Gallagher

Insurance | Risk Management | Consulting

Global Employee Privacy Notice

Contents

Gallagher

Insurance | Risk Management | Consulting

This privacy notice describes how Arthur J. Gallagher & Co. (which includes its affiliates and subsidiaries, and is collectively the "Gallagher Group") collects and processes personal information about prospective, present, and past employees, contractors, secondees, agency staff and those on work placement (“you”, “your”); how that information is used and protected; and, depending on the country you live in, any rights you may have in relation to your personal information.

The Gallagher Group company which employs you (“we”, “us”) is the controller, business or party responsible for processing your personal information in accordance with this privacy notice.

This privacy notice applies to all personal information that we collect or process about you in association with your employment. Personal information is information, or a combination of pieces of information, that could reasonably allow you to be identifiable or identified.

1. The personal information we collect

We will collect and hold personal information about you from a variety of sources, including information we collect from you directly, and information we collect from other sources.

We may be required by law to collect certain personal information about you, as a result of our relationship with you as your employer. We will inform you at the time your information is collected whether certain personal information is compulsory and the consequences of failure to provide such information.

1.1. Information we collect directly from you

We typically collect your personal information directly from you, for example, when you apply for a job with us, during your onboarding process, when you commence your role, and from time to time throughout your employment when we ask you to provide information.

The types of information that we collect directly from you may include:

a) personal details (e.g. name, title, marital status, gender, date and place of birth, age, language(s) spoken and nationality);

b) contact details (e.g. phone/mobile number, email address and postal address);

c) educational and professional details (e.g. educational history, qualifications, certifications including expiration dates, licenses, skills, membership in professional or trade organizations, CVs, references, interviews and associated notes, cover letters, outside directorships and external business interests);

d) travel and expenses information (e.g. travel booking details, membership numbers, vehicle data, expense claims, gifts, entertainment, hospitality and dietary preferences);

e) other relevant information (e.g. bank account details, remuneration and benefit information, tax information, national identification numbers and training records);

f) citizenship or immigration information (e.g. documents relating to work authorization, such as passports, visa-related documents, details of residency and national identification documents);

g) details relating to dependents and family, next of kin, beneficiaries, and emergency contact information;[1]

h) self-identifying or authenticating information (e.g. passports, birth certificates, driving license and photo identification);

i) absence information (e.g. time off, volunteering); and

j) military service information.

1.2. Information we collect from other sources

The type of information we may collect about you from other sources includes:

a) background check information from employment screening agencies, recruitment agencies or publicly available registers, as allowed by local law (e.g. criminal and credit history, education, employment verification, regulatory references, directorship search, public safety verification and professional qualifications);

[1] We encourage you to inform those whose personal information you provide to us about the content of this privacy notice and to explain the use (including transfer and disclosure) of that personal information by us as set out in this privacy notice.

b) professional profiles available on public or membership only websites or social media (e.g. LinkedIn);

c) health information or claims information from external service providers (e.g. insurance companies, occupational health providers or other companies that help administer our employee benefits);

d) information about your performance or conduct (e.g. from other employees, clients or service providers you work with who may provide feedback about you or participate in your performance evaluations or reviews); and

e) records of qualifications, training and accreditation from educational and professional bodies (e.g. such as the Chartered Insurance Institute).

1.3. Other information we collect about you

The categories and types of information we may collect about you in the course of your employment with us include:

a) compensation and payroll (e.g. employee ID number, salary, bonus, compensation and remuneration pay history and reviews, benefits and awards, working hours, time tracking and absence records, and termination date);

b) position (e.g. start and end date(s), description of current position, job title, role profile, work assignment and location of employment or workplace, work history, relocation dates and details, training records and professional memberships, employing entity name, department, employment status and type, terms of employment, retirement eligibility, exit interview notes, reason for leaving, reporting manager(s) information and workers compensation claims);

c) work performance and history (e.g. time recording, appraisals, commendations, performance and development data, ratings and reviews, grievance, complaint, bullying, harassment and disciplinary information);

d) talent management information (e.g. job application notes, personality assessments, skills assessments, professional development, development programs planned and attended, e-learning programs, and information used to populate employee biographies);

e) audio, video and other electronic data (e.g. call and other audio and video recordings (recorded meetings and webinars) and CCTV footage);

f) building access records (e.g. time recording and other information obtained through paper or electronic means such as swipe card records);

g) data about your compliance with our policies, procedures and standards, your compliance with obligations of confidentiality and other legal and regulatory obligations, as well as your processing of Gallagher Group information, wherever that information is processed, stored or accessed from (e.g. monitoring logs and reviews); and

h) data about your use of our information and communication devices, services and systems however accessed (e.g. usage data, system and application access data, call logs, and geolocation data).

