MCDERMOTT INTERNATIONAL, LTD GLOBAL RECRUITING PRIVACY STATEMENT

Last Updated: *29 October 2025*

At McDermott International, Ltd, together with our subsidiaries and majority-owned affiliates as described in the McDermott Companies section below (collectively, "McDermott," "we," "us," or "our"), we recognize the importance of protecting your ("you" or "your") personal data and are committed to maintaining its privacy and security. We understand that you care about how your information is collected, used, and shared, and we value the trust you place in us.

Scope of this Recruiting Privacy Statement

This Global Recruiting Privacy Statement describes the ways in which McDermott collects, processes, and discloses Personal Data (defined below) about and from you when you apply to work for us or when you are recruited by us.

If we hire you, we will collect additional Personal Data from you and we will supply you with additional applicable employee-related privacy policies at that time. McDermott employees and contractors may access the Global Personal Data Privacy Policy and Notice through McDermott's internal information management system, unifi, to learn more about how we process their Personal Data.

Your access to and use of our websites including our Careers site, apps, social media channels or pages (collectively, the "Websites") is also subject to our Terms of Use.

Definitions

"**Controller,**" "**Business**," "**Data Fiduciary**," or similar terms have definitions that vary slightly across the globe, but it generally refers to a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

"**Cookies**" means small text documents or pieces of code that often include an anonymous unique identifier that are downloaded to your device when you visit a website), web beacons, pixel tags and other similar technologies. Cookies collect information about when and how you visit websites or use mobile applications.

"**Personal Data**," "**Personal Information**," "**Personally Identifiable Information**," or similar terms have definitions that vary slightly across the globe, but these terms generally refer to any information that relates to an identified or identifiable individual. It does not include anonymized data.

"**Process**" means any operation or set of operations performed on Personal Data, whether or not by automated means, such as collecting, recording, organizing, structuring, storing, adapting, altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, aligning or combining, restricting, erasing or destroying Personal Data.

"**Sensitive Personal Data**," "**Sensitive Personal Information**," "**Special Category Data**," or similar terms have definitions that vary slightly across the globe, but these terms generally refer to data that, if mishandled, could cause significant harm to an individual.

"**Third Parties**" means contractors, service providers, and other parties such as recruiting agencies, background or credit screening services, legal advisors, auditors, IT and software providers, communication and analytics providers, and logistics providers that may Process Personal Data on our behalf.

Our Collection and Use of Your Personal Data

Depending on where you reside, the company identified as the recruiting McDermott company is the Controller responsible for processing your Personal Data, either solely or in conjunction with its McDermott affiliates.

We must collect Personal Data, which may include Sensitive Personal Data, from prospective candidates in order to consider them for employment and to comply with other employment-related legal requirements. In the case of contractors, we may collect Personal Data from your employer in order to enter into a contract with you. If you choose not to provide us with certain Personal Data we request, it may limit our ability to assess your application and could affect your consideration for employment opportunities with us.

As part of our legitimate interest to be able to identify and contact qualified candidates for future roles at McDermott, if your initial application is unsuccessful, we may retain the information we collect about you through the recruiting process to assess your suitability for future opportunities that match your skills and experience. We do this by using tools, including automated tools, that help our recruiters identify candidates for open roles. These tools may analyze your resume, work history, education, and skills to suggest roles that may be a good fit. Based on that evaluation, we may use your Personal Data to contact you about your interest in applying for new job openings. Your Personal Data will only be used for recruiting purposes and will not be sold or used for marketing. If you object to our retention of your application information for this purpose, you may delete your candidate profile data or exercise other data privacy-related rights by contacting Privacy@McDermott.com.

The information below describes **what** types of Personal Data we collect, **from whom** we collect it, **what** we use the data for (purpose), and **why** we collect it (lawful bases). Depending on how you interact with us, we do not necessarily (i) collect all data listed in a particular category, (ii) collect all categories of data for all individuals, or (iii) use Personal Data for all the purposes specified.

We have disclosed Personal Data in each of the below categories with our affiliates and third-party service providers for hiring-related purposes within the last twelve (12) months. ***We do not sell your information or share personal information for cross contextual or targeted advertising, nor do we use personal information for profiling or automated decision making that produces legal or similarly significant effects***.

If you live outside the US, please see the International Transfers section for additional information. If you live in California or Texas, please see the Additional Information for California and Texas Residents section below.

