NIXON PEABODY PRIVACY PRACTICES – PERSONNEL

This policy and notice of privacy practices explains how and why we collect, use, and share information to facilitate the employment relationship or administer benefits. It applies to current and former Nixon Peabody personnel, as well as prospective employees and partners. Further information for current employees about your privacy when you use firm technology resources is available in the firm's Responsible Use of Technology policy. Information provided to the firm outside of the employment relationship, is governed by the general Nixon Peabody Privacy Policy, available here.

INFORMATION WE COLLECT

When you apply for a position at the firm, we collect contact information and information about your education, background and professional experience(s) from you.

When you are offered a job with the firm, we collect a wide range of personal information, including sensitive information, directly from you and from third-party sources, in order to perform background screening and conflicts checks.

When you work at the firm, we collect additional personal information, directly from you and from third parties, in order to administer benefit programs, pay our personnel, review and pay for expenses, foster professional development, and for other firm administrative and operational purposes.

WHERE WE GET PERSONAL INFORMATION

Directly from you, such as when you fill out an online form or share information with human resources, employee benefits or finance personnel

Indirectly from you, when you browse our website, access and use other firm technology resources

From Nixon Peabody vendors that support operations and administration, such as background screening services, payroll and benefits administrators

HOW WE USE PERSONAL INFORMATION

Nixon Peabody may use and disclose your personal information to further its legitimate business purposes (e.g., for operational and administrative uses) and/or with your consent. These uses will vary depending on the nature of our relationship with you, but include:

- To administer employee benefits and payroll
- To facilitate professional development
- To track billing and expenses
- To provide you with technology resources
- To provide alerts and corporate communications, e.g., workplace emergencies, updated benefits information

- To operate, troubleshoot, analyze and improve the firm's technology resources, e.g., email, document management, intranet
- As reasonably necessary and appropriate, to detect or prevent fraud, to comply with legal obligations, or protect your, our, or others rights
- To allow Nixon Peabody to pursue remedies or limit liabilities if a dispute arises
- To fulfill other purposes permitted or required by law
- For other uses disclosed to you, with your consent

WHEN WE SHARE PERSONAL INFORMATION

We share information with third parties for operational and administrative purposes, when we have your consent, or when required by law.

When required or appropriate and feasible, we obtain written assurances from third parties that access personal information that their privacy and security practices are in accord with applicable legal requirements.

Nixon Peabody may share personal information with its affiliates and subsidiaries for the purposes set out in this policy. However, under no circumstances does Nixon Peabody sell, trade, barter or exchange the information. We may also disclose your personal information to third parties where we sell or merge any or all of our business and/or our assets to a third party, or where we are legally required to disclose your information.

LINKS TO OTHER THIRD PARTIES

Our website and NP Connect may link to third-party sites and services that we do not control. Our website and NP Connect may include integrated content or links to third parties, e.g. for recruiting purposes, social media platforms, employee benefits providers, meal-delivery services. This personnel privacy policy does not address the privacy, security or other practices of these third-party service providers, where you are sharing information directly with them. Please review the privacy policies of such third-party providers before submitting personal information to them.

PRIVACY PRACTICES: FINER PRINT

The chart below provides more detailed information about the information we collect, the reason we collect it, and with whom it may be shared, e.g., the categories of third parties with whom your

information may be shared. The chart further notes whether that information has been collected or disclosed in the past 12 months.

PERSONAL INFORMATION	REASON FOR COLLECTING AND/OR SHARING	CATEGORIES OF THIRD PARTIES	COLLECTED OR DISCLOSED IN PAST 12 MONTHS
Common identifiers, e.g. 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.	Legal recruiting, background screening, administration of employee benefits, payroll, corporate communications, operation of technology resources	Benefits administrators; banks and related financial services; expense and payroll processing; information technology and security providers; document management and storage vendors; legal and other professional support vendors; government agencies	Collected and disclosed
Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)). This includes: 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, or any other financial information, medical information, or health insurance information. Some personal information included in this category may overlap with other categories.	Legal recruiting, background screening, administration of employee benefits, payroll, corporate communications, physical (office building) security, operation of technology resources	Benefits administrators; banks and related financial services; expense and payroll processing; information technology and security providers; document management and storage vendors; legal and other professional support vendors; government agencies	Collected and disclosed

