Gallagher Re Global Privacy Notice
Updated 27 November 2023

This Privacy Notice applies to Arthur J. Gallagher & Co., and all of its affiliates and subsidiaries (collectively, "we," "our," "us," or "Gallagher"). A full list of the Gallagher group of companies is available here.

In this Privacy Notice, we identify the personal data that we collect about you and how we use that data. This Privacy Notice applies to any personal data you provide to Gallagher and any personal data we collect from other sources, unless you are provided a more specific privacy statement at the time of data collection. This Privacy Notice does not apply to any third-party websites, applications or portals ("Sites") linked to Gallagher's Sites, or to any Gallagher Sites that have their own privacy notices. If you provide personal data to us about other people, you must provide them with a copy of this Privacy Notice and obtain any consent required for the processing of that person's data in accordance with this Privacy Notice.

If you have any questions about this Privacy Notice, please contact us using the details set out in the Contact Us section. When using our Sites, you should read this Privacy Notice alongside the Site's Terms of Use.

The following sections will guide you through our practices for the collection, usage, disclosure and retention of your personal data:

1. Who we are

We are a global company providing a range of professional services including insurance, (re)insurance brokerage, risk and claims management, employee benefits and human resources consulting and administration, financial, pension administration and actuarial services through our various affiliates and subsidiaries.

2. How we process your personal data

2.1 Individuals in scope of this Privacy Notice

This Privacy Notice provides information for those individuals whose personal data we process, including:

- **Business contacts**, such as brokers, (re)insurers, managing agents (MGAs), loss adjusters, experts instructed in relation to claims, service providers, suppliers, professional advisors, conference attendees, visitors to our offices, government officials and authorities.
- **Customers, claimants and plan beneficiaries**, such as those in respect of insurance policies we place as part of our core insurance business activities (e.g., parties covered under the policies, potential beneficiaries of the policies, claimants and other parties involved in claims in respect of the policies), and any other customers in relation to our various service offerings (e.g., employers sponsoring health and benefit plans, pension trustees, premium financing services, current, former and retired plan members, spouses and other beneficiaries entitled to payment from pension and/or benefit plans for whom we provide administrative services).

- **Users of our Sites**.
- **Other individuals**, such as those requesting or receiving our marketing information, making general inquiries, entering competitions or promotions, or whose images we use in marketing or are captured on CCTV.

2.2 How we collect your personal data

We collect your personal data in a number of ways, which vary based on how you interact with us and as allowed by applicable law. The following summarizes our various collection points:

- **Directly from you** or your authorized representative, such as when you provide your personal data to us, including from any of our Sites, surveys, live events, market research, and other direct communications and/or solicitations.
- **From our clients and partners**, such as commercial clients, (re)insurers, network partners, brokers, employers, benefit plan sponsors, benefit plan administrators, premium finance companies, health service providers, pension trustees, data/marketing list providers and third-party service providers.
- **Publicly available sources**, such as social media platforms, property and assets registers, and claims and convictions records.
- **Gallagher affiliate companies**.
- **Government authorities**, such as police and regulators.
- **Background checks and screening tools**, such as insurance industry fraud prevention and detection databases, credit agencies and sanctions screening tools.
- **Other third parties**.

2.3 Personal data we collect

We collect the following types of personal data depending on the purpose of your interaction with us (e.g., as business contact, customer, claimant, insured) and as allowed by applicable law:

- **Basic personal and demographic information**, such as your name, date of birth, age, gender and marital status.
- **Contact information**, such as your address, telephone number and email address.
- **Unique identifiers**, such as identification numbers issued by government bodies or agencies (e.g., your national identifier number or social security number, passport number, ID number, tax identification number, driver's license number, birth, death and marriage certificates, military passbook, and copies of official documents).
- **Beneficiary information**, such as details of relationships, family members and dependents.
- **Employment information**, such as your job title, employer, employment status, salary information, employment benefits, pensionable service periods, employment history and professional certifications and training.
- **Financial information**, such as your bank account numbers and statements, credit card numbers, brokerage account numbers, transaction information, tax information, details of your income, property, assets, investments and investment preferences, pension and benefits, debts, and creditworthiness.
- **Policy information**, such as your policy number, policy start and end dates, premiums, individual terms, mid-term adjustments, reasons for cancellation, risk profile, details of policy coverage, enrolment, eligibility for insurance or benefits, benefit amounts and underwriting history.