1. Identifiers, Contact Data, and Other Information About You

Description: Includes data used to identify or contact you and employment-related data about you such as names, email addresses, phone numbers, work history, work status, job qualifications, and other identifiers.

Source:

- Provided by you, and/or in the case of contractors, by your employer.
- Third parties and educational institutions.
- Cookies (as defined below) or Third Parties that gather our Website visitor data automatically.
- Publicly available information, including social media and networking services.

Purpose of Processing:

- Communicate with you.
- Evaluate your qualifications and suitability for current and future employment opportunities and related recruiting activities, including background screening to verify information provided by you and conducting background, credit, and/or criminal checks where permitted or required by law.
- Facilitate the administration of the interview process.
- Execute and fulfill employment offers or contracts with successful candidates.
- Perform employee or contactor onboarding and meet legal obligations (e.g., data protection, privacy, sanctions, anti-corruption, anti-money laundering).

- Comply with employment-related legal and reporting obligations, enforce legal rights, defend against legal claims, facilitate business transitions (e.g., mergers, acquisitions, bankruptcy).
- Analyze, evaluate, and improve the effectiveness, fairness, efficiency, and inclusivity of our recruitment processes and practices, in accordance with applicable data protection laws and only to the extent necessary for making informed hiring decisions.
- Maintain employment-related business records.
- Physically secure prospective candidates, employees, contractors, offices, fabrication sites, equipment, and assets.
- Detect security incidents and protect against malicious, deceptive, fraudulent, or illegal activity.
- Conduct data analytics to support employment-related activities and strategy.
- Send corporate communications for media and public relations purposes.
- Provide Websites, including displaying required notices and recording Cookie preferences.
- Promote services online and offline and improve Website effectiveness.

Lawful Bases:

- Consent: Provided when you submit your application; other voluntary Personal Data or activities related to your application, such as surveys, and for Cookies chosen by Careers Website visitors that are not strictly necessary Cookies.
- Legitimate Interests: Attract and hire qualified candidates; fulfill future roles/positing efficiently by identifying and contacting qualified candidates; operate our business effectively and profitably; accommodate prospective candidates with disability or accessibility needs; enhance online presence; secure our facilities; defend legal rights; ensure network and information security; prevent and detect fraud or misconduct; operate and investigate claims made through our HelpLine; provide relevant information; and enhance online presence.
- Performance of a Contract: Enter into an employment contract or relationship; to fulfill employment-related contractual obligations.
- Compliance with a Legal Obligation: Meet regulatory and reporting requirements.

2. Image Data

Description: Includes visual data, such as photographs or video recordings, captured via security systems or other means at McDermott locations, including offices, project sites, or hosted events.

Source:

- Security systems (e.g., closed circuit television (CCTV), video surveillance, building access controls) at our offices, fabrication sites, or other assets, with public notice provided where deployed.
-

Purpose of Processing:

- Physically secure prospective candidates, visitors, employees, contractors, offices, fabrication sites, equipment, and assets.
- Detect security incidents and/or protect against malicious, deceptive, fraudulent, or illegal activity.
- Comply with legal and reporting obligations, enforce legal rights, defend against legal claims, and facilitate business transitions (e.g., mergers, acquisitions, bankruptcy).

Lawful Bases:

- Consent: Where applicable, provided when you submit your application. Legitimate Interests: Operate our business effectively; secure our facilities; ensure network and information security; prevent and detect fraud or misconduct; operate and investigate claims made through our HelpLine; and defend legal rights.
- Compliance with a Legal Obligation: Meet regulatory and reporting requirements.

3. Electronic Usage and Technical Data

Description: Includes data related to our Websites' usage, such as browsing activity, technical interactions, or Cookie preferences.

Source:

- Provided by you.
- Social media, our Websites, and technology platforms.
- Cookies or Third Parties that gather our Website visitor data automatically.
- Publicly available data, including social media and networking services.

Purpose of Processing:

- Provide our Websites, including displaying required notices and recording Cookie preferences.
- Promote our job opportunities online and communicate with prospective candidates.
- Assess, analyze, and evaluate current and future recruiting and prospective candidate-related activities and opportunities, and employment-related recruiting

programs and events, including sign-up rates, social media monitoring, and related feedback.
- Analyze, evaluate, and improve the effectiveness, fairness, efficiency, and inclusivity of our recruitment processes and practices, in accordance with applicable data protection laws and only to the extent necessary for making informed hiring decisions.
- Analyze Website usage to evaluate and improved Website effectiveness.
- Detect security incidents and protect against malicious, deceptive, fraudulent, or illegal activity.

