Russell Reynolds Associates Global Privacy Principles

Executive Summary

1. Follow the Rules **(GLOBAL PRIVACY LAWS).**
2. Be **TRANSPARENT** and **INFORM** individuals about what personal information we collect, how and why we use it, and who we share it with.
3. Give individuals **CHOICES** about how we use their data, and seek and record their **CONSENT** where legally required.
4. **COLLECT ONLY DATA WE NEED** for a specific purpose, **USE** and **RETAIN** it only for that same purpose.
5. Ensure that data gathered is **ACCURATE** and can be accessed, fixed or deleted upon request.

Principle Details

Principle 1

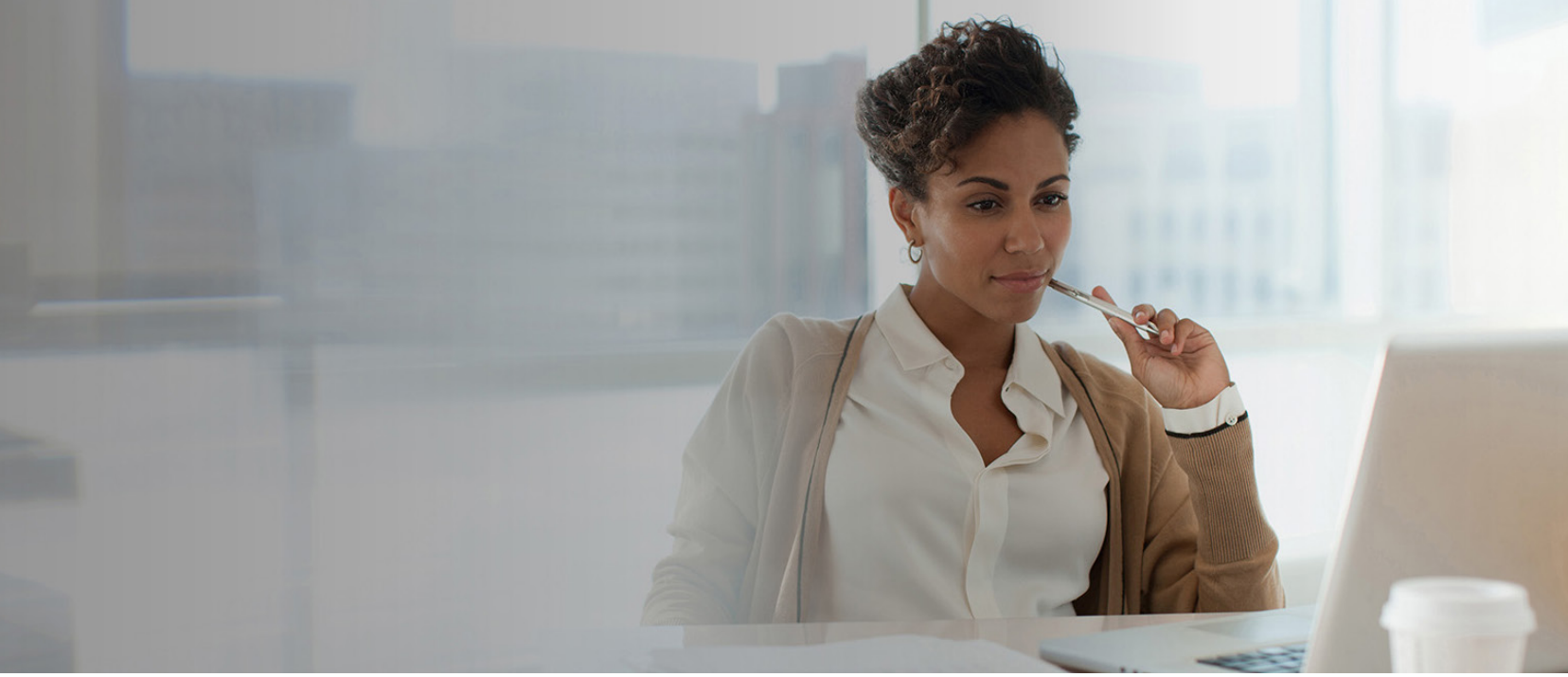
Follow the Rules **(GLOBAL PRIVACY LAWS).**

- We will comply with the privacy laws in the geographies in which we operate, which may include laws specific to that location and laws specific to the population served.
- We will comply with any applicable consumer, advertising, employment, or other laws that are relevant to our services.

