



United States Candidate Notice

Introduction

This privacy notice ("Candidate Notice") describes how Baker & McKenzie LLP and/or Baker & McKenzie LLC ("firm," "we," or "us"), will collect, process, and use your personal data when you apply for a current or future position with us at one of our offices in the United States. If you are offered a job or become an employee, the personal data you provide during the application process will be used for employment related purposes.

Collection of Personal Data

We may collect or obtain personal data about you from various sources, including:

- Directly from you (e.g., when you contact us).
- When you make your personal data public (e.g., via a job board).
- When you use our software or visit our sites.
- From third parties (e.g., referrals).

Use of Personal Data

We use personal data for the following purposes:

- Administering and processing your application;
- Determining your suitability for the role(s) for which you applied or for similar roles within the firm;
- Determining the need to provide you appropriate adjustments or accommodations during the recruitment process or employment;
- Determining your eligibility to work in the jurisdiction;
- Conducting background checks as part of your application;
- Conducting internal audits and workplace investigations;
- Compliance with applicable laws and regulations, companies policies and procedures, and employment-related requirements;
- Supporting any claim or defense the firm may face before any jurisdictional and/or administrative authority, arbitration, or mediation panel;
- Cooperating with or informing law enforcement or regulatory authorities to the extent required by law;
- Authentication and security purposes;

- Completing the on-boarding/new hire process, should you be offered and accept a position with the firm;
- Diversity and legal compliance monitoring;
- To perform the services or provide the goods reasonably expected by you in your role, including those services and goods that are reasonably necessary for us to administer the application process and for our employees to perform their duties;
- To prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal information, including in or via our premises, computers, software, networks, communications devices, and other similar system;
- To resist malicious, deceptive, fraudulent or illegal actions directed at us and to prosecute those responsible for those actions;
- To ensure the physical safety of natural persons;
- For short-term, transient use;
- To perform services on behalf of us;
- To verify or maintain the quality or safety of our services and products;
- To improve, upgrade, or enhance our services and products;
- To perform functions that are required under laws that apply to us; and
- To collect or process it where such collection or processing is not for the purpose of inferring characteristics about a consumer.

Disclosure of Personal Data

We may share personal data with third parties such as:

- Other firm members and affiliates.
- Third-party service providers who perform services on our behalf.
- Regulatory bodies and law enforcement agencies as required by law.

Data Retention

We retain personal data for the longer of as necessary to fulfill the purposes for which it was collected and any additional time periods necessary for the compliance with laws, exercise or defense of legal rights, and archiving, back-up and deletion processes.

California Residents

If you are a resident of California, please see our California Consumer Privacy Act (CCPA) disclosures below in respect of the personal information of job applicants or other potential employees we process as a Business. Please see our [California Consumer Privacy Act Disclosures | Baker McKenzie](#) to learn more about your rights under California law.

What Categories of Personal Information Do We Collect?

Non-Sensitive Personal Information:

- Identifiers such as 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.
- Any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her 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, or any other financial information, medical information, or health insurance information, but excluding publicly available information that is lawfully made available to the general public from federal, state, or local government records.
- Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website application, or advertisement.
 - Specifically, cookies and other data linked to a device, and data about usage of our sites.
- Geolocation data.
 - Specifically including via IP address.
- Audio, electronic, visual, thermal, olfactory, or similar information.
 - Specifically including data relating to your use of computers, software, networks, communications devices, and other similar systems that we or our affiliates own or make available to you and information relating to your activities on our or our affiliates' premises including as captured by routine video monitoring for security purposes.
- Professional or employment-related information
- Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99).
- Inferences drawn from any personal information to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.
 - Specifically including for any applicant that applies to our roles we look at their resume/cv and review that against our role description for the position. If the relevant requirements of our role description are demonstrated by the candidate's resume/cv, we could consider them as a candidate for the role and short-list for consideration to interview.

Sensitive Personal Information:

- A consumer's social security, driver's license, state identification card, or passport number.
 - Specifically including ID confirmation provided at the hire stage if applicable when completing I-9 form. In addition, we ask for social security number.
- A consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account.
 - Specifically including applicants creating an account with an applicant tracking system.
- Personal information collected and analyzed concerning a consumer's health.
 - Specifically including for accommodations requested as part of the interview process.

For What Purposes Do We Collect and Use Personal Information?

We use personal and sensitive personal information about you as a job applicant or other potential employee for the purposes of:

Non-Sensitive Personal Information

- Administering and processing your application
- Determining your suitability for the role(s) for which you applied or for similar roles within the firm
- Determining the need to provide you appropriate adjustments or accommodations during the recruitment process or employment
- Determining your eligibility to work in the jurisdiction
- Conducting background checks as part of your application
- Conducting internal audits and workplace investigations
- Compliance with applicable laws and regulations, companies policies and procedures, and employment-related requirements
- Supporting any claim or defense the firm may face before any jurisdictional and/or administrative authority, arbitration, or mediation panel
- Cooperating with or informing law enforcement or regulatory authorities to the extent required by law
- Authentication and security purposes
- Completing the on-boarding/new hire process, should you be offered and accept a position with the firm; and
- Diversity and legal compliance monitoring

Sensitive Personal Information

- To perform the services or provide the goods reasonably expected by you in your role, including those services and goods that are reasonably necessary for us to administer the application process and for our employees to perform their duties;
- To prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal information, including in or via our premises, computers, software, networks, communications devices, and other similar system;
- To resist malicious, deceptive, fraudulent or illegal actions directed at us and to prosecute those responsible for those actions;
- To ensure the physical safety of natural persons;
- For short-term, transient use;
- To perform services on behalf of us;
- To verify or maintain the quality or safety of our services and products;
- To improve, upgrade, or enhance our services and products;
- To perform functions that are required under laws that apply to us; and
- To collect or process it where such collection or processing is not for the purpose of inferring characteristics about a consumer.

What Criteria Do We Consider When Retaining Personal Information?

In general, with respect to categories of personal and sensitive personal information about job applicants and other potential employees of the firm, we retain each category until the withdrawal or rejection of your application, or if you are engaged by the firm, until the end of your employment, and any additional time periods necessary for the compliance with laws, exercise or defense of legal rights, and archiving, back-up and deletion processes.

Contact Information

If you have any questions or concerns about this notice or our data privacy practices, please contact us at:

Office of General Counsel- Data Privacy
Baker & McKenzie Global Services NI Limited
City Quays One, 7 Clarendon Road, Belfast, BT13BG, United Kingdom
Email: dataprivacy@bakermckenzie.com