Lawful Bases:
- Legitimate Interests: Attract and hire qualified candidates; operate our business effectively; defend legal rights; ensure network and information security; prevent and detect fraud or misconduct; operate and investigate claims made through our HelpLine; improve our Websites; and protect Website visitors.
- Consent: For Cookies chosen by Website visitors that are not strictly necessary Cookies.

4. Social Media Data

Description: Includes data from social media interactions, such as likes, shares, views, and demographic insights.

Source:
- Provided by you.
- Collected via social media, our Websites, electronic job boards, and technology platforms.
- Cookies or Third Parties that gather Website visitor data automatically.
- Publicly available data, including social media and networking services.

Purpose of Processing:
- Publish pages and/or links on social media platforms (e.g., LinkedIn) and electronic job boards to attract prospective candidates; enable discovery, engagement, and updates about our business and related employment opportunities.
- Receive insights from social media platforms and electronic job boards on prospective candidate/user interactions, including views, engagement, actions (e.g., Website visits, clicks), and prospective candidate/user demographics (e.g., age, gender, location).

- Determine which prospective candidates/users have engaged with, commented on, or shared content on social media platforms and electronic job boards.
- Assess, analyze, and evaluate current and future employment-related activities and opportunities.
- Analyze the success of employment-related advertising, events, and marketing programs, including sign-up rates, social media and job board monitoring, and event feedback.

Lawful Bases:

- Legitimate Interests: Attract and hire qualified candidates; operate our business effectively; ensure network and information security; prevent and detect fraud or misconduct; operate and investigate claims made through our HelpLine; improve online presence and Websites; and enhance social media content.
- Consent: In connection with voluntary activities related to your application, such as in your social media postings, and for Cookies chosen by Careers website visitors that are not strictly necessary Cookies.
- Compliance with a Legal Obligation: Meet regulatory requirements.

5. Safety Incident Data

Description: Includes data related to safety incidents, such as emergency medical or transportation needs.

Source:

- Provided by you and/or in the case of contractors, by your employer.
- Collected during any safety incidents at our offices associated with pre-employment activities.

Purpose of Processing:

- Provide or facilitate access to medical treatment or transportation in emergencies or serious safety incidents.
- Comply with legal obligations, enforce legal rights, and defend against legal claims, and facilitate business transitions (e.g., mergers, acquisitions, bankruptcy).

Lawful Bases:

- Legitimate Interests: Secure prospective candidates, employees and assets; manage safety incidents effectively; prevent and detect fraud or misconduct; operate and investigate claims made through our HelpLine; operate our business profitably; and defend legal rights.

- Compliance with a Legal Obligation: Meet regulatory and reporting requirements.
- Vital Interests: Protect the vital interests of individuals in emergencies.
- Consent: Where possible under the circumstances.

Sensitive Personal Data

We will only process Personal Data, including Sensitive Personal Data, during the pre-employment process where you have provided it and we have a lawful basis for doing so, as more fully described herein. During the recruiting and interviewing process and applicable legal and regulatory requirements, we may collect the following Sensitive Personal Data:

- Health information, such as disability-related information if needed for accommodations during the interview process and pre-employment medical evaluations and information associated with determining your ability to perform a job.
- Citizenship and or nationality information to determine work authorization.
- Ethnic origin data to satisfy local employment requirements.
- Where permitted by law, we invite prospective candidates to optionally provide gender data to allow us to analyze, evaluate, and improve the effectiveness, fairness, efficiency, and inclusivity of our recruiting process and practices. We aggregate this information, and do not use it to make hiring decisions or determine eligibility for a role.

Candidate Screening, Artificial Intelligence (AI) Tools

McDermott screens prospective candidates using publicly available or government-issued sanctions lists and media sources to comply with our legal and regulatory obligations related to trade controls/sanctions, anti-money laundering, and/or anti-bribery laws in order to protect our existing personnel and our assets.

We use technology that includes artificial intelligence (AI) to help match candidates with job opportunities. These tools analyze information such as your resume, work history, education, and skills to suggest roles that may be a good fit or to help our recruiters identify suitable candidates.