- **Claim information**, such as a claimant's relationship to a policyholder/insured, claims history and claims data, and the date and particulars of a claim, including causes of death, injury or disability and claim number.
- **Plan information,** such as contributions levels and benefit options
- **Commercial information**, such as records of your personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
- **Events or meeting information**, such as details about your visits to our offices (including CCTV), your interest in and attendance at events or meetings, audio recordings, photographs or videos captured during meetings, events or calls with you.
- **Lifestyle information**, such as travel history and plans and general health data.
- **Special category data and sensitive personal data**, such as data relating to your health (including protected health information), genetic or biometric data, sex life, sexual orientation, gender identity, racial or ethnic origin, political opinions, religious or philosophical beliefs and trade union membership.
- **Criminal records information**, such as criminal charges or convictions, including driving offences, or confirmation of clean criminal records.
- **Professional disciplinary information**.
- **Personal information received from background checks and sanctions screenings,** including status as a politically exposed person.
- **Marketing information**, such as your consent to or opt out from receiving marketing communications from us and/or third parties, your marketing preferences, or your interactions with our marketing campaigns and surveys, including whether you open or click links in emails from us or complete our surveys.
- **Sites and communication usage information**, such as your username, your password, other information collected by visiting our Sites or collected through cookies and other tracking technologies as described in our cookie policy, including your IP address, domain name, your browser version and operating system, traffic data, location data, browsing time, and social media information, such as interactions with our social media presence.

2.4 How we use your personal data

Depending on the purpose of your interaction with us (e.g., as business contact, customer, claimant, insured, pension member), we use your personal data to:

- **Perform services for you or our clients**
    - Provide services and fulfill our contractual obligations, including providing services that you may not have personally requested but were requested by our client(s) and require us to interact, directly or indirectly, with you.
    - Facilitate and enable placement of policies and assist in the ongoing management of such policies, including premium management, renewals, adjustments, cancellations, claims management and settlement.
    - Provide various consulting, administration, financial, pension and actuarial services and claims administration.
    - Advise on the management of our clients' business risks and opportunities, affairs and insurance arrangements and on the administration of claims.
- **Manage our business operations**

- Enter into business relationships and perform due diligence and background checks, such as fraud, trade sanctions screening, and credit and anti-money laundering checks.
- Create, maintain, customize and secure your account with us.
- Maintain accounting records, analyze financial results, comply with internal audit requirements, receive professional advice, apply for and make claims on our own insurance policies, manage or dispute a claim and recover a debt.
- Conduct data analytics, surveys, benchmarking, and risk modelling to understand risk exposures and experience, for the purposes of creating de-identified and/or aggregate industry or sector-wide reports, to share within Gallagher's group of companies and with third parties.

- **Communicate and market to you**
  - Communicate with you regarding your account or changes to our policies, terms and conditions, respond to any inquiries you may have, and send you invitations for events or meetings.
  - Advertise, market and promote our services or the services of others, including by email, LinkedIn, SMS, post or telephone.
  - Send you newsletters, offers or other information we think may interest you, as well as offer and administer promotions.
  - Monitor usage of our Sites and personalize your experience with our Sites and the messages we send you to deliver content, product and service offerings relevant to your interests, including targeted offers and ads through our Sites, third-party Sites, and via email, SMS or text (with your consent, where required by law).
- **Comply with legal obligations**
  - Comply with national security or law enforcement requirements, discovery requests, or where otherwise required or permitted by applicable laws or regulations, court orders or regulatory authorities.
  - Exercise and defend ours, yours or third parties' legal rights.
- **Monitor and prevent fraud or wrongdoing**
  - Maintain the safety, security, quality, integrity and availability of our products, services, systems and data, detect security incidents, protect against inadvertent data loss, malicious, deceptive, fraudulent, or illegal activity, and debug or identify and repair errors that impair existing intended functionality.
  - Monitor and ensure the safety and security of our premises, property, employees and visitors.
- **Improve our services**
  - Develop, enhance, expand or modify our services through research and development.
  - Monitor, review, assess and improve our technology systems, including any Sites, and our content on social media platforms.
  - Improve and develop systems and algorithms involving machine learning and artificial intelligence.
  - Improve quality, training and security (for example, with respect to recorded calls).
- **Mergers and acquisitions**
  - Facilitate commercial transactions, including a reorganization, merger, sale of all or a portion of our assets, a joint venture, assignment, transfer, or other disposition

of all or any portion of our business, assets, or stock (including in connection with any bankruptcy or similar proceedings). Should such a sale or transfer occur, we will use reasonable efforts to ensure the entity to which we transfer your personal data agrees to use it in a manner consistent with this Privacy Notice.

