State of Oklahoma Office of Management and Enterprise Services

STATE OF OKLAHOMA AMENDMENT NO. 4 TO NASPO CONTRACT WITH AXON ENTERPRISE, INC...

This Fourth Amendment to the NASPO Master Service Agreement (the "Fourth Amendment") is effective as of the date of the last signature below (the "Effective Date"), between the State of Oklahoma by and through the Office of Management and Enterprise Services and Axon Enterprise, Inc.. ("Supplier"). This Fourth Amendment supplements and amends the NASPO Master Service Agreement with The State of Oklahoma and Axon Enterprise, Inc., entered into by the parties and effective September 26, 2023 (the "Master Agreement"), including all supplements and amendments thereto. Unless otherwise indicated herein, capitalized terms used in this Amendment without definition shall have the respective meanings specified in the Contract.

For good and valuable consideration, the parties agree to amend the Contract as follows:

1. The State and Supplier agree to the addition of the Carbyne Products and Services and the Prepared Products and Services (collectively, the "Added Offerings") to the Master Agreement. The Added Offerings are hereby incorporated into and made part of the Master Agreement's Scope as approved by the State.
2. The following document(s) are hereby incorporated into the Contract as additional appendices. The document(s) are incorporated for the purposes stated within the respective document and shall have the same force and effect as if fully set forth in the Master Agreement. The incorporation of these documents is intended to supplement the existing terms and does not alter, replace, or diminish any other document or provision of the Master Agreement.

    2.1. Axon Cloud Services Terms of Use Appendix, Attachment A
    2.2. Privacy Policy, Attachment B

3. In the event of a conflict between the terms and conditions hereof and the terms and conditions of the Contract, the specific terms set forth in this Amendment shall govern the subject matter herein.
4. Except as expressly modified in this Amendment, all terms and/or provisions of the Contract not addressed herein remain as executed by the parties in the Contract and remain in full force and effect.
5. This Amendment may be executed by electronic signature in counterparts (e-mail, facsimile or otherwise). The counterparts each of which shall constitute an original, but all of which together shall constitute one and the same instrument.

Signatures

The undersigned represent and warrant that they are authorized, as representatives of the party on whose behalf they are signing, to sign this Amendment and to bind their respective party thereto:

STATE OF OKLAHOMA
by and through the
OFFICE OF MANAGEMENT AND ENTERPRISE SERVICES:

By: Dan Cronin (Apr 28, 2026 16:00:09 CDT)

Name: Dan Cronin

Title: Chief Information Officer/Chief Transformation Officer

Date: Apr 28, 2026

AXON ENTERPRISE, INC:

By: Robert E. Driscoll, Jr. (Apr 28, 2026 11:37:52 PDT)

Name: Robert E. Driscoll, Jr.

Title: Deputy General Counsel

Date: Apr 28, 2026

Fourth Amendment to the NASPO ValuePoint Master Agreement OK-MA-145-21-100

This Fourth Amendment ("**Amendment**") is between Axon Enterprise, Inc. (f/k/a Taser International, Inc.), a Delaware corporation ("**Axon**"), and the State of Oklahoma by and through the Office of Management and Enterprise Services ("State" or "Customer"). This Amendment is effective as of the last signature date on this Amendment ("**Effective Date**"). Axon and Customer are each a "**Party**" and collectively "**Parties**".

Axon and the State are Parties to the NASPO Contract OK-MA-145-21-100 by and between Axon Enterprise, Inc. and the State of Oklahoma by and through the Office of Management and Enterprise Services, dated July 1, 2023, (the "**Master Agreement**").

This Amendment supplements and amends the Contract, including all supplements and amendments thereto. Unless otherwise indicated herein, capitalized terms used in this Amendment without definition shall have the respective meanings specified in the Master Agreement.

1. The following are changes to the Contractor's Terms and Conditions under the Master Agreement titled "Master Services and Purchasing Agreement" ("MSPA"):

    a. **Incorporation of Appendices**: The following documents are hereby incorporated into the Contract as additional appendices:
        i. Axon Cloud Services Terms of Use Appendix - Supplemental *(This appendix is supplemental; adds to, but does not replace, the existing Axon Cloud Services Terms of Use Appendix).*
            1. Carbyne Products and Services
            2. Prepared Products and Services

2. All other terms and conditions of the Agreement shall remain unchanged and in full force and effect.

Each representative identified below declares that they are an authorized representative of the respective Party with authority to execute this Amendment as of the date of signature.

Axon Enterprise, Inc.

Signature: Robert E. Driscoll, Jr.
Robert E. Driscoll, Jr. (Apr 28, 2026 11:37:52 PDT)

Name: Robert E. Driscoll, Jr.