These AI tools do not make final hiring decisions but may influence which candidates are reviewed or contacted. You may opt out of AI-based matching by contacting Privacy@McDermott.com.

Disclosure of Your Personal Data

We may share your Personal Data with our subsidiaries, affiliates, and trusted Third Parties to help us carry out recruiting and hiring functions. These parties may need access to your data for specific purposes as described above. We put contracts and security measures in

place to protect your data, limit its use, and maintain its confidentiality. We apply the same protections when sharing data within our subsidiaries and affiliates.

Specifically, and subject to the appropriate contractual and consent requirements, we may disclose Personal Data to the following parties:

- To our subsidiaries and affiliates.
- To trusted Third Parties.
- To business partners, buyers or successors in the event of a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of McDermott's assets, including as part of bankruptcy, liquidation, or similar proceedings.

We may also disclose your Personal Data in the following situations:

- To law enforcement or regulatory/government authorities when legally required, to exercise or defend legal rights, or to protect our or others' rights, property, or safety.
- To comply with any court order, law, or legal process, including a response to a government or regulatory request, demand, or investigation.
- To enforce or apply our Terms of Use and other agreements, including for billing and collection purposes.
- If we believe disclosure is necessary or appropriate to protect the rights, property, or safety of our customers, or others, including exchanging information with other companies and organizations for the purposes of fraud protection.
- To fulfill the purpose for which you provide the Personal Data.
- With your consent.
- For any other purpose disclosed when you provide the information.

Our Use of Cookies

We may use Cookies on our Websites. We use certain Cookies (called "strictly necessary Cookies") that must be allowed for our Websites to function and they cannot be switched off. Other functional and analytical and performance Cookies are used for other purposes described in this Global Recruiting Privacy Statement. We collect your consent for Cookies via a Consent Management Platform ("CMP") displayed on our Websites during your first and subsequent visits. The platform provides details about the Cookies we use and their purposes. You can manage your consent any time through the CMP or you can adjust preferences through your browser.

If you wish to exercise your rights under applicable privacy laws, we recommend submitting your Cookie preferences via our consent management platform and/or by submitting a request using one of the methods outlined in the Exercising Your Rights section below. We do not currently support the capability to respond to web browser "do not track" signals.

Our Websites include plugins that link to Indeed. We do not control this platform or its data practices, and we recommend you review their privacy policies and practices for more information. If we receive user data from your interactions with McDermott affiliated pages on these platforms, we may act as joint Controllers of that data.

Retention of Your Personal Data

We keep Personal Data only as long as needed to fulfill the purposes for which we collected it or until you delete your candidate profile. Additionally, we may retain and use your Personal Data as long as necessary to meet legal and regulatory obligations, support business needs, resolve disputes, or enforce agreements. To be clear, we will not delete any Personal Data before the required retention period ends or while a legal or regulatory investigation is ongoing.

We follow a business records retention and information management policy that sets requirements for how long we keep and when we delete records. This policy considers how long we need the records to:

- Conclude contracts and agreements with employees, customers, vendors, and other partners;
- Support our business operations;
- Protect our legal rights; and/or
- Comply with applicable laws and regulations.

Your Personal Data may appear in multiple records and serve different purposes, each with its own retention period based on these factors.

We store video surveillance footage securely and only access it when necessary, such as during safety investigations. Normally, the system automatically deletes footage after a short time unless we need to keep it for an investigation.

Security of Your Personal Data

We are committed to keeping Personal Data secure. We have implemented reasonable and appropriate information security policies and technical, administrative, operational, and procedural measures to protect Personal Data under our control and prevent its unauthorized access or modification, improper use or disclosure, and unlawful destruction

or accidental loss. We use, and we require our Third Parties to use, industry standard security measures for securing and protecting Personal Data, including encrypting data in transit and at rest, limiting access to Personal Data on a least-privileged basis (that is, giving users access only to the Personal Data they need to perform their job). In addition, our personnel and Third Parties are obliged to respect the confidentiality of the Personal Data relating to users of our Websites and our business more broadly.

While we strive to protect your Personal Data, we cannot guarantee the security of your Personal Data transmitted to our Websites. Any transmission of Personal Data is at your own risk. We are not responsible for circumvention of any privacy settings or security measures contained on our Websites.