1.4. Sensitive personal information

We may also collect certain information about you, in accordance with local laws, which is considered more sensitive, such as:

a) information about your race, ethnic origin, religious or philosophical beliefs, political opinions, membership of professional or trade associations, disclosed gender identity or sexual orientation;

b) photograph, fingerprint or other biometric identifiers;

c) health or disability status information;

d) absence/attendance information (e.g. sickness records, “fit” notes); and

e) criminal background check information.

2. How we use your personal information and the legal basis on which we use it

We use your personal information to:

a) establish and manage our employment relationship with you, for example recruiting, onboarding, compensation and benefits administration, work visa administration, performance reviews, healthcare, pensions and savings plans, managing absence, managing employee relations issues (including investigating grievances or any allegations of misconduct), training and career development, honoring contractual benefits, performing workforce analysis, restructuring, performing employee surveys, managing travel and business

expenses and reimbursements, employee communications, transfers of and termination of employment;

b) conduct employment and regulatory vetting including criminal, educational, right to work, professional and credit record checks, as permitted by applicable law;

c) determine employment authorization in the applicable jurisdiction to ensure compliance with legal obligations;

d) manage our reporting hotlines;

e) support compliance with our policies and all applicable laws and regulations, for example tax deductions, record keeping, diversity and inclusion monitoring, complying with global trade laws, managing any internal complaints or claims, conducting audits and investigations, safeguarding Gallagher Group information and complying with internal policies and procedures;

f) pursue our legal rights and remedies;

g) cooperate with regulators and law enforcement, governmental or quasi-governmental bodies;

h) contact nominated emergency contacts, dependents, or beneficiaries in the event of an emergency or as otherwise required;

i) conduct business management, financial forecasting, strategic planning, business continuity, record-keeping, company asset and human resources allocation;

j) manage mergers, acquisitions, sales, re-organizations, disposals and integrations;

k) maintain information on the business and technical environment in which we operate, for example, managing product and service development, security management, maintaining audit trails and other reporting tools;

l) safeguard IT infrastructure, systems, office equipment and other property/assets;

m) accommodate a disability or illness;

n) de-identify and aggregate the personal information for any other purposes, provided that no identifiable personal information can be readily identified; and

o) for any other purpose with your consent.

Where we are required by local law to have a legal basis to process your personal information, in most cases our legal basis for processing your personal information will be one of the following:

a) to fulfil our contractual obligations to you in connection with your employment contract with us; failure to provide this information may mean that we cannot fulfil our obligations under our employment contract with you;

b) to comply with our legal obligations, for example obtaining proof of your identity to enable us to meet our anti-money laundering obligations, or obtaining proof of your employment authorization status to enable us to meet relevant work authorization obligations;

c) to comply with our legal obligations to you, for example health and safety obligations that we must comply with as your employer, or to a third party (e.g. tax authorities);

d) to meet our legitimate business operational needs and interests, for example to manage our employees effectively, for budgeting, forecasting, and resource distribution, to protect and safeguard Gallagher Group information, to ensure compliance with obligations of confidentiality, to protect us against theft or other crime, to protect our business from unlawful activity, to allow you access to our technology and resources, and to conduct analytics that allows us to manage our workforce efficiently and plan recruitment activities. When we process personal information to meet our legitimate interests, we put in place robust and reasonable safeguards to ensure that your privacy is protected and to ensure that our legitimate interests are protected and are not overridden by your interests or fundamental rights and freedoms; and

e) to protect your or another person's vital interests, for example by providing your health information to a healthcare provider in an emergency.