If we intend to use your personal data for any other purpose not described in this Privacy Notice or which is not compatible with the purpose for which your personal data was collected, we will contact you and let you know of that purpose, which may include the need to satisfy our legal and regulatory obligations. Where we require your consent to the processing, we will request it in advance.

2.5 Legal basis for processing personal data

Local law and regulation may require us to have a legal basis to process your personal data. In most cases, our legal basis for processing your personal data will be one of the following:

- **Legitimate Business Interest**, such as seeking to and entering into or performing our contractual duties, maintaining our business records, keeping records of insurance policies or other products we place, and analyzing and improving our business model, services, systems and algorithms. When using your personal data for these purposes, we ensure our business need does not conflict with the rights afforded to you under applicable laws.
- **For the performance of a contract with you** or in order to take steps at your request prior to entering into that contract.
- **Compliance with legal obligations**, such as when you exercise your rights under data protection laws and make requests, for compliance with legal and regulatory requirements and related disclosures and for the establishment and defense of legal rights.
- **Fraud detection or prevention**.
- **Consent,** such as when we have to obtain your consent to process your personal data.

When we process sensitive personal data, sometimes referred to as special category data, in most cases our legal basis will be one of the following:

- **As required to establish, exercise or defend legal claims.**
- **As necessary for insurance operations** when it is in the substantial public interest, where applicable under local data protection laws.
- **As necessary for the prevention or detection of an unlawful act and/or fraud** when it is in the substantial public interest, where applicable under local data protection laws.
- **You have given us your explicit consent**-where we receive sensitive personal data or special category data indirectly, the third party is responsible for obtaining your explicit consent to enable us to collect and use your data for the purposes described in this Privacy Notice.

2.6 Who we share your personal data with

We share your personal data within Gallagher's group of companies for the purpose of your interaction with us, such as for the provision of our services, general business operations and controls, marketing, data analytics, systems and algorithm improvements, surveys, benchmarking, and compliance with applicable laws.

We may also share your personal data with the following third parties for the purpose of your interaction with us:

- **Your employer,** as part of our provision of the services to you or your employer.
- **Professional Advisors**, such as underwriters, actuaries, claims handlers and investigators, surveyors, loss adjustors/assessors, accident investigators, specialist risk advisors, pension providers or trustees, banks and other lenders (including premium finance providers), health professionals, health service providers, lawyers (including third party legal process participants), accountants, auditors, tax advisors, financial institutions, investment advisors and other fiduciaries and consultants.
- **Business partners**, such as customers, (re)insurance companies, MGAs, brokers, other insurance intermediaries, claims handlers or other companies who act as insurance distributors and premium financing companies.
- **Providers of insurance broking and other platforms we use**.
- **Service providers,** such as IT software, security and cloud suppliers, finance and payment providers, marketing agencies, external venue providers, address tracers, printers, document management providers, telephony providers, debt collection agencies, background check and credit reference agencies.
- **Fraud detection agencies and credit bureaus** which operate and maintain fraud detection or credit registers.
- **Industry bodies.**
- **Insurers** who provide you with insurance and us with our own insurance.
- **Regulators, public authorities and law enforcement agencies,** such as police, judicial bodies, governments, quasi-governmental authorities, financial and pension regulators and workers' compensation boards, where we are required or requested to do so by law.
- **Asset purchasers,** such as those who may purchase or to whom we may transfer our assets and business.
- **Other third parties,** where we have your consent or are required by law.

When required by applicable law, we will obtain your explicit consent before sharing your data with any third parties. We will also require third parties (where applicable) to maintain a comparable level of protection of personal data as set out in this Privacy Notice by the use of contractual requirements or other means. On request and where required by law, we will confirm the name of each third party to which your personal data has, or will be, transferred. To the extent permitted by applicable law, we disclaim all liability for the use of your personal data by third parties.