International Transfers

As a company with global operations, we may transfer Personal Data to and store it on electronic servers in countries other than in which it was collected or from where you may have accessed our Websites. In some cases, our group companies and businesses may transfer Personal Data to Third Parties located in countries that do not have data protection laws that protect Personal Data in the same way as the similar data privacy laws of the originating country. These countries may not give you the same rights as your local data privacy laws and may not have a regulator to help you if you have any concerns.

We only share Personal Data with these Third Parties or other entities within our group of companies when we are legally permitted to do so. When Personal Data is transferred outside of the countries in which it was collected, we will ensure that legally required safeguards protect your Personal Data.

If European Union ("EU") data privacy laws (i.e., the Global Data Protection Regulation, or "GDPR"), the United Kingdom ("UK") GDPR, the Brazilian personal data protection law (the LGPD), or the Chinese personal data protection law (the PIPL) applies, such safeguards may include:

- Contractual safeguards. We may use specific contracts approved by the European Commission ("EC"), the UK, Brazilian, and/or Chinese governments, or any other relevant governmental body to safeguard Personal Data, including for transfers of data among McDermott's group of companies. The contract clauses that we rely on to do this for exports of Personal Data outside the EU and Brazil, respectively, are referred to as Standard Contractual Clauses ("SCCs"); we use the UK International Data Transfer Agreement ("IDTA") for exports of Personal Data outside the UK that are subject to the GDPR. Other exports of Personal Data outside the countries in

which it was collected are covered by contracts containing the SCCs or similar required terms.

- Adequacy decisions. We may also transfer your Personal Data to countries or organisations that have been deemed to provide an adequate level of protection for Personal Data by the EC, or the UK, Brazilian, or Chinese governments, or any other relevant government body, including transfers to organisations that participate in the EU-US Data Privacy Framework.

Your Personal Data-Related Rights

Depending on your location and whether you are considered a "consumer," "data subject," or "data principal," and whether we are considered a Controller, you may have some or all of the following rights in relation to your Personal Data:

- **Right of access/right to know** the categories and specific Personal Data we may collect, the purpose for which we collect it, the parties we may disclose Personal Data to, and whether we disclose Personal Data for business purposes that would be considered a "sale" or "sharing" of Personal Data. You may have the right to obtain Personal Data about you in a portable and, to the extent technically feasible, readily usable format that allows you to transmit the information to another entity without hindrance. Before providing any of this information, we must be able to verify your identity.

- **Right to correct/rectify.** You have the right to request correction of any inaccurate information we hold about you. We may not be able to accommodate your request if we believe it would violate any law, any legal requirements, or cause the information to be incorrect. Information solely retained for data backup purposes is generally excluded. If we have shared your Personal Data with others, we will notify them of the correction where possible, and where possible and lawful to do so, we will also tell you who we have shared your Personal Data with so that you can contact them directly if needed.

- **Right to erasure/deletion (in some countries, "right to be forgotten").** Subject to certain conditions, you are entitled to request that we delete Personal Data about you. Before deleting information, we must be able to verify your identity. We will not delete Personal Data about you when the information is required to fulfill a legal obligation, is necessary to exercise or defend legal claims, or where we are required or permitted to retain the information by law.

  If we are unable to erase or delete your data, we will notify you of that fact. If we have shared your Personal Data with Third Parties, we will request that they erase your Personal Data where possible, and where possible and lawful to do so, we will also tell

you who we have shared your Personal Data with so that you can contact them directly if needed.

- **Right to restrict processing.** Upon your request, we will stop or suppress the processing of your Personal Data in certain circumstances, such as where you contest the accuracy of that Personal Data or you object to us processing it for a particular purpose. We may still store your Personal Data while restrictions are in place and some restrictions that we put in place may only be for a temporary period, but we will tell you if we remove any restriction that we have placed on your Personal Data. If we have shared your Personal Data with Third Parties and where it is possible for us to do so, we will notify them of your requested restriction, and where possible and lawful for us to do so, we will also tell you who we have shared your Personal Data with so that you can contact them directly.

- **Right to object.** You can ask us to stop processing your Personal Data if we are relying upon our own or someone else's legitimate interest to process your Personal Data and we cannot demonstrate compelling legal grounds to continue the processing.