Title: Deputy General Counsel

Date: Apr 28, 2026

State/Lead Agency

Signature:
Dan Cronin (Apr 28, 2026 16:00:09 CDT)

Name: Dan Cronin

Title: Chief Information Officer/Chief Transformation Officer

Date: Apr 28, 2026

The following is added to the Axon Cloud Services Terms of Use Appendix:

Carbyne Products and Services

1.1. **Privacy Policy**. Axon will only use Customer Content to provide Customer Carbyne Products and Services. Axon will not use Customer Content for any advertising or similar commercial purposes. The Participating Addendum, the Master Agreement and the Carbyne Privacy Policy governs the collection, use and disclosure of certain data provided to Axon in connection with Customer's use of the Carbyne products and services. The current policy is attached hereto and incorporated into this Agreement by reference. If any conflict arises between the Participating Addendum, the Master Agreement, and the Carbyne Privacy Policy, the privacy policies incorporated into the Participating Addendum and the Master Agreement shall control with respect to the collection, use, and disclosure of data provided to Axon in connection with Customer's use of the Carbyne products and services.

1.2. **Data Retention and Storage**. Unless Customer provides Axon with written instruction otherwise, Axon will retain Customer Content which uploaded to the Carbyne cloud services or which is recorded or stored in the course of your use of the Carbyne products and services, for a period of two years (the period we retain your data referred to as the "Data Retention Period"), provided that Customer acknowledges it is responsible for your compliance with any applicable data retention laws. Customer Content is automatically deleted after the Data Retention Period; however, at any time prior to such deletion, Customer may download Customer Content which has been stored on the Carbyne Cloud Services. Customer is solely responsible for the retention of such data for any applicable retention periods and for the purpose of any subsequent data requests.

1.3. **Disclaimer**. **CUSTOMER ACKNOWLEDGES THE CARBYNE PRODUCTS DO NOT PROVIDE TELEPHONE SERVICES, INTERCONNECTED VOIP SERVICES, OR 911 SERVICES. AXON MAKES NO REPRESENTATION THAT CARBYNE PRODUCTS ARE AN INTERCONNECTED VOIP SERVICE.**

Prepared Products and Services.

1.4. Prepared product deployment timelines for Prepared products within the Scope of Work (SOW) shall be mutually agreed to by the Parties in the SOW. The initial deployment of Assistive Call Taking (ACT) may take up to 12 months from the execution of the SOW and the service start date listed in the Agreement; deployments of the remaining Prepared products may take up to twenty-four (24) months from the execution of the SOW. Axon must confirm feasibility based on technical requirements for Prepared products prior to the execution of the SOW.

1.5. Customers using Solacom (Comtech CHE) call handling equipment in a multi-tenant configuration are not eligible for Prepared ACT or Prepared AQA, as call audio cannot be isolated to a single agency. Such Customers remain eligible for ANET and Assistive Dispatch. Customers on Solacom single-tenant configurations are eligible for all Prepared products, subject to SPAN port fees described below.

Carbyne Privacy Policy

Important Information

This Privacy Policy gives you information about who we are and how and why we collect, store, use and share your personal data. It also explains your rights in relation to your personal data and how to contact us or supervisory authorities in the event you have a complaint.

Controller

Carbyne is made up of different legal affiliate entities, including Carbyne Ltd., Carbyne911 Mexico S. de RL de CV and Carbyne, Inc. (collectively, the "Group"). This Privacy Policy is issued on behalf of the Group. When we mention "Carbyne", "we", "us" or "our" in this Privacy Policy, we are referring to the relevant company in the Group responsible for processing your data. Carbyne Ltd. is the controller responsible for this website.

We collect, use and are responsible for certain personal data about you under applicable privacy laws.

Processor

When Carbyne provides services to our customers, we are acting as processor on behalf of our customers, who are the controllers. This means that we only process your personal data in accordance with the instructions of our customers. Our activities as processor are outside the scope of this Privacy Policy. If you have any questions regarding how our customers process your personal data (i.e., because we are supporting services they make available to you), we recommend that you contact them directly.

We are also subject to the EU General Data Protection Regulation (EU GDPR) and the UK General Data Protection Regulation and Data Protection Act 2018 (UK GDPR) in relation to goods and services we offer to individuals and our wider operations in the European Economic Area (EEA) and the United Kingdom (UK).

Please note that if you are usually a resident in the EEA or the UK, this Privacy Policy is supplemented with the 'Additional Information for EEA/UK Residents' section below. The Additional Information for EEA/UK Residents does not apply if you are usually a resident elsewhere. In the event of any conflict between the terms of this Privacy Policy and the Additional Information for EEA/UK Residents, the latter shall prevail.

For further information on our reliance on the Data Privacy Framework Program, please view the 'DPF Program Disclosures' section below. In the event of any conflict between the terms of this Privacy Policy and the DPF Program Disclosures, the latter shall prevail.

Information We Collect

We collect information about you in a variety of ways depending on how you interact with us and our websites and services, including:

- Directly from you when you provide it to us, such as when you register for an account, sign up to receive communications from us, purchase our services, or contact us by phone, email, or otherwise.
- Automatically through the use of cookies, server logs, and other similar technologies when you interact with our websites, applications, advertisements, and emails.
- From other sources, including, for example, our affiliates, business partners, service providers, and other third parties, or from publicly available sources. For example, if you submit a job application, or become an employee, we may conduct a background check.

We also collect, use and share aggregated data such as statistical or demographic data which is not personal data as it does not directly (or indirectly) reveal your identity. For example, we may aggregate data related to individuals' usage of

our website and services to calculate the percentage of users accessing a specific feature in order to analyze general trends in how users are interacting with our website or services to help improve the website and our service offerings.