2.7 Children

Our Sites are not intended for children and we do not knowingly collect, use, or disclose information about children. If you are a minor, please do not provide any personal data even if prompted to do so. If you believe that you have inadvertently provided personal data, please ask your parent(s) or legal guardian(s) to notify us. In the event that we learn that we have inadvertently collected personal data via our Sites from a child, we will delete that information as quickly as possible.

3. How we protect your personal data

We use a range of organizational and technical security measures to protect your personal data, including, but not limited to, the following:

- **Restricted access** to those who need to know for the purposes set out in our underlying agreement or this Privacy Notice, and who are subject to confidentiality obligations.
- **Firewalls** to block unauthorized traffic to servers.
- **Physical servers** located in secure locations and accessible only by authorized personnel.
- **Internal procedures** governing the storage, access and disclosure of your personal data.
- **Additional safeguards** as may be required by applicable laws in the country where we process your personal data.

Please note that where we have given you (or you have chosen) a password, you are responsible for keeping the password confidential. Please do not share your password with anyone.

4. How we protect your personal data when sending it internationally

We operate as a global business and may transmit your personal data across borders, including within Gallagher's group of companies and to certain third parties, including our partners and service providers. This sharing of data allows us to provide you services as set out in our underlying agreement or as otherwise indicated in this Privacy Notice. When required by applicable law, we will obtain your explicit consent before transferring your data.

The laws that apply to the country where the data is transferred may not be equivalent to that in your local country (or in the country in which we provide the services). Transfers of personal data will comply with applicable law and be subject to suitable safeguards to ensure an adequate level of protection, including, where required, the use of standard contractual clauses approved by the local data protection regulator, that require each party to ensure that the personal data receives an adequate and consistent level of protection. Please contact us using the details provided under the Contact Us section if you would like further information regarding our international transfers and the steps we take to protect your personal data when sending it internationally.

5. Marketing activities

From time to time, we may provide you with information about our products or services or those of our partners that we think will be of interest to you. We may send you this information by email, LinkedIn, SMS, text, post or we may contact you by telephone. We may also share your personal data with other Gallagher group companies so that they can provide you with information about their products and services we believe will be of interest to you. We ensure that our marketing activities comply with all applicable legal requirements. In some cases, this may mean that we ask for your consent in advance of sending you marketing materials.

You can opt out of receiving marketing communications from us at any time. Please use the "unsubscribe" link in our marketing emails to opt out of receiving those emails. Alternatively, please contact us using the details provided under the Contact Us section. In such circumstances, we will continue to send you service-related communications where necessary.

6. Profiling and automated decision-making

Insurance market participants benchmark insured, beneficiary and claimant attributes and risk factors, and insured event likelihoods in order to determine insurance limits, insurance premiums and fraud patterns. This means that we compile and analyze data in respect of insureds, beneficiaries and claimants to model such likelihoods. In doing so, we use personal and

commercial data in order to create the models and/or match that data against the models (profiling) to determine both the risk and the premium price based on similar exposures and risks. We also use this information to help us advise insurance companies about the typical levels of insurance coverage that our clients may have in place.

We will only make automated decisions about you where:

- Such decisions are necessary for entering into a contract (e.g., we may decide not to offer services to you, the types or amount of services that are suitable for you, or how much to charge you for services based on your credit history or financial or related information we have collected about you);
- Such decisions are required or authorized by law (e.g., fraud prevention purposes); or
- You give your consent for us to carry out automated decision-making. You may withdraw your consent at any time by contacting us.

These automated decisions may have a legal or similar effect on you, namely, your eligibility for or access to products or services.

We may also make automated decisions based on your personal data or browsing history to send you personalized offers, discounts or recommendations, subject to any applicable local laws and regulations. These automated decisions will not have legal or similar effects for you.

Subject to local laws and regulations, you can contact us to request further information about our automated decision-making, object to our use of automated decision-making, or request that an automated decision be reviewed by a human being.

7. How long we keep your personal data

We keep your personal data for as long as reasonably necessary to fulfil the purposes set out in this Privacy Notice based on our business needs and legal requirements.