- **Right to complain.** If you have a concern about the way we process your Personal Data, please email us at Privacy@McDermott.com. You can also report any issues or concerns to a national supervisory authority in the country of your residence or the place of the alleged infringement.

Exercising Your Rights

If you would like to exercise one or more of your data privacy rights, please contact us at Privacy@McDermott.com, specifying the right(s) you would like to exercise. If we collect or process Personal Information based on your consent, you may revoke such consent at any time.

To process certain data privacy-related requests, we may be permitted or required by law to collect certain information about you to verify your identity and to prevent fraudulent requests including, to the extent applicable to your relationship with us, first and last name, email address, telephone number, postal address, account information, or other personal identifying information. We will match this information against information we have previously collected about you to verify your identity and to respond to your request. If we cannot verify your identity from the information already maintained by us, we may request additional information from you which will only be used for that purpose.

Depending on where you live, you may have the right to use an authorized agent to submit a request but only if you provide the agent with your written permission. In these situations,

we may also require you to both verify your identity directly with us and provide proof that your agent is authorized to act on your behalf.

Once you contact us, we will make every effort to respond to your request within the timeline in your jurisdiction. If you have a complex request, some privacy laws allow us additional time to respond. If we require additional time, we will notify you to let you know we need more time to respond.

If we decline to take action on your request, we will notify you and explain our reasons for doing so, and we will provide instructions for how to appeal our decision where applicable. Depending on where you live, you may have the right to appeal within a reasonable period of time after you have received our decision. If you have this appeal right, we will inform you in writing of any action taken or not taken in response to the appeal with our reasons within the time period we are allowed for such responses. We will also provide you with a method for contacting your regulator or enforcement agency to submit a complaint.

Please note that under applicable privacy law, and for the protection of your Personal Data, we may be limited in what personal information we can disclose.

We will maintain your rights requests for two (2) years. This information will not be used for any other purpose except to review compliance processes; it will not be shared except as necessary to comply with a legal obligation.

If you live in the following countries, you also have the right to request regulatory assistance or to lodge a complaint with the following regulatory, national, or supervisory authorities:

- **EU**: You can find a list of contact details for all EU supervisory authorities here.
- **UK**: You can find contact details for the Information Commissioner's Office on its website here.
- **Brazil**: You can find complaint information issued by the Autoridade Nacional de Proteção de Dados (ANPD) here
- **Canada**: You can find complaint information issued by the Office of the information & Privacy Commissioner for British Columbia here and the Office of Privacy Commissioner of Canada here
- **China**: You can find complaint information issued by the Cyberspace Administration of China here
- **Mexico**: You can find complaint information issued by the Secretariat of Anti-Corruption and Good Governance here

- **Malaysia**: You can find complaint information issued by the Personal Data Protection Commissioner (Jabatan Perlindungan Data Peribadi) here

Non-Discrimination

We do not discriminate against anyone who wishes to exercise their privacy rights. Specifically, we will not (a) deny you goods or services, (b) suggest we will or actually charge you different prices or rates for goods or services or receiving a different level or quality of goods or services, including by denying you discounts or other benefits or by imposing penalties; or (c) provide you a different level or quality of goods or services.

Links to Other Websites

Our Websites may include links to website plug-ins and applications that direct users to other websites. Clicking on those links or enabling those connections may allow those parties to collect or share data about you. We do not control other parties' websites and are not responsible for their privacy statements. When you leave our Websites, we encourage you to read the privacy policy on every website you visit. If you submit personal information to any third-party websites or service providers, your information is governed by their privacy policies.

Children's Personal Data

We do not, through our Websites or business activities, market or target our business services to children. We do not knowingly collect, sell, or share the personal data of children or minors, as defined by applicable personal data privacy and protection laws and regulations. Should we discover that we have collected a minor's personal data, we will use reasonable efforts to promptly delete the data. If you believe that a minor has provided us with personal data, please contact us.

Additional Information for California and Texas Residents

Information in this section should be read in conjunction with all the other information contained in this Global Recruiting Privacy Statement, including the Sensitive Personal Data section above.

California:

The Personal Information about you that we collect includes information within the categories of data below. These categories also represent the categories of Personal Information that we have collected over the past twelve (12) months. Note that the categories listed below are defined by the California Consumer Privacy Act, as amended by the California Privacy Rights Act, and applicable regulations. Inclusion of a category in the

list below indicates only that we may collect some information within that category. It does not necessarily mean that we collect all information listed in a particular category in all instances.