The following provides examples of the type of information that we collect about our customers or that we collect on our website:

Context	**Types of Data**	**Primary Purpose for Collection and Use of Data**
Applicant Information	If you apply for a job posting, we collect information necessary to process your application and make a hiring decision. This may include, among other things, your email address, Social Security Number and work history. Providing this information is required for employment.	We have a legitimate interest in processing your application, meeting our legal obligations, and communicating with you regarding your application.
Cookies and First-Party Tracking	We use cookies and clear GIFs. “Cookies” are small pieces of information that a website sends to a computer’s hard drive while a website is viewed.	We collect this information to analyze our website and ensure that it runs efficiently. Where required by law, we base the use of cookies upon consent.
Cookies and Third-Party Tracking	We may place tracking technology on our website that collects analytics, records how you interact with our website, or allows us to participate in behavior-based advertising. This means that a third party uses technology (*e.g.*, a cookie) to collect information about your use of our website so that they can report analytics to us or provide advertising about products and services tailored to your interests. That third party might also collect information over time and across different websites in order to serve advertisements on our website or other websites.	Where required by law, we base the use of cookies on your consent.
Demographic Information	We collect personal information, such as your age or location.	We have a legitimate interest in understanding our users and providing tailored services.
Mailing List	When you sign up for one of our mailing lists we collect your email address or postal address.	We share information about our products and services with individuals that consent to receive such information.
Mobile Devices	We collect information from your mobile device	We collect this information to identify

	such as location or other unique identifying information broadcast from your device when visiting our website	unique visitors, and understand how users interact with us on their mobile devices. Where required by law, we will obtain your consent to gathering such information.
Public Health and Safety	In certain situations where a serious public health threat has been identified, we may collect information from employees, guests, and other individuals accessing our facilities. This may include medical and health information, such as body temperature, symptoms, and underlying health conditions. In some cases, we may also collect medical, health, and related information about an employee's children, family members, or other individuals under the employee's care.	We have a legitimate interest in protecting the health and safety of our employees and guests. In some jurisdictions we may be required by law, regulation, or governmental order to collect and retain information related to issues of public health and safety. We have a legitimate interest in complying with the laws in the jurisdictions in which we operate.
Surveys	When you participate in a survey, we collect information that you provide through the survey. If the survey is provided by a third party service provider, the third party's privacy policy applies to the collection, use, and disclosure of your information.	We have a legitimate interest in understanding your opinions and collecting information relevant to our organization.
Web logs	We collect information, including your browser type, operating system, Internet Protocol (IP) address (a number that is automatically assigned to a computer when the internet is used), domain name, click-activity, referring website, and/or a date/time stamp for visitors.	We have a legitimate interest in monitoring our networks and the visitors to our websites. Among other things, it helps us understand which of our services is the most popular. Where required by law, we base the use of cookies which collect such information upon consent.
Website interactions	We use technology to monitor how you interact with our website. This may include which links you click on, or information that you type into our online forms. This may also include information about your device or browser.	We have a legitimate interest in understanding how you interact with our website to better improve it, and to understand your preferences and interests in order to select offerings that you might find most useful. We also have a legitimate interest in detecting and preventing fraud.

The following provides examples of the type of information that we collect as part of providing our products and services:

Context	**Types of Data**	**Primary Purpose for Collection and Use of Data**
Account Registration	We collect your name and contact information when you create an account on our website or by using our products. We also collect information relating to the actions that you perform while logged into your account.	We have a legitimate interest in providing account related functionalities to our users. We also need to register your account in order to provide services or features you have requested, for example, Accounts can be used for easy checkout and to save your preferences and transaction history and to provide the emergency call enhancement service.
Customer Employee's Information	We collect the name, and contact information, of our customers and their employees with whom we may interact.	We have a legitimate interest in contacting our customers and communicating with them concerning normal business administration such as projects, services, and billing. We also collect such information in order to administer the contract we have with our customers and to provide our services.
Customer Information	We collect personal information about you, or other people, on behalf of our customers. Our customers determine what information we collect when we act on their behalf.	When we collect personal information on behalf of our customers, our customers determine the purpose for which we collect that information and how we are permitted to use it, including with whom we are permitted to share it. You should refer to our customer's privacy notice to better understand the privacy practices that will apply to your data. Please note that such information will generally be collected on the basis of your consent when using the services or in order to safeguard your vital interests.
Distance Information	When you use one of our products we may collect your location from the GPS, Wi-Fi, and/or cellular technology in your device to determine your location and your distance from an emergency, emergency responder, law enforcement officer or other events or individual who may be relevant to	When we collect personal information on behalf of our customers, our customers determine the purpose for which we collect that information and how we are permitted to use it, including with whom we are permitted to share it. You should refer to our

	the situation.	customer's privacy notice to better understand the privacy practices that will apply to your data.
Feedback/Support	If you provide us feedback or contact us for support we will collect your name and email address, as well as any other content that you send to us, in order to reply.	We have a legitimate interest in receiving, and acting upon, your feedback or issues.
Mobile Devices	Some of our products may permit individuals to transmit information from their mobile devices, such as audio, video, or text.	When we collect personal information on behalf of our customers, our customers determine the purpose for which we collect that information and how we are permitted to use it, including with whom we are permitted to share it. You should refer to our customer's privacy notice to better understand the privacy practices that will apply to your data. Please note that such information will generally be collected on the basis of your consent when using the services or in order to safeguard your vital interests.

