**SEYFARTH - DATA PROTECTION NOTICE**

We are providing you with this data protection notice (**Notice**), as required by the General Data Protection Regulation ("GDPR"), to inform you about our practices regarding the processing of your personal data. You should read this Notice in conjunction with our Caribou Privacy Policy.

References in this Notice to "we", "us" or "our" are a reference to the attorneys or employees of the Seyfarth partnerships listed below:

| Company Name | Contact Details |
|---|---|
| Seyfarth Shaw LLP | dataprotection@seyfarth.com |
| Seyfarth Shaw LLP (UK) | dataprotection@seyfarth.com |

**Categories of Personal Data Processed**

We will typically collect your personal data from you, either directly, or through your interaction with our information technology resources. We may also collect personal data about you from third parties (that is, individuals and organizations that are not part of Seyfarth). These third parties will include government agencies, third parties to whom we provide services which involve you, and third parties who provide services to you or to us in connection with the legal services we provide. We will also create records of personal data about you. We will collect personal data about you in accordance with the ethical obligations we are required to follow in the course of providing legal representation, including our duty of confidentiality and duty of loyalty to you if you are a client.

The personal data about you that we may collect includes the following categories of data:

- **Personal and Family Information:** information such as name(s) (and any former name(s)), home address, home and mobile telephone number, personal e-mail address, date and place of birth, nationality, gender, governmental social security or insurance number, passport number, driver's license number, photograph, family status (e.g. marital status, dependents), details of family members (name, date of birth, relationship to employee, nationality and marital status) and emergency contact (name, address and telephone number).

- **Employment Information**: information such as job application (e.g., CV, education history and certificates, notes of candidate interviews, decisions to offer employment, background information, third-party references); immigration-related details; employment contracts (start date of employment); job descriptions (business unit, grade, function, job family, code and type, status (full-time or part-time)); work location (area, department, cost center, desk location, shift, hours) and contact details; employment and career history (job titles, transfers, promotions, managers or supervisors, reporting structure); termination details (end date of employment); working time and work schedule records, absence records, leave or vacation records, sickness certificates, work-related disabilities or health conditions, accident reports; your performance information (including any appraisals or other internal communication regarding performance), disciplinary or grievance procedures, skills records, training records, records of projects you have worked on, professional memberships; salary and pay records (frequency and pay) and any deductions, bonus, health insurance, pension arrangements, benefits provided to you (gym membership etc.); bank account details, including payroll information, tax codes, expense information; and any other information necessary in connection with your immigration case.

- **Other Information**: other information collected for reasons related to your immigration case. We will collect and further process sensitive personal data, such as medical information and information which may reveal your race or ethnicity, your sexual orientation or gender identity, your religious or philosophical beliefs, or your trade union membership, only when necessary and permitted to do so by law, on the basis outlined in this Notice.

**Legal Basis and Purposes for Processing Personal Data**

We process personal data about you because it is necessary for one or more of the following:

- the performance of a contract between you and us or in order to take steps at your request prior to entering into a contract;
- the performance of a contract between your employer and us;
- compliance with a legal obligation that applies to us; or
- the purposes of our legitimate interests, except where such interests are overridden by your interests or fundamental rights and freedoms relating to protection of personal data. In general, our legitimate interests for processing your personal data are ensuring the efficient administration of your immigration case and the efficient management of our business.

In general terms, we process personal data about you for the purposes of providing services in connection with your immigration case, administering our workforce generally and running our business operations. Processing for these general purposes includes processing for the following specific purposes:

- communication with you;
- communication with third parties necessary in connection with your immigration case;
- compliance and risk management;
- investigations and audits by Seyfarth or government or supervisory authorities;
- internal technical and operational support; or
- compliance with law.

We will collect and further process sensitive personal data about you only when such processing:

- has been consented to by you, or is under your instruction;
- is necessary for reasons of substantial public interest (e.g. equality of opportunity or treatment);
- is necessary for the establishment, exercise or defense of legal claims; or
- is necessary for a reason for which such processing is permitted expressly by law.

**Transfers of Personal Data**

We transfer information relating to our operations, including personal data about you, to other entities within the Seyfarth group of partnerships. We do this in order to streamline and improve the provision of legal services and our overall business operations. Seyfarth has attorneys who operate in countries that European authorities have identified as not having alevel of legal protection for personal data that is equal to the GDPR (**Non-Adequate Country**). Non-Adequate Countries include the United States of America. There are intercompany agreements between the several Seyfarth partnerships that include Standard Contractual Clauses, approved by relevant European authorities, requiring those partnerships operating in a Non-Adequate Country to safeguard any personal data about you, to comply with EU Data Protection Authorities, and to honor your privacy rights in relation to cross-border processing or storage of personal data.

We may transfer personal data about you to third parties in accordance with this Notice. The broad classes of third parties to which we may transfer your personal data include: our IT infrastructure

providers; our document archive administrator; other service providers that process your personal data in connection with your immigration case; accountants; lawyers; HR, benefits and compensation consultants, and other third-party service providers who provide services to us in connection with your immigration case. We may also transfer some of your personal data to governmental authorities (including tax authorities) where required by, or in order to comply with, law.