We may also obtain your consent to collect and use certain types of personal information when we are required to do so by local law (for example, in certain jurisdictions where consent is required to collect, process and/or transfer personal information or sensitive personal information).

If we ask for your consent to process your personal information, local law may give you the right to withdraw your consent at any time. You can withdraw your consent by contacting us using the details in the “Contact us” section. We will let you know if you have that right at the time we ask for your consent.

3. Your rights over your personal information

Depending on your country of residence and subject to certain limitations, local law may give you certain rights regarding your personal information. These may include rights to:

a) access your personal information;

b) request proof of the authorization or previous consent given to us to collect and process your personal information;

c) correct errors in the information we hold about you;

d) erase your personal information;

e) restrict our use or disclosure of your personal information;

f) object to our use or disclosure of your personal information;

g) request details on the use and processing of your personal information by the Gallagher Group;

h) receive your personal information in a usable electronic format and transmit it to a third party (right to data portability);

i) revoke your consent (where applicable) to the processing of your personal information at any time; and

j) make a complaint with your local data protection authority.

If you would like to discuss or exercise any of these rights, please contact us using the details in the “Contact us” section. We will let you know whether or not the right applies to you.

We encourage you to contact us to update or correct your information if it changes or if the personal information we hold about you is inaccurate.

4. Monitoring tools, profiling and automated decision-making

The Gallagher Group does not base any significant employment-related decision about you based solely on automated processing of your personal information.

Some of the technology we use to protect Gallagher Group confidential information and ensure compliance with internal policies, procedures, the law and our obligations of confidentiality, as well as to protect our legitimate business interests from unlawful activity, monitors; IT usage, call records, print records, transmission of Gallagher Group information and employee communications (e.g. email, transfers of Gallagher Group information to external devices, collaboration tools, portals, websites, cloud applications and storage, use of instant messaging and other collaboration tools, voice and video calls, mobile phones and the Internet) and may automatically filter, record or block the sending of communications, or flag certain communications or actions undertaken for further review, subject to meeting local legal requirements.

5. Information Sharing

We may share your personal information with third parties, for any purpose described in this privacy notice, under the following circumstances:

a) professional advisors: we may share your personal information with accountants, auditors, lawyers, insurers, bankers, consultants and other outside professional advisors;

b) service providers and business partners: we may share your personal information with our service providers and business partners that perform business operations with and/or for us. For example, we may partner with other companies for HR and payroll administration, to provide insurance or other benefits, host the HR database and other applications and to analyze information to improve performance;

c) Gallagher Group companies: we work closely with other businesses and companies that fall under the Gallagher Group Family. We may share certain information about you and your employment with other Gallagher Group companies for human resource management and internal reporting. This includes all companies within the Gallagher Group;

d) law enforcement agency, judicial body, regulator, government, quasi-governmental authority or other third party: we may share your personal

information with these parties where we believe this is necessary to comply with a legal or regulatory obligation, to prevent criminal conduct or other wrongdoing, or otherwise as reasonably necessary to protect our rights or the rights of any third party; and

e) asset purchasers: we may share your personal information with any third party that seeks to purchase or purchases, or to which we transfer, some, all or substantially all of our assets and business. Should such a sale or transfer occur, we will use reasonable efforts to ensure the entity to which we transfer your personal information uses it in a manner consistent with this privacy notice.

Because we operate as part of a global business, the recipients referred to above may be located outside the jurisdiction in which you are located (or in which we provide the services). See the section on "International Data Transfer" below for more information.

When required by applicable law, when we share personal information with corporate third parties we will ensure that those third parties maintain a comparable level of protection for the personal information as set out in this privacy notice by using contractual or other means.

To the fullest extent permitted by applicable law, we disclaim all liability arising from the use of your personal information by third parties. When required by applicable law, data transfers will be logged and documented, identifying the recipient of the data, the purpose of the transmission, and the type of data that was transmitted. On request and where required by law, we will confirm the name of each third party to which your personal information has, or will be, transferred.

6. International Data Transfer

Due to the global nature of Gallagher Group operations, we will transfer certain personal information across geographical borders to our Gallagher Group companies or service providers (working in conjunction with us or on our behalf) to fulfil the purposes described in this privacy notice.