How We Use Information.

In addition to the purposes and uses described above, we use information in the following ways:

- To identify you when you visit our websites and analyze your use of our website and services.
- To provide and improve our products and services.
- To communicate with you, such as to respond to and/or follow-up on your requests, inquiries, issues, or feedback.
- To send marketing and promotional materials including information relating to our products, services, sales, or promotions, or those of our business partners.
- To detect and protect against malicious, deceptive, fraudulent, or illegal activity, including violation of our policies and terms and conditions, security incidents, and harm to the rights, property, or safety of our company and our users, employees, or others.
- To debug, identify and repair errors that impair existing intended functionality of our website and services.
- To comply with our legal or regulatory obligations, to establish or exercise our rights, and to defend against a legal claim.
- For internal administrative purposes, as well as to manage our relationships.
- For such other purposes as you may consent (from time to time).

Although the sections above describe our primary purpose in collecting your information, in many situations we have more than one purpose. For example, if you or your employer engages us to provide our services, we may collect your information to perform our contract with you or your employer, but we also collect your information as we have a legitimate interest in maintaining your information so that we can help our customers meet their data retention requirements and for other legally required reasons and to quickly and easily respond to questions about your order.

To the extent we maintain and use personal information in a deidentified form, we will not attempt to reidentify the information, except for the purpose of determining whether our deidentification processes satisfy our legal obligations.

How We Share Information.

In addition to the specific situations discussed elsewhere in this Privacy Policy, we may disclose personal information to third parties outside the Group. We require all third parties to respect the security of your personal data and to treat it in accordance with the law. We may share your personal data in the following situations:

- **Affiliates and Acquisitions.** We may share information with our corporate affiliates (*e.g.*, parent company, sister companies, subsidiaries, joint ventures, or other companies under common control). If another company acquires, or plans to acquire, our company, business, or our assets, we will also share information with that company, including at the negotiation stage. Where required by law, we implement measures to ensure that our affiliates provide adequate protection of personal information and comply with their responsibilities under applicable law. If a change happens to our business, then the new owners may use your personal data in the same way as set out in this Privacy Policy.

- **Other Disclosures without Your Consent.** We may disclose information in response to subpoenas, warrants, or court orders, or in connection with any legal process, or to comply with relevant laws. We have processes in place to review the validity and lawfulness of any such requests before deciding if or how to respond. We may also share your information in order to establish or exercise our rights, to defend against a legal claim, to investigate, prevent, or take action regarding possible illegal activities, suspected fraud, safety of our product platform, person or property, or a violation of our policies. We may also share information without your consent in the event of an emergency where the health and safety of an individual or the general public may be at risk.

- **Service Providers.** We share your information with service providers. Among other things service providers help us to administer our website, conduct surveys, provide technical support, process payments, and assist in the fulfillment of the services. Where required by law, we endeavor to ensure that these service providers are subject to contractual obligations to provide adequate protection of personal information and comply with their responsibilities under applicable law. Additionally, we do not allow our third-party service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions.

- **Other Disclosures with Your Consent.** We may disclose your information to other third parties only when we have your consent or direction to do so.

Cookies

For more information about the cookies we use and how to change your cookie preferences, please see our cookie policy by clicking on the cookie settings icon on the bottom left of our site.

Your Choices

In some instances you may request that we take certain action regarding your information. You may exercise these choices by following the directions provided below and we will respond to your request where required by law. In any case, we will not discriminate against you on the basis of your decision to exercise any of these choices.

- **Access To Your Personal Information.** You may request access to your personal information, confirmation that we have information about you, or information about the public and private entities to whom we have shared data as a controller. In certain limited circumstances, you may also request to receive access to your data in a portable, machine-readable format.

- **Changes To Your Personal Information.** We rely on you to update and correct your personal information through your account. If your account does not permit you to update or correct certain information, you can contact us at the email address below. You may ask us to correct information that is inaccurate or incomplete. Note that we may keep historical information in our backup files as permitted by law.

- **Deletion Of Your Personal Information.** In some circumstances, you may request that we delete or anonymize your personal information. If required by law, we will grant requests to delete or anonymize information, but in many situations we are required to keep your personal information to comply with our legal obligations, resolve disputes, enforce our agreements, or for another business purpose.

- **Objection to Certain Processing.** You may object to our use or disclosure of your personal information by contacting us at the address described below.

- **Online Tracking.** We do not currently recognize the "Do Not Track" signal.

- **Opt-out of Targeted Advertising.** You may opt-out of online tracking based targeted advertising (e.g., cookies) by clicking the cookie settings on our site. Please note that if you change browsers or computers, or if you clear your browser's cache, you may need to click the link again to apply your preference. You may also opt-out of other forms of targeted advertising by submitting a request as described below.

