will need to verify your identity before processing your request, which may require us to request additional personal information from you or require you to log into your account, if you have one. In certain circumstances, we may decline or limit your request, particularly where we are unable to verify your identity or locate your information in our systems, or as permitted by law.

To exercise your California Consumer Rights, please submit a request by:

Emailing Privacy@exitcertified.com with the subject line "California Rights Request,".

California's "Shine the Light" Law. California's "Shine the Light" law (Civil Code Section §1798.83) provides certain rights to California residents that have an established business relationship with us about the disclosure of certain types of personal information to third parties for their direct marketing purposes. To opt-out of having your personal information disclosed to third parties for their direct marketing purposes, please use one of the California Consumer Rights request submission methods listed above.

Your Right To Object

If we process your personal data based on our legitimate interest, you may have the right to object to such processing by contacting Privacy@exitcertified.com. In this case, personal data shall no longer be processed unless ExitCertified demonstrates that our legitimate reasons for the processing dominate over your rights and freedoms. In case you object to the processing for direct marketing purposes, we will immediately cease to use your personal information for this purpose.

International Data Transfers

If personal data is transferred from a member state of the European Economic Area, UK, Turkey and Switzerland to a region deemed to not provide an adequate level of protection according to European Commission, we implement appropriate contractual safeguards, such as Standard Contractual Clauses, with third parties and for intragroup transfers or apply other appropriate safeguards as approved by the European Commission and as required to secure your personal data. Further, if such third parties engage sub-processors in support of our agreement with them, the third party will be required to implement the same standards and safeguards with their sub-contractors.

If you would like to learn more about the relevant transfer mechanism or categories of relevant Service Provider, please contact us by sending an email to Privacy@exitcertified.com.

Google Analytics 4 – Websites in the European Economic Area

We use Google Analytics 4 (“GA 4”) on websites, a web analysis service provided by Google LLC analytics on users in the EU/EEA and Switzerland and is provided by Google Ireland Limited, Google Building Gordon House, 4 Barrow St, Dublin, D04 E5W5, Ireland (“Google”).

If you have given your consent: **Scope Of Processing**

GA 4 uses cookies, which enable an analysis of the use of our websites by you. The information collected by the cookies about your use of this website is usually transmitted to a Google server in the USA and stored there.

We use the User ID function. User ID allows us to assign a unique, persistent ID to one or more sessions (and the activities within those sessions) and to analyze user behavior across devices.

We use Google Signals. This allows Google Analytics to gather additional information about users who have opted into personalized ads (interests and demographics) and allow ads to be served to those users in cross-device remarketing campaigns. With GA 4, the anonymization of IP addresses is activated by default. Due to IP anonymization, your IP address will be shortened by Google within member states of the European Union or in other contracting states of the Agreement on the European Economic Area. Only in exceptional cases will the full IP address be sent to a Google server in the USA and shortened there. According to Google, the IP address transmitted by your browser as part of Google Analytics will not be merged with other Google data.

During your visit to the website, your user behavior is recorded in the form of "Events". Events can be pageviews, visiting the website for the first time, start of session, your "click path", interaction with the website, scrolls), clicks on external links, internal searches, interacting with videos, file downloads, ads seen/clicked on, language setting.

In addition, the following information is recorded: your approximate location (region), your IP address (in abbreviated form), technical information about your browser and the end devices you use (e.g. language setting, screen resolution), your internet provider, the referrer URL (from which website/which advertising medium you came to this website).

Purposes of Processing

On behalf of the operator of this website, Google will use this information to evaluate your [pseudonymous [NOT USING USER ID]] use of the website and to compile reports on website activity. The reports provided by Google Analytics are used to analyze the performance of our website and the success of our marketing campaigns.

Recipients

Recipients of the data are/can be:

- Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland (as processor according to Art. 28 GDPR)
- Google LLC, 1600 Amphitheater Parkway Mountain View, CA 94043, USA

- Alphabet Inc., 1600 Amphitheater Parkway Mountain View, CA 94043, USA

Please note that it is possible that US authorities will access the data stored by Google.

Third Country Transfer

Insofar as data is processed outside the EU/EEA, and there is no level of data protection corresponding to the European standard, we have concluded [EU standard contractual clauses with the service provider](#) to establish an appropriate level of data protection. The parent company of Google Ireland, Google LLC, is based in California, US. A transfer of data to the US and access by US authorities to the data stored by Google cannot be ruled out. The US is currently considered a third country from a data protection perspective. You do not have the same rights with regard to your personal data being processed in the US as within the EU/EEA. You may not be entitled to any legal remedies against access by US authorities.

Duration Of Storage

The data sent by us and linked to cookies are automatically deleted after 2 months. The deletion of data whose retention period has been reached occurs automatically once a month.

Legal Basis

The legal basis for this data processing is your consent pursuant to Art.6 para.1 p.1 lit. a GDPR [and](#) Art.49a GDPR].

Revocation

You can revoke your consent at any time with effect for the future by accessing the cookie settings on our website and changing your selection there. Revoking your consent will not affect the lawfulness of the processing carried out on the basis of the consent prior to the revocation.

You can also prevent the storage of cookies from the outset by setting your browser software accordingly. However, if you configure your browser to reject all cookies, this may result in a restriction of functionalities on this and other websites.

You can further prevent the collection of data generated by the cookie and related to your use of the website (including your IP address) to Google and the processing of this data by Google, by:

- a. not giving your consent to the setting of the cookie or
- b. downloading and installing the browser add-on to disable Google Analytics [HERE](#).

For more information on Google Analytics' terms of use and Google's privacy policy, please visit <https://marketingplatform.google.com/about/analytics/terms/us/> and at <https://policies.google.com/?hl=en>