This means that your personal information may be transferred to, stored, and processed outside your local jurisdiction. The data protection laws that apply to the country where your personal information is transferred may not be equivalent to that in your local jurisdiction (or in the jurisdiction in which we provide the services).

Transfers of personal information will be subject to reasonable and appropriate safeguards (such as contractual commitments) in accordance with applicable legal requirements to ensure that your personal information is adequately protected. For more

information on the appropriate safeguards in place, please contact using the details in the "Contact us" section.

7. Information Security and Storage

We implement technical, organizational, administrative and physical measures to help ensure a level of security appropriate to the risk to the personal information we collect, use, disclose, process, de-identify and destroy. These measures are aimed at ensuring the ongoing integrity and confidentiality of the personal information we collect. We evaluate these measures regularly to help ensure the security of the processing. Please be aware that, despite our ongoing efforts, no security measures are perfect or impenetrable.

We restrict access to your personal information to those who require access to such information for legitimate, relevant business purposes.

We will keep your personal information for as long as you remain employed with us. Once our relationship with you has come to an end, we will retain your personal information for a period of time that enables us to comply with our regulatory and/or legal obligations and deal with any post-employment issues such as to:

a) provide you with any continuing benefits such as equity administration, long-term benefits, pension or insurance;

b) maintain business records for analysis and/or audit purposes;

c) comply with record retention requirements under applicable laws and regulations;

d) defend or bring any existing or potential legal claims; and

e) deal with any queries or complaints you may have.

We will de-identify or delete your personal information when it is no longer required for any of these purposes. If there is any information that we are unable, for technical reasons, to delete entirely from our systems, we will implement reasonable measures to prevent any further processing or use of the personal information.

For further information please refer to your local retention requirements: https://ajg0.sharepoint.com/teams/Go-legal.

Gallagher

Insurance | Risk Management | Consulting

8. Contact Us

If you have any questions about how we collect, store or use your personal information contact us by emailing GallagherEthicsandCompliance@ajg.com.

In some jurisdictions, there is a legal requirement to provide the name of the individual responsible for Data Protection.

Country	Role and name
Bermuda	Privacy Officer: Aaron Lutkin
Brazil	Data Protection Officer: br.privacidade@ajg.com or br.privacidade@gallagherre.com
India	Grievance Officer: Sridevi Bangera
Malaysia	Chief Privacy Officer: Sarah Dale +44(0)7395 881 930
South Africa	Information Officer: Amanda Lightfoot

We are committed to working with you to obtain an appropriate and fair resolution of any complaint or concern about privacy. If, however, you believe that we have not been able to assist with your complaint or concern, you may have the right to make a complaint to the data protection authority in your country of residence. Please contact us if you require the contact details of the applicable data protection authority.

9. Changes to the Notice

You may request a copy of this privacy notice from us using the contact details set out in the “Contact us” section. We may modify or update this privacy notice from time to time, under applicable local laws so we encourage you to review this privacy notice periodically.

If we make material changes to this privacy notice, we will notify you of the changes. Where changes to this privacy notice will have a fundamental impact on the nature of the processing of your personal information or otherwise have a substantial impact on you, we will give you sufficient advance notice so that you have the opportunity to exercise any rights you may have under local law (including to object to the proposed changes).

Effective August 22, 2023

Gallagher

Insurance | Risk Management | Consulting

UNITED STATES OF AMERICA: STATE OF CALIFORNIA ADDENDUM TO THE GALLAGHER GLOBAL EMPLOYEE PRIVACY NOTICE

This United States of America: State of California Addendum (the "Addendum") supplements the terms of Gallagher's Global Employee Privacy Notice.

I. CALIFORNIA PRIVACY POLICY

The Addendum applies only to Gallagher employees who are residents of the State of California. For purposes of this Addendum, "you" means residents of the State of California.

This Addendum will provide you with information about our Information Practices and your privacy rights under the California Consumer Privacy Act (CCPA), the California Privacy Rights Act (CPRA) and applicable regulations (collectively referred to as "CPRA"). Any terms defined in the CPRA have the same meaning when used in this Addendum.