- **Promotional Emails.** You may choose to provide us with your email address for the purpose of allowing us to send free newsletters, surveys, offers, and other promotional materials to you. You can stop receiving promotional emails by following the unsubscribe instructions in emails that you receive. If you decide not to receive promotional emails, we may still send you communications related to services we provide to you.

- **Revocation Of Consent**. Where we process your personal information based upon your consent, you may revoke consent. Please note, if you revoke your consent for the processing of personal information then we may no longer be able to provide you services.

Submitting Requests

You may exercise the choices described above by contacting us as indicated in the "Contact Information" section below.

As required by law, we will require you to prove your identity. We may verify your identity by phone call or email. Depending on your request, we will ask for information such as your name, the organizational customer of ours that you are affiliated with, or the date and context that we collected the requested information from you. We may also ask you to provide a signed declaration confirming your identity. Following a request, we will use reasonable efforts to supply, correct, or delete personal information.

We will not be able to honor any requests relating to personal information collected by us in our capacity as a processor (i.e., when we are performing services for our customer). Such requests should be sent to our customer and not to Carbyne.

How We Protect and Retain Information

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorized way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need-to-know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

However, please note that no method of transmission over the internet, or method of electronic storage, is fully secure. While we use reasonable efforts to protect your personal information from unauthorized access, use, or disclosure, we cannot guarantee the security of your personal information. In the event that we are required by law to inform you of a breach to your personal information we may notify you electronically, in writing, or by telephone, if permitted to do so by law.

Some of our websites permit you to create an account. When you do you will be prompted to create a password. You are responsible for maintaining the confidentiality of your password, and you are responsible for any access to or use of your account by someone else that has obtained your password, whether or not such access or use has been authorized by you. You should notify us of any unauthorized use of your password or account.

We process and retain your personal information for only as long as necessary to fulfill the purposes outlined in this Privacy Policy, including for the purposes of satisfying any legal, accounting, or reporting requirements, unless a longer retention period is required or permitted by law. To determine the appropriate retention period for personal information, we consider the amount, nature, and sensitivity of the information, the potential risk of harm from unauthorized use or disclosure of the information, the purposes for which we obtained the information and whether we can achieve those purposes through other means, as well as applicable legal requirements. We may retain your personal data for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect to our relationship with you.

In some circumstances we will anonymize your personal data (so that it can no longer be associated with you) for research or statistical purposes, in which case we may use this information indefinitely without further notice to you

Transmission Of Information To Other Countries

As a multi-national company, we may transmit information between and among our Group members and service providers. As a result, your information may be processed in a foreign country where privacy laws may be less stringent than the laws in your country. Nonetheless, where possible we take steps to treat personal information using the same privacy principles that apply pursuant to the law of the country in which we first received your information. If you are in either the EEA or the UK, such processing may involve transferring your personal information outside of the EEA or the UK. For such processing, if we transfer your personal information outside of the EEA or the UK, we will only transfer your personal data to a country outside the EEA or the UK where:

- in the case of transfers subject to UK data protection law, the UK government has decided the particular country ensures an adequate level of protection of personal data (known as an '**adequacy regulation**') further to Article 45 of the UK GDPR. We rely on the adequacy regulation for transfers to the United States pursuant to the UK extension to the Data Privacy Framework.
- in the case of transfers subject to EEA data protection laws, the European Commission has decided that the particular country ensures an adequate level of protection of personal data (known as an '**adequacy decision**') further to Article 45 of the GDPR. We rely on the adequacy decision for transfers to the United States pursuant to the Data Privacy Framework.
- in the case where no adequacy regulation or adequacy decision has been issued, there are appropriate safeguards in place, together with enforceable rights and effective legal remedies for you (i) you expressly consent to such transfers; or (ii) a specific exception applies under relevant data protection law.

We will notify you of any changes to the transfer mechanisms we rely on to transfer personal data internationally in accordance with the section on 'Changes to this Privacy Policy' below.

Third-Party Applications/Websites

For your convenience, we may provide links to websites and other third-party content or services that we do not own or operate. The websites and third-party content to which we link may have separate privacy notices or policies. We have no control over the privacy practices of websites or services we do not own. We encourage you to review the privacy policies of any third-party website or application for details about such third party's privacy practices.

Changes To This Privacy Policy and Your Duty to Keep Us Updated

We may change our Privacy Policy and practices over time. To the extent that our policy changes in a material way, the policy that was in place at the time that you submitted personal information to us will generally govern that information unless we receive your consent to the new Privacy Policy. Our Privacy Policy includes an "effective" and "last updated" date. The effective date refers to the date that the current version took effect. The last updated date refers to the date that the current version was last substantively modified.

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your relationship with us, for example a new address or email address.

Contact Information

If you have any questions, comments, or complaints concerning our privacy practices, or if you need to access this Privacy Policy in an alternative format due to having a disability, please contact us by email at privacy@carbyne.com or via the contact form available here.

Additional Information For California Residents

In some jurisdictions businesses may be required to disclose the following additional information related to their privacy practices. If you are a resident of such a jurisdiction, the following privacy disclosures may apply to you in addition to the rest of the Privacy Policy.