Non-governmental third parties to which we transfer your personal data must agree, as part of their contract with us, to treat your personal data in accordance with this Privacy Statement. To the extent that we transfer personal data about you to any third party that operates in a Non-Adequate Country, our contract with the third party will be consistent with contractual provisions approved by European authorities that will safeguard your personal data and your privacy rights.

**Storage and Retention of Personal Data**

We store personal data about you on computer servers operated by or under the instruction of Seyfarth. We will maintain personal data about you for as long as necessary and in accordance with our Records Management Policy, both during and following the completion of your immigration case: for the purposes for which it was collected; to defend or advance legal claims; or as otherwise required by applicable law. We and other Seyfarth partnerships will delete personal data about you in accordance with our Records Management Policy, at your request (where such request conforms to the relevant legal requirements and is not otherwise limited) and, in any case, upon expiration of the maximum storage term set forth by applicable law.

**Protecting Personal Data**

We have appropriate measures in place to prevent personal data from being accidentally lost, used, or accessed in an unauthorized way. We limit access to personal data to those who have a business need for such access. Those individuals who process personal data on our or on another Seyfarth partnership's behalf may do so only in an authorized manner. They are also subject to a duty of confidentiality and loyalty. Seyfarth has policies in place that regulate how our employees and partners must handle data, including personal data about you. We limit access to our premises and to our computer networks and take appropriate steps to safeguard against unauthorized access to such premises and networks. We have procedures in place to manage any actual or suspected data security breach and will notify you and any applicable regulator of any event affecting the integrity, confidentiality or availability of personal data where we are legally required to do so.

**Your Rights to Personal Data**

You may access the personal data about you that we store. You may also review or make certain corrections to the personal data we store about you. You may also request the deletion of personal data about you or object to its processing. In limited circumstances, you may have data portability rights in relation to certain personal data we hold about you. However, please note that all of these rights are not unlimited and the exercise of these rights, and the limits upon them, are specified in applicable law. If you have any questions or concerns you wish to raise about our use of your personal data please call 1-877-860-3852 or email dataprotection@seyfarth.com. Alternatively, you can contact the relevant Data Protection Authority for further information about your rights and how to make a formal complaint about the processing of personal data about you. You can find the Data Protection Authority with jurisdiction over your country of residence by visiting The European Commission's website at: http://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index en.htm

**Rights of California Residents**

This California Privacy Notice ("California Notice") applies to California residents whose Personal Information is processed by Seyfarth pursuant to the California Consumer Privacy Act ("CCPA") or other California privacy laws described below. The California Notice describes how we protect the Personal Information we process and control relating to California residents and rights California residents may have in relation to this Personal Information. For purposes of this California Notice, "Personal Information" has the meaning provided by the CCPA and does not include information that is publicly

available, that is deidentified or aggregated such that it is not capable of being associated with you, or that is excluded from the CCPA's scope.

Users who are residents of California may be able to request to exercise the following rights:

- The Right to Know any or all of the following information relating to your Personal Information we have collected and disclosed in the last 12 months, upon verification of your identity:
    - The specific pieces of Personal Information we have collected about you;
    - The categories of Personal Information we have collected about you;
    - The categories of sources of the Personal Information;
    - The categories of Personal Information that we have disclosed to third parties for a business purpose, and the categories of recipients to whom this information was disclosed;
    - The categories of Personal Information we have sold and the categories of third parties to whom the information was sold; and
    - The business or commercial purposes for collecting or selling the Personal Information.

- The Right to Request Deletion of Personal Information we have collected from you.

However, this right is limited by a number of exceptions. Fundamentally, if Seyfarth has a permissible need to retain Personal Information, it is not under an obligation to delete such information, even when requested. Generally, we retain Personal Information so we may complete the transaction for which the Personal Information was collected, provide a good or service requested by you, or reasonably anticipated within the context of our ongoing business relationship with you, or otherwise perform a contract between us and you; detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity; debug to identify and repair errors that impair existing intended functionality of our online properties; enable solely internal uses that are reasonably aligned with your expectations based on your relationship with Seyfarth; comply with a legal obligation; or otherwise use your Personal Information, internally, in a lawful manner that is compatible with the context in which you provided the information. As such, we generally do not accept requests to delete Personal Information.

- The Right to Opt-Out of Personal Information Sales to third parties now or in the future.

You also have the right to be free of discrimination for exercising these rights. However, please note that if the exercise of these rights limits our ability to process Personal Information, for example, if you submit a deletion request, we may no longer be able to provide you our products and services or engage with you in the same manner.

Seyfarth does not sell or share your Personal Data with third parties for their direct marketing purposes.

You may submit a request to exercise your California Consumer Rights through one of the mechanisms described below. We will need to verify your identity before processing your request, which may require us to request additional Personal Information from you or require you to log into your account, if you have one. In certain circumstances, we may decline or limit your request, particularly where we are unable to verify your identity or locate your information in our systems, or as permitted by law.

To exercise your California Consumer Rights to Know, Delete, or for additional information, please submit a request to 1-877-860-3852 or dataprotection@seyfarth.com].

Finally, you may also submit a verifiable consumer request through an authorized agent. To do so please be prepared for your agent to provide a signed permission to do so, to verify their own identity with us, and to directly confirm with us that you provided the agent permission to submit the request.