When we no longer need your personal data, we de-identify or aggregate the data or securely destroy it based on our retention policy. Please note that de-identified or aggregated data is not treated as personal data under this Privacy Notice and may be used for analytics purposes.

We have a detailed retention policy that governs how long we hold different types of information. Please contact us using the details provided under the Contact Us section for further information regarding how long we keep your personal data.

8. Your personal data rights

Based on the country in which you reside, and subject to permitted exemptions, you may have certain rights in relation to your personal data. We are committed to respecting your personal data rights. Please refer to your country-specific addendum for information on the rights that apply to individuals in your country.

You can exercise your rights by contacting us using the details provided in the Contact Us section. We will usually not charge you for processing these requests. There may be cases where we are unable to comply with your request (e.g., via a permitted exemption or where the request would conflict with our obligation to comply with other legal requirements). We will tell you the reason if we cannot comply with your request and we will always respond to any request you make.

9. Contact us

Please contact us if you have any questions about how we collect and process your personal data. You may contact us by writing to GlobalPrivacyOffice@ajg.com. To assist in providing you with an accurate response, please let us know the Gallagher business you interact with and your applicable country.

10. Updates to this Privacy Notice

We may update this Privacy Notice from time to time. When we make updates, we will post the current version on our Sites and will revise the version date located at the bottom of the Privacy Notice. We encourage you to review this Privacy Notice periodically so that you will be aware of our current privacy practices.

11. United States of America Addendum ("Addendum") to the Gallagher Global Privacy Notice

Updated: 27 November 2023

This United States of America Addendum ("Addendum") supplements the terms of Gallagher's Global Privacy Notice and applies to individuals who are residents of California, Colorado, Connecticut, Virginia and Utah and who are acting in their individual or household context. For residents of California, this Addendum also applies to individuals who are acting in their commercial context.

This Addendum provides you with information about your privacy rights under the California Consumer Privacy Act, the California Privacy Rights Act and applicable regulations (collectively referred to as "CCPA"), the Colorado Privacy Act ("CPA"), the Connecticut Data Privacy Act ("CDPA"), the Virginia Consumer Data Protection Act ("VCDPA") and the Utah Consumer Privacy Act ("UCPA"). Any terms defined by the applicable state privacy laws shall have the same meaning when used in this Addendum. "Personal data" as used in this Addendum shall also mean "personal information" as defined by the applicable laws.

1) Personal data we collect

You have a right to know the categories and types of personal data we collect about you. We make this information available to you in the Personal Data We Collect section of our Global Privacy Notice.

For residents of California, Gallagher collects data that identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular California consumer or household ("CCPA Covered Personal Data" or "personal data"). CCPA Covered Personal Data does not include personal data that has been de-identified or aggregated, or that is publicly available information from government records.

In particular, we have collected the following categories of CCPA Covered Personal Data from consumers within the last twelve (12) months:

Category	Examples	Collected
A. Identifiers.	A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers.	Yes
B. Personal data categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)).	A name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, medical information, or health insurance information. Some personal data included in this category may overlap with other categories.	Yes
C. Protected classification characteristics under California or federal law.	Age (40 years or older), race, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status.	Yes
D. Commercial information.	Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.	Yes
E. Biometric information.	Genetic, physiological, behavioral, and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as, fingerprints, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data.	Yes
F. Internet or other similar network activity.	Browsing history, search history, information on your interaction with a Site, application, or advertisement.	Yes
G. Geolocation data.	Physical location or movements.	No

H. Sensory data.	Audio, electronic, visual, thermal, olfactory, or similar information.	Yes
I. Professional or employment related information	Occupation, title, employer information, current or past job history or performance evaluations.	Yes
J. Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99)).	Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records.	No
J. Inferences drawn from other personal data.	Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.	No
L. Sensitive personal data	Social security, driver's license, state identification or passport numbers; account log-in, financial account, debit or credit card number in combination with any required security or access code, password or credentials allowing access to an account; precise geolocation data; racial or ethnic origin, religious or philosophical beliefs or union membership, content of mail, email and text messages unless business is the intended recipient; genetic data; processing of biometric information for the purposes of uniquely identifying a consumer; personal data collected and analysed concerning your health.	Yes

2) Categories of sources from which we collect personal data

You have the right to know the categories of sources from which we collect your personal data. We make this information available to you in the How we Collect Your Personal Data section of our Global Privacy Notice.