- **California Shine the Light.** If you would like more information concerning the categories of personal information (if any) we share with third parties or affiliates for those parties to use for direct marketing, please submit a written request to us using the information in the **Contact Information** section above.
- **Notice of Collection.** The table below describes the categories of personal information we collect, disclose for a business purpose, "sell" and/or "share" (as those terms are defined under some state privacy laws). Please note, in addition to the recipients identified below, we may disclose any of the categories of personal information we collect with government entities, as may be needed to comply with law, provide our services or prevent illegal activity. We do not "sell" your personal information for money. As discussed elsewhere in the Privacy Policy, we use cookies and similar tracking technologies for purposes of targeted advertising. For more information and further details regarding how we use personal information, please see the **Information We Collect** section of the Privacy Policy. For information regarding how long we retain personal information, please refer to the **How We Protect and Retain Information** section of the Privacy Policy.

Category of Personal Information	**Category of Recipients**	
	Disclosures for a Business Purpose	**Sharing for Cross-Context Behavioral Advertising**
Identifiers – this may include real name, alias, postal	Affiliates or subsidiaries Other service providers Professional	Advertising networks

address, unique personal identifier, online identifier, email address, account name, or other similar identifiers.	services organizations, this may include auditors and law firms	
Government Issued Identification – this may include social security number, driver's license number, or state issued identification number, passport number.	Affiliates or subsidiaries Other service providers Professional services organizations, this may include auditors and law firms	N/A
Characteristics of protected classifications – this may include age, sex, race, ethnicity, physical, or mental handicap, etc.	Affiliates or subsidiaries Other service providers Professional services organizations, this may include auditors and law firms	N/A
Internet or other electronic network activity information – this may include browsing history, search history, and information regarding an individual's interaction with an internet website, application, or advertisement.	Affiliates or subsidiaries Other service providers Professional services organizations, this may include auditors and law firms	Advertising Networks
Geolocation data	Affiliates or subsidiaries Other service providers Professional services organizations, this may include auditors and law firms	N/A
Audio, electronic, visual, thermal, olfactory, or similar information	Affiliates or subsidiaries Other service providers Professional services organizations, this may include auditors and law firms	N/A
Inferences drawn from any of the information listed above	Affiliates or subsidiaries Other service providers Professional services organizations, this may include auditors and law firms	Advertising Network

Professional or employment-related information	Affiliates or subsidiaries Other service providers Professional services organizations, this may include auditors and law firms	N/A
Additional categories of personal information described in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)) – this may include signature, physical characteristics, or description, , insurance policy number.	Affiliates or subsidiaries Other service providers Professional services organizations, this may include auditors and law firms	N/A

California Sensitive Information Disclosure. We collect the following categories of sensitive personal information (as defined under California law): precise geolocation data, and protected classes of personal information. This information is collected in order to provide our services and assist law enforcement with information necessary to respond to reports of criminal activity and emergencies. We do not use such information for any purposes that are not identified within the California Privacy Rights Act Section 1798.121. We do not "sell" or "share" sensitive personal information for purposes of cross-context behavioral advertising.

ADDITIONAL INFORMATION FOR EEA/UK RESIDENTS

This section only applies to you if you are usually resident in the EEA or the UK. It does not apply to you if you are located elsewhere.

Legal basis

The EU GDPR and UK GDPR require us to have a legal basis for collecting and using your personal data. We rely on one or more of the following legal bases for the primary purposes of collection and processing set forth in our Privacy Policy:

- Performance of a contract: Where we need to perform the contract we are about to enter into or have entered into.
- Legitimate interests: We may use your personal data where it is necessary to conduct our business and pursue our legitimate interests, for example to prevent fraud and enable us to give you the best and most secure customer experience. We make sure we consider and balance any potential impact on you and your rights (both positive and negative) before we process your personal data for our legitimate interests. We do not use your personal data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law).
- Legal obligation: We may use your personal data where it is necessary for compliance with a legal obligation that we are subject to. We will identify the relevant legal obligation when we rely on this legal basis.
- Consent: We rely on consent only where we have obtained your active agreement to use your personal data for a specified purpose, for example if you subscribe to an email newsletter.

Special Category Data

Special category data, also known as sensitive data, includes personal information revealing racial or ethnic origin, political opinions, religious beliefs, philosophical beliefs or trade union membership, genetic data, biometric data (where used for identification purposes), data concerning health, sex life or sexual orientation. We do not process special category data unless you expressly and voluntarily provide this to us. If we do process special category data, we will always ensure we are permitted to do so under data protection laws, such as on the basis of your explicit consent, the processing is necessary to protect your (or someone else's) vital interests where you are physically or legally incapable of giving consent or the processing is necessary to establish, exercise or defend legal claims.

Marketing

We will use your personal data to send you updates (by email, text message, telephone or post) about services, including exclusive offers, promotions or services.

We have a legitimate interest in using your personal data for marketing purposes. This means we do not usually need your consent to send you marketing information if you have requested information from us or purchased goods or services from us and you have not opted out of receiving the marketing.