We have disclosed each of the categories of information below to other parties, including our affiliates and Third Parties, for a business purpose in the past twelve (12) months. **We do not sell your information or share Personal Information for cross contextual advertising, nor do we intend to do so.** We also have not done so for the last twelve (12) months. We do not engage in targeted advertising or profiling of consumers, including prospective candidates, in furtherance of decisions that produce a legal or similarly significant effect concerning the consumer.

1. Identifiers

Description: Includes real name, postal address, email address.

Source: Collected directly from you or in the case of contractors, from your employer; where applicable, from educational institutions and/or references; through Cookies or Third Parties that gather Website visitor data automatically; and from publicly available information, including social media and networking services.

Purpose of Processing:

- Communicate with prospective candidates.
- Evaluate your qualifications and suitability for current and future employment opportunities and related recruiting activities, including background screening to verify information provided by you and conducting background, credit, and/or criminal checks where permitted or required by law.
- Facilitate the administration of the interview process.
- Execute and fulfill employment offers or contracts with successful candidates.
- Perform employee or contactor onboarding and meet legal obligations (e.g., data protection, privacy, sanctions, anti-corruption, anti-money laundering).
- Comply with employment-related legal and reporting obligations, enforce legal rights, defend against legal claims, and facilitate business transitions (e.g., mergers, acquisitions, bankruptcy).
- Analyze, evaluate, and improve the effectiveness, fairness, efficiency, and inclusivity of our recruitment processes and practices, in accordance with applicable data protection laws and only to the extent necessary for making informed hiring decisions.
- Maintain employment-related business records.

- Physically secure prospective candidates, employees, contractors, offices, fabrication sites, equipment, and assets.
- Detect and prevent security incidents and fraudulent or illegal activity.
- Conduct data analytics to support employment-related activities and strategy.
- Send corporate communications for media and public relations purposes.
- Provide Websites, including displaying required notices and recording Cookie preferences.
- Promote services online and offline and improve Website effectiveness.

2. Information About You

Description: Includes information that identifies, relates to, describes, or is capable of being associated with an individual, including name, signature, address, and telephone number.

Source: Collected directly from you or, in the case of contractors, from your employer; from Third Parties; where applicable, from educational institutions and/or references; through Cookies or third-party service providers that gather Website visitor data automatically; and publicly available information, including social media and networking services.

Purpose of Processing:

- Communicate with prospective candidates, including calling, emailing, and reviewing, evaluating, and processing applications.
- Evaluate your qualifications and suitability for current and future employment opportunities and related recruiting activities, including background screening to verify information provided by you and conducting background, credit, and/or criminal checks where permitted or required by law.
- Facilitate the administration of the interview process.
- Execute and fulfill employment offers or contracts with successful candidates.
- Perform employee or contactor onboarding and meet legal obligations (e.g., data protection, privacy, sanctions, anti-corruption, anti-money laundering).
- Comply with employment-related legal and reporting obligations, enforce legal rights, defend against legal claims, and facilitate business transitions (e.g., mergers, acquisitions, bankruptcy).
- Analyze, evaluate, and improve the effectiveness, fairness, efficiency, and inclusivity of our recruitment processes and practices, in accordance with applicable data protection laws and only to the extent necessary for making informed hiring decisions.
- Maintain employment-related business records.
- Physically secure prospective candidates, employees, contractors, offices, fabrication sites, equipment, and assets.

- Detect and prevent security incidents and fraudulent or illegal activity.
- Conduct data analytics to support employment-related activities and strategy.
- Send corporate communications for media and public relations purposes.
- Provide Websites, including displaying required notices and recording Cookie preferences.
- Promote services online and offline and improve Website effectiveness.

3. Internet or Other Electronic Network Activity Information

Description: Includes data related to our Websites' usage, such as browsing activity, technical interactions, or Cookie preferences.

Source: Collected directly from you, through Cookies or third-party service providers that gather Website visitor data automatically, and publicly available information, including social media and networking services.