3) Our processing of your personal data

You have the right to know how we process and use your personal data. We make this information available to you in the How We Use Your Personal Data section of our Global Privacy Notice.

To the extent that we use or maintain de-identified data, we take reasonable measures to ensure that de-identified data cannot be associated with a natural person, we publicly commit to using and maintaining de-identified data without attempting to re-identify the data, and we contractually obligate any recipient of de-identified data to comply with the same obligations.

4) Disclosure of personal data

You have the right to know if we share your personal data with any third parties and the categories of those third parties. We make this information available to you in the Who we Share Your Personal Data With section of our Global Privacy Notice.

5) We do not sell personal data and we do not share or use personal data for cross-context behavioural advertising or targeted advertising

We do not sell personal data for monetary or other consideration and do not sell the personal data of consumers under 16 years of age.

We also do not share personal data for cross-context behavioural advertising or use your personal data for targeted advertising (as those terms are defined by applicable state law). We may send you advertising in response to your request for information or feedback or based on your activities with our Sites, including your search queries and visits to our Sites. However, we will not send you targeted advertising based on your activities across non-affiliated Sites to predict your preferences or interests.

6) Your rights

Where we act as the controller/business of your personal data (as opposed to a processor/service provider as those terms are defined in your applicable state privacy law), you have the right to submit a request to us for the following:

Your right to access

You have the right to know if we process your personal data and have access to such information and certain details of how we use it.

For California residents, you have the right to request that we disclose the categories of personal data we collected about you, the categories of sources for the personal data we collected about you, our business or commercial purpose for collecting your personal data, the categories of third parties with whom we share your personal data, and the specific pieces of personal data we collected about you. Under California's "Shine the Light" law (Civil Code Section § 1798.83), you also have the right to request certain information

regarding our disclosure of personal data to affiliates and other third parties for their direct marketing purposes.

Your right to data portability

You have the right to obtain a copy of your data in a portable, and to the extent technically feasible, readily usable format that allows you to transmit the data to a third party.

Your right to delete

You have the right to request that we delete your personal data where we act as a controller/business. This right is subject to several exceptions and we may deny your deletion request if retaining the data is necessary for us or our processors/service providers to:

1. Complete the transaction for which we collected the personal data and take actions reasonably anticipated within the context of our ongoing business relationship with you or our client;

2. Detect bugs or errors in our Sites, detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities;

3. Enable solely internal uses that are reasonably aligned with consumer expectations based on your relationship with us;

4. Comply with a legal obligation; or

5. Make other internal and lawful uses of that information as permitted by law or that are compatible with the context in which we collected it.

Your right to correct

We take reasonable steps to ensure that data we hold about you is accurate and complete. However, you have the right to request that we correct any inaccurate personal data that we have about you.

Your right to non-discrimination and no retaliation

We will not discriminate or retaliate against you for exercising any of your rights, including but not limited to, by denying you goods or services, charging you different prices for goods or services, or providing you a different level or quality of goods or services.

Your right to restriction of processing (opt-out)

For residents of Colorado, Connecticut and Virginia, you have the right to opt-out of processing your personal data for purposes of profiling in furtherance of any automated processing of your data that produce legal or similarly significant effects concerning you.

Your right to restrict the processing of sensitive personal data

Unless we are processing your sensitive personal data pursuant to any of the legal exemptions listed below or as otherwise allowed by law:

- For residents of California, we do not use or disclose sensitive personal data for purposes other than those specified in section 7027, subsection (m) of the CCPA regulations and we do not collect or process sensitive personal data for purposes of inferring characteristics about you.
- For residents of Connecticut, Virginia and Colorado, we will not process your sensitive personal data without first obtaining your consent.
- For residents of Utah, we will not process your sensitive personal data without providing you with notice and an opportunity to opt out.

a) Exercising your rights

You may exercise your rights to know, delete and correct as described above by submitting a verifiable request to us by either:

- Emailing us at GlobalPrivacyOffice@ajg.com;
- Completing the Privacy Rights Request Form available at https://cloud.info.ajg.com/privacy-rights-request-form; or
- Calling us at 1-833-208-9359.

b) Authentication or verification process

We will use the personal data you provide in a request only for purposes of authenticating or verifying your identity or authority to make the request.