1) Personal Information we collect

Gallagher collects information 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 ("CPRA Covered Personal Information" or "personal information"). CPRA Covered Personal Information does not include personal information that has been de-identified or aggregated, or that is publicly available information from government records.

In particular, and in addition to the personal information described in The personal information we collect section of the Global Employee Privacy Note, we have collected the following categories of CPRA Covered Personal Information from consumers (as that term is defined in the CPRA) 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 information 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 information 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.	No
E. Biometric information.	Genetic, physiological, behavioral, and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as, fingerprints, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data.	No
F. Internet or other similar network activity.	Browsing history, search history, information on 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, LinkedIn profile, compensation and benefits information (including next of kin, beneficiaries and dependent information), emergency contact information, documents related to the application or hiring process (such as a CV, cover letter, references, interview notes, licensing information, qualifications, certifications, and similar items), information relating to your authorization to work in the relevant jurisdiction, memberships in trade or professional organizations, outside directorships and external business interests, training information.	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 information.	Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.	No
L. Sensitive Personal Information	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 information collected and analysed concerning your health, and criminal background check information.	Yes

2) Categories of sources from which we collect personal information

You have the right to know the categories of sources from which we collect your personal information. We make this information available to you in The personal information we collect section of our Global Employee Privacy Notice.

3) Our processing of your personal information

You have the right to know how we process and use your personal information. We make this information available to you in the How we use your personal information and the legal basis on which we use it section of our Global Employee Privacy Notice.

4) Disclosure of Personal Information

You have the right to know if we share your personal information with any third parties and the categories of those third parties. We make this information available to you in the Information Sharing section of our Global Employee Privacy Notice.

5) No Sales or Sharing of Personal Information

We do not sell personal information for monetary or other consideration, and we do not share your personal information for cross-context behavioural advertising (as that term is defined in the CPRA). We have also not sold or shared the personal information of consumers under 18 years of age.

6) Use of Sensitive Personal Information

We do not use or disclose sensitive personal information for purposes other than those specified in section 7027, subsection (m) of the CPRA regulations and we do not collect or process sensitive personal information for purposes of inferring characteristics about you.

7) Your CPRA Consumer Rights

You have the following rights:

Your right to Access

You have the right to request that we disclose the categories of personal information we collected about you, the categories of sources for the personal information we collected about you, our business or commercial purpose for collecting your personal information, the categories of third parties with whom we share your personal information; and the specific pieces of personal information we collected about you.

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 may have the right to request that we delete your personal information. This right is subject to several exceptions and we may deny your deletion request if retaining the information is necessary for us or our service providers to:

1. Complete the transaction for which we collected the personal information and take actions reasonably anticipated within the context of our ongoing 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 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 information we hold about you is accurate and complete. However, you have the right to request that we correct any inaccurate personal information 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 under the CCPA.

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 at http://cloud.info.ajg.com/privacy-rights-request-form
- Calling us at 1-833-208-9359

b) Verification Process

We are only required to fulfill verifiable requests. Only you, you as a parent or a legal guardian on behalf of a minor child, or your authorized agent may make a verifiable request related to personal information.

If you submit your request through an authorized agent, we may require you to provide your agent with written permission to do so and verify your identity. We may deny any request by an authorized agent that does not submit proof that the agent has been authorized by you to act on your behalf.

- **For requests for access to categories of personal information,** 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 information (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 consumer whose personal information 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 information and the risk of harm to the consumer posed by unauthorized deletion.

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

c) Response Timing and Format

We will respond to a verifiable 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.

Any information we provide in response to a verified request to know will include information 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.)

If we cannot comply with a request or a portion of the request, we will include the reasons in our response. 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, delete or correct it would not impact you in any material manner.

We do not charge a fee to process or respond to your verifiable request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request.

8) CPRA exemptions

This Addendum does not apply to the following data which is exempt from the CPRA, including but not limited to: medical information governed by the California Confidentiality of Medical Information Act (CMIA); protected health information collected by a covered entity or business associate governed by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), or personal information 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) or California Financial Information Privacy Act (FIPA), and the Driver's Privacy Protection Act of 1994 (DPPA).

Effective January 1, 2023