Where legally required, we will always seek your consent prior to sending you marketing materials.

If we change our marketing approach in the future so that consent is needed, we will ask for this separately and clearly.

You have the right to opt out of receiving marketing communications at any time by:

- contacting us at contact@carbyne.com; or
- using the 'unsubscribe' link in emails you receive.

We may ask you to confirm or update your marketing preferences if you ask us to provide further services in the future, or if there are changes in the law, regulation, or the structure of our business.

We will always treat your personal data with the utmost respect and never sell it with other organizations outside the Group for marketing purposes.

Please note that if you opt out of receiving marketing communications, you will still receive service-related communications that are essential for administrative or customer service purposes.

Your legal rights

Under the EU GDPR and UK GDPR, you have a number of rights in relation to your personal data.

You have the right to:

- Request access to your personal data (commonly known as a "subject access request"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.
- Request correction of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.
- Request erasure of your personal data in certain circumstances. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply

with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.

- Object to processing of your personal data where we are relying on a legitimate interest (or those of a third party) as the legal basis for that particular use of your data (including carrying out profiling based on our legitimate interests). In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your right to object.

You also have the absolute right to object any time to the processing of your personal data for direct marketing purposes (the section 'Marketing' above for details of how to object to receiving direct marketing communications).

- Request the transfer of your personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.

- Withdraw consent at any time where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.

- Request restriction of processing of your personal data. This enables you to ask us to suspend the processing of your personal data in one of the following scenarios:

    - If you want us to establish the data's accuracy;

    - Where our use of the data is unlawful but you do not want us to erase it;

    - Where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or

    - You have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.

If you wish to exercise any of the rights set out above, please contact us (see Contact Information details above).

- No fee usually required

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. Alternatively, we could refuse to comply with your request in these circumstances.

- What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

- Time limit to respond

We try to respond to all legitimate requests within one month. Occasionally it could take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

How To Complain

Please contact us if you have any queries or concerns about our use of your personal data (see above, 'Contact Information'). We hope we will be able to resolve any issues you may have.

You also have the right to lodge a complaint with:

- the Information Commissioner in the UK, if you are usually resident in the UK; or
- a relevant data protection supervisory authority in the EEA state of your habitual residence, place of work or of an alleged infringement of data protection laws in the EEA.

The UK's Information Commissioner may be contacted using the details at https://ico.org.uk/make-a-complaint or by telephone: 0303 123 1113.

For a list of EEA data protection supervisory authorities and their contact details see here: https://edpb.europa.eu/about-edpb/about-edpb/members_en.

Data Privacy Framework Disclosures

These Data Privacy Framework Disclosures ("Disclosures") describes how Carbyne, Inc., and its subsidiaries and affiliates in the United States ("US") ("Carbyne, Inc.,", "we," or "us") collect, use, and disclose certain personally identifiable information that we receive in the US from the EEA, the UK and Gibraltar ("Personal Data"). These Disclosures supplement our Privacy Policy set out above and unless specifically defined in these Disclosures, the terms in these Disclosures have the same meaning as in our Privacy Policy.

Carbyne, Inc., recognizes that the EEA, the UK, and Gibraltar have established strict protections regarding the handling of Personal Data, including requirements to provide adequate protection for Personal Data transferred outside of the EEA, the UK, and Gibraltar. To provide adequate protection for certain Personal Data about consumers, corporate customers, clients, suppliers, business partners, job applicants and employees received in the US from the EEA, the UK, and Gibraltar, Carbyne Inc., has elected to self-certify to the EU-US Data Privacy Framework, and the UK Extension to the EU-US Data Privacy Framework administered by the US Department of Commerce ("DPF Program"). Carbyne, Inc., complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF, as set forth by the U.S. Department of Commerce. Carbyne, Inc., adheres to the DPF Program Principles of Notice, Choice, Accountability for Onward Transfer, Security, Data Integrity and Purpose Limitation, Access, and Recourse, Enforcement, and Liability and the Supplementary Principles and 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 and the United Kingdom in reliance on the EU-U.S. DPF and the UK Extension to 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.

For purposes of enforcing compliance with the DPF Program, Carbyne, Inc., is subject to the investigatory and enforcement authority of the US Federal Trade Commission. For more information about the DPF Program, see the US Department of Commerce's DPF website: https://www.dataprivacyframework.gov/. To review Carbyne's representation on the DPF list, see the DPF self-certification list which is located at: https://www.dataprivacyframework.gov/list.

Your Rights

Under the DPF, you have rights in relation to your Personal Data. These include, as further described in our Privacy Policy and detailed in these Disclosures:

- Information on the types of Personal Data collected;
- Information on the purposes of collection and use;

- Information on the type or identity of third parties to which your personal data is disclosed;
- Choices for limiting use and disclosure of your Personal Data;
- Access to your personal data;
- Notification of the requirement to disclose your Personal Data in response to lawful requests by public authorities;
- Reasonable and appropriate security for your Personal Data;
- A response to your complaint within 45 days;
- Cost-free independent dispute resolution to address your data protection concerns;

Personal Data Collection and Use

Our Privacy Policy describes the categories of Personal Data that we may receive in the US as well as the purposes for which we use that Personal Data. Carbyne, Inc., will only process Personal Data in ways that are compatible with the purpose that we collected it for, or for purposes the individual later authorizes. Before we use your Personal Data for a purpose that is materially different than the purpose we collected it for or that you later authorized, we will provide you with the opportunity to opt out. Carbyne, Inc., maintains reasonable procedures to help ensure that Personal Data is reliable for its intended use, accurate, complete, and current.