We will only fulfill requests when we can authenticate or verify your identify and confirm that you have the authority to make such a request.

Only you, you as the parent or legal guardian on behalf of your minor child, or your authorized agent, guardian or conservator may make a request related to personal data. If

an authorized agent, legal guardian or conservator submits the request, we may require your written permission to do so and may require additional information to authenticate or verify your identity. We may deny a request by an authorized agent, legal guardian or conservator who does not submit proof of authorization to act on your behalf.

- **For requests for access to categories of personal data,** we will verify your request to a "reasonable degree of certainty." This may include matching at least two data points that you would need to provide with data points we maintain about you and that we have determined to be reliable for the purposes of verification.

- **For requests for specific pieces of personal data (portability request),** we will verify your request to a "reasonably high degree of certainty." This may include matching at least three data points that you would need to provide with the data points we maintain about you and that we have determined to be reliable for the purposes of verification. We will also require you to submit a signed declaration under penalty of perjury that you are the individual whose personal data is the subject of the request.

- **For requests to delete,** we will verify your request to a "reasonable degree" or a "reasonably high degree of certainty" depending on the sensitivity of the personal data and the risk of harm to you posed by the unauthorized deletion.

c) Response timing and format

We will respond to a verifiable or authenticated request within forty-five (45) days of its receipt, and will notify you within those forty-five (45) days if we require more time to respond and the reasons for the additional time.

If you have an account with us, we will deliver our written response to that account. If you do not have an account with us, we will deliver our written response by mail or electronically, at your option.

If we cannot comply with a request or a portion of the request, we will include the reasons in our response. For residents of California, if we deny your request on the basis that it is impossible or would involve a disproportionate effort, we will explain our reasons, such as the data is not in a searchable or readily accessible format, is maintained for only legal or compliance purposes, or is not sold or used for any commercial purpose and our inability to disclose it, delete or correct it would not impact you in any material manner.

For residents of California, any data we provide in response to a verified request to know will include data we have collected about you on or after January 1, 2022, including beyond the 12-month period preceding our receipt of the request, unless doing so proves impossible or would involve disproportionate effort, or you request data for a specific time period. (Note that the law prohibits us from disclosing at any time a consumer's Social Security number, driver's license number or other government-issued identification number, financial account number, any health insurance or medical

identification number, an account password, security questions and answers, or any unique biometric data.)

We do not charge a fee to process or respond to your authenticated or verifiable request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request. For residents of Colorado, Connecticut and Utah, you may make one request within a twelve-month period at no charge. For residents of Virginia, you may make a request up to two (2) times within a twelve (12) month period at no charge.

Right to appeal

You have the right to appeal our decision within a reasonable period of time after receipt of our response. You may appeal our decision by sending us an email at GlobalPrivacyOffice@ajg.com. We will respond to your appeal within sixty (60) days of receipt (forty-five (45) days of receipt for residents of Colorado) and will inform you of any decisions and the reasons for such decisions.

*Please note that in certain cases we may collect your personal data as a processor/service provider (as opposed to a controller/business, as those terms are defined in your applicable state privacy law) pursuant to a contract we have with a commercial client (the controller/business) to provide a service. In such a case, we are required to collect and process your data only based on the instructions received from the controller/business. Should you direct your requests to exercise your rights to us, we may be required to share your request with the controller/business, who is the party responsible under your applicable state privacy law for receiving, authenticating/verifying and responding to your requests, or we may direct you to make your request directly to the controller/business.

7) Exemptions

This Addendum does not apply to certain data exempt from the applicable state privacy laws, including but not limited to: protected health information collected by a covered entity or business associate and governed by the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), or personal data collected, processed, sold, or disclosed pursuant to certain sector-specific privacy laws, including the Fair Credit Reporting Act (“FCRA”), the Gramm-Leach-Bliley Act (“GLBA”) and the California Financial Information Privacy Act (“FIPA”).

For residents of Colorado, Connecticut, Virginia and Utah Privacy Rights, this Addendum also does not apply to the extent we may be a business associate governed by the HIPAA. For residents of Connecticut, Virginia and Utah Privacy Rights, this Addendum also does not apply to the extent we may be a financial institution subject to the GLBA.