Purpose of Processing:

- Provide our Websites, including displaying required notices and recording Cookie preferences.
- Promote our job opportunities online and communicate with prospective candidates.
- Assess, analyze, and evaluate current and future recruiting and prospective candidate-related activities and opportunities, and employment-related recruiting programs and events, including sign-up rates, social media monitoring, and related feedback.
- Analyze, evaluate, and improve the effectiveness, fairness, efficiency, and inclusivity of our recruitment processes and practices, in accordance with applicable data protection laws and only to the extent necessary for making informed hiring decisions.
- Detect security incidents and protect against malicious, deceptive, fraudulent, or illegal activity.
- Publish pages and/or links on social media platforms (e.g., LinkedIn) and electronic job boards to attract prospective candidates; enable discovery, engagement, and updates about our business and related employment opportunities.
- Receive insights from social media platforms on prospective candidate/user interactions, including views, engagement, actions (e.g., Website visits, clicks), and prospective candidate/user demographics (e.g., age, gender, location).
- Determine which prospective candidates/users have engaged with, commented on, or shared content on social media platforms.
- Assess, analyze, and evaluate current and future employment-related activities and opportunities.

- Analyze the success of employment-related advertising, events, and marketing programs, including sign-up rates, social media monitoring, and event feedback.
- Analyze Website usage to evaluate and improved Website effectiveness.

4. Geolocation Data

Description: Includes geolocation-related information.

Source: Collected directly from you, through Cookies or third-party service providers that gather Website visitor data automatically, and publicly available information, including social media and networking services.

Purpose of Processing:

- Support operational functions, including interviewing and employment-related functions, including calling, emailing, and processing applications.
- Detect security incidents and protect against malicious, deceptive, fraudulent, or illegal activity.
- Conduct data analytics to support employment-related activities and strategy.

5. Sensory Data

Description: Includes audio or visual data including photographs or video recordings captured via our security systems.

Source: Security systems (e.g., closed circuit television (CCTV), video surveillance, building access controls) at our offices, fabrication sites, or other assets, or hosted events.

Purpose of Processing:

- Physically secure McDermott prospective candidates, employees, contractors, offices, fabrication sites, equipment, and assets.
- Detect and prevent security incidents and fraudulent or illegal activity.
- Comply with legal obligations, enforce legal rights and defend against legal claims.
- Facilitate actual or proposed business transitions, such as mergers, acquisitions, joint ventures, consortia, reorganizations, asset sales, bankruptcies, or other insolvency events involving some or all of our assets.

Texas residents (not applicable to McDermott employees and business partners):

Under the Texas Data Privacy and Security Act, you have the following rights to:

- **confirm** whether we are processing your Personal Data and to **access** it;
- **correct** your Personal Data if it is not accurate, taking into account the nature and purpose of the processing of your Personal Data;
- **request deletion** of the Personal Data you have provided or that we have obtained about you;
- **obtain a copy** of your Personal Data that we process if it is available in a digital format; and
- **not be discriminated against** based upon your choices and/or requests you may make in connection with your Personal Data.

We do not sell your Personal Data or share your Personal Data for targeted advertising, so we do not offer an option for you to "opt-out" of the sale or sharing of your Personal Data.

If you are a Texas resident and wish to exercise your consumer rights or if you wish to appeal a decision we have made about your request, please contact us at Privacy@McDermott.com. We will notify you in writing within sixty (60) days after we receive your appeal request of any action we take or do not take on your request, including an explanation of the reason(s) for our decision. If you are not satisfied with our response, you may contact the Texas Attorney General by clicking here or by calling its Consumer Protection Hotline at 1-800-621-0508.

McDermott Companies

McDermott is comprised of (a) McDermott International, Ltd, (b) its subsidiaries, and (c) any majority-owned affiliated companies (e.g., those companies or partnerships in which McDermott International, Ltd directly or indirectly owns or controls more than 50% of the ownership interest of, or in which McDermott International, Ltd has the right to vote or appoint directors or functional equivalents), and/or (d) any joint venture in which McDermott International, Ltd has operational control. The controller or entity responsible for the activities described in this Global Recruiting Privacy Statement will be the McDermott company that provides services to you (or the organization you are employed by) or that you otherwise interact with.

Updates to this Statement

This Global Recruiting Privacy Statement is subject to periodic updates at our discretion. We will revise the effective date at the top of the document when we make updates.

Contact Us

If you have questions or would like more information about this Global Recruiting Privacy Statement, please contact us by emailing us at Privacy@McDermott.com and GPS.EEE@McDermott.com.