Sensitive Personal Data

When we directly collect sensitive Personal Data, we will obtain your opt-in consent where the DPF requires, including if we disclose your sensitive Personal Data to third parties, or before we use your sensitive Personal Data for a different purpose than we collected it for or that you later authorized.

Data Transfers to Third Parties

Third-Party Agents or Service Providers. We may transfer Personal Data to our third-party agents or service providers who perform functions on our behalf as described in our Privacy Policy. Where required by the DPF, we enter into written agreements with those third-party agents and service providers requiring them to provide the same level of protection the DPF requires and limiting their use of the data to the specified services provided on our behalf. We take reasonable and appropriate steps to ensure that third-party agents and service providers process Personal Data in accordance with our DPF obligations and to stop and remediate any unauthorized processing. We may remain liable for the acts of our third-party agents or service providers who perform services on our behalf for their handling of Personal Data that we transfer to them.

Third-Party Data Controllers

In some cases, we may transfer Personal Data to unaffiliated third-party data controllers. These third parties do not act as agents or service providers and are not performing functions on our behalf. We may transfer your Personal Data to third-party data controllers for the purposes described in our Privacy Policy. We will only provide your Personal Data to third-party data controllers where you have not opted-out of such disclosures, or in the case of sensitive Personal Data, where you have opted-in if the DPF requires consent. We enter into written contracts with any unaffiliated third-party data controllers requiring them to provide the same level of protection for Personal Data the DPF requires. We also limit their use of your Personal Data so that it is consistent with any consent you have provided and with the notices you have received. If we transfer your Personal Data to one of our affiliated entities within our Group, we will take steps to ensure that your Personal Data is protected with the same level of protection the DPF requires.

Disclosures for National Security or Law Enforcement

Under certain circumstances, we may be required to disclose your Personal Data in response to valid requests by public authorities, including to meet national security or law enforcement requirements. We will only do so in accordance with the DPF Principles.

Security

Carbyne, Inc., maintains reasonable and appropriate security measures to protect Personal Data from loss, misuse, unauthorized access, disclosure, alteration, or destruction in accordance with the DPF.

Access Rights

You may have the right to access the Personal Data that we hold about you and to request that we correct, amend, or delete it if it is inaccurate or processed in violation of the DPF. These access rights may not apply in some cases, including where providing access is unreasonably burdensome or expensive under the circumstances or where it would violate the rights of someone other than the individual requesting access.

If you would like to request access to, correction, amendment, or deletion of your Personal Data, you can submit a written request to the contact information provided below. We may request specific information from you to confirm your identity. In some circumstances we may charge a reasonable fee for access to your information.

Opt-out

Carbyne, Inc., respects your privacy rights and offers you the opportunity to choose (opt-out) whether your Personal Data is disclosed to third parties or used for purposes materially different from the original collection purpose. You have the right to opt out of such disclosures or uses. If you would like to exercise your right to opt out of such disclosures or uses, then you can submit a written request to the contact information provided in the section 'Contact Information' in our Privacy Policy. Please note, however, that in certain circumstances, such as when disclosure of your Personal Data is necessary for third parties acting as agents to perform tasks on our behalf and under our instructions, your opt-out right will not be applicable. However, we always establish contractual agreements with such agents to safeguard your personal data as further described under the section "Data Transfers to Third Parties" above.

Complaints

In compliance with the EU-US DPF, and the UK Extension to the EU-US DPF, Carbyne Inc., commits to resolve DPF Principles-related complaints about our collection and use of your personal information. EEA and UK individuals with inquiries or complaints regarding our handling of personal data received in reliance on the EU-US DPF, and the UK Extension to the EU-US DPF should first contact Carbyne, Inc., using the details set out in our Privacy Policy at privacy@carbyne.com or via the contact form available here.

You can direct any questions or complaints about the use or disclosure of your Personal Data to us using those contact details. We will investigate and attempt to resolve any complaints or disputes regarding the use or disclosure of your Personal Data within 45 days of receiving your complaint.

Independent Recourse Mechanism

For any unresolved complaints, we have agreed to cooperate with the EU data protection authorities, or the UK Information Commissioner. If you are unsatisfied with the resolution of your complaint, you may contact the EU data protection authorities or the UK Information Commissioner for further information and assistance. Their details are set out in the Additional Information for EEA/UK Residents.

Contact Us

If you have any questions about these Disclosures or would like to request access to your Personal Data or opt-out as described in these Disclosures, please contact us using the details set out in our Privacy Policy.

Changes To These Disclosures

We reserve the right to amend these Disclosures from time to time consistent with the DPF's requirements.

Effective Date: January 15, 2025

Last modified: April 1, 2023