Protected classification characteristics under California or federal law. This includes: Age (40 years or older), race, color, ancestry, 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, genetic information (including familial genetic information).	Legal recruiting; immigration-related services, background screening, administration of employee benefits	Information technology and security providers; document management and storage vendors; legal and other professional support vendors; government agencies	Collected and disclosed
Commercial information. This includes: Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.	This information may be collected from publicly available sources or third-party vendors for screening prospective employees and partners	Not applicable	Collected
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.	Personnel may choose to use a fingerprint or faceprint ID to secure a firm-provided or firm-supported laptop or other mobile. However, this information is not stored on firm servers or accessible to other firm personnel.	Not applicable	Not applicable
Internet or other similar network activity. Browsing history, search history, information on a consumer's interaction with a website,	The firm has the ability to track and audit users access and use of firm-provided technology	Information technology and security vendors	Collected

application, or advertisement.	resources for IT security and compliance purposes.		
Geolocation data. Physical location or movements.	This information may be collected when firm personnel submit information collected from ride-sharing or similar sites for expense reports, and when enabled on firm-connected mobile devices and laptops	Expense reporting and payment processing vendors	Collected and disclosed
Sensory data. Audio, electronic, visual, thermal, olfactory, or similar information.	The firm may make audio and visual records of events or meetings; photos may be used for internal and external websites and for security purposes	Communications support vendors	Collected and disclosed
Professional or employment-related information. Current or past job history or performance evaluations.	Collected from job applicants on a third-party site accessible from NixonPeabody.com; the firm maintains personnel files on current and former personnel as may be required by law or the rules of professional responsibility	Background screening services; information technology and security providers; document management and storage vendors; other third parties with consent or as required by law or the rules of professional responsibility	Collected and disclosed
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.	Collected from job applicants on a third-party site accessible from NixonPeabody.com; the firm maintains personnel files on current and former personnel as may be required by law or the rules of professional responsibility	Background screening services; information technology and security providers; document management and storage vendors; other third parties with consent or as required by law or the rules of professional responsibility	Collected and disclosed

Inferences drawn from other personal information. Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.	Employee satisfaction and similar polling, and professional development activities (e.g. online training activities) may create profile data	Human resource vendors	Collected and disclosed

LEGAL RIGHTS FOR EUROPEAN RESIDENTS

Under the European Union's General Data Protection Regulation ("GDPR"), transfers of personal information from the European Economic Area (EEA) may be made to jurisdictions that provide adequate protections to the rights of data subjects in the European Union. The United States has not been deemed to provide such protection; therefore, we more generally rely on the following lawful bases for cross-border transfers from the EEA: standard contractual clauses, and the derogations available for contracts and consent.

In addition, residents of the European Union, whose personal information, has been provided to the firm, may have additional rights under the GDPR, including, among other things, the right to see a copy of your Personal Information, the right to correct inaccurate information, the right to object to or restrict use of your information, and the right to have your Personal Information erased. If you would like to discuss or exercise these rights, or have additional questions about our compliance with the GDPR, please contact compliance@nixonpeabody.com.

Nixon Peabody International LLP, which is based in London, is the firm's representative with respect to the General Data Protection Regulation. Nixon Peabody International LLP can be reached at 17 Hanover Square; London W1S1BN; United Kingdom; or, +44 (0) 20 7096 6600

DATA SECURITY

Nixon Peabody secures data through a mix of technical and administrative safeguards that are audited annually by third-party information security experts. The firm's Rochester, NY data center has been certified as compliant with ISO 270001, a globally recognized standard for information security. Nixon Peabody also has policies and procedures designed to promote commercially reasonable security practices in accord with US and international requirements. Nonetheless, the transmission of information via the Internet is not completely secure and we cannot guarantee the security of data sent to us electronically over cellular and wireless networks that we do not control.

CHANGES TO THIS PRIVACY POLICY

The effective date of this policy is January 1, 2020 and it was last reviewed on December 21, 2019. It will be reviewed at least annually, and updated in accord with evolving privacy practices and requirements. We encourage you to periodically review this page. If we make any material changes in the way we collect, use and/or share the personal information that you have provided, we will notify you.

CONTACT INFORMATION

If you have any questions or comments about this policy or the ways in which Nixon Peabody collects and uses your information, please do not hesitate to contact us at:

Phone: 617-345-1037

Email: compliance@nixonpeabody.com or sragland@nixonpeabody.com

Postal Address:

Nixon Peabody LLP
Exchange Place
53 State Street
Boston, MA 02109
Attn: Sarah Ragland, Compliance Officer