Principle 2

Be **TRANSPARENT** and **INFORM** individuals about what personal information we collect, how we use it, and who we share it with.

- We will make available concise, transparent and easily accessible information to individuals (like candidates and employees) from whom we collect information about how and why we will use their personal information.
- The information we provide to individuals will be sufficient for them to make an informed decision about the uses of their personal information.
- We will inform individuals about their data protection rights (including rights of access, correction, deletion, objection, restriction and portability, where applicable).
- We will inform individuals about how to contact us with any privacy-related questions or concerns.
- When we collect information directly from individuals, we will provide notice at the point (or as soon as reasonably possible after) that personal information is collected.
- If we collect personal information from someone other than the individual (for example, from LinkedIn or other publicly available sources), we will inform the individual at the earliest opportunity unless this is impossible or involves disproportionate effort.
- If we will share an individual's personal information with third parties, we will identify the categories of third party recipients in the privacy notice provided to the individual.



Principle Details (cont'd)

Principle 3

Give individuals **CHOICES** about how we use their data, and seek and record their **CONSENT** where legally required.

- We will only use personal information if we can show that we have lawful grounds to use the personal information.
- If we collect an individual's consent, we will keep records to demonstrate what the individual has consented to, including what they were told, and when and how they consented.
- Where required by applicable data protection law, we will collect individuals' express consent when collecting Sensitive Personal Data (which in certain countries, like those in the European Economic Area, can include health and diversity data).
- When we collect an individual's consent, we will ensure the consent obtained is freely given, specific, informed and unambiguous.
- We will ensure that it is as easy for an individual to withdraw consent as it is to give consent.
- We will only share an individual's personal information with third parties if we have the necessary permissions or there is a legitimate business need to share the personal information.
- We will only send direct marketing messages to individuals in accordance with their marketing preferences (including allowing an opt-out at any time) and in compliance with direct marketing laws.
- We will make clear to individuals, at the point of data collection, whether the personal information we are requesting from them is mandatory or optional.

Principle Details (cont'd)

Principle 4

COLLECT ONLY DATA WE NEED for a specific purpose, **USE** and **RETAIN** it only for that same purpose.

- We will only collect an individual's personal information for a legitimate business purpose and will only collect as much personal information as is needed for that purpose.
- We will use and retain an individual's personal information only for purposes that are consistent with the notice provided to individuals at the time of collection.
- We will only retain personal information where we have a genuine legal need to do so and consistent with our document retention policy. We will not keep personal information indefinitely.
- Where we process personal information on behalf of our clients as a data processor, we will only process and retain such personal information for as long as our client instructs, unless otherwise required by law or to manage an ongoing business relationship.
- If an individual whose data we process requests deletion of their information, we will delete the information unless applicable law allows us to retain it for our legitimate business purposes (such as to comply with a legal requirement we are subject to).
- If we use an individual's personal information with consent and the individual withdraws consent, we will stop processing their information for that purpose, and delete their

Principle 5

Ensure that data gathered is **ACCURATE** and can be accessed, fixed or deleted upon request.

- We will keep personal information accurate and up to date.
- We will respect and comply with individuals' data protection right requests (including requests to exercise their rights of access, correction, and deletion) in accordance with law.

Principle Details (cont'd)

Principle 6

SUPPORT THE INFORMATION SECURITY TEAM by securing and protecting individual data against inappropriate disclosure or destruction.

- We will implement appropriate security measures to protect the personal information we process from security incidents and to preserve the security and confidentiality of the personal information.
- The security measures will be consistent with the sensitivity of that information. For example, sensitive personal information should be protected with elevated security measures.
- We will only share an individual's personal information with vendors who have provided sufficient guarantees that they will protect the information consistent with our privacy principles and policies.

Privacy Definitions

Personal Information: Means any information relating to an identified or identifiable person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

Sensitive Personal Data: What is considered "sensitive" (or a "special" category of) data varies in different countries. However, it typically includes personal information relating to or revealing a person's: (i) racial or ethnic origin, (ii) political opinions, (iii) religious or philosophical beliefs, (iv) trade union membership, (v) genetic data, (vi) biometric data used for uniquely identifying that person, (vii) physical or mental health, (viii) sex life, (ix) sexual orientation, and (x) criminal activity or alleged criminal activity. In addition, in some countries (like the U.S.), payment or banking details and social security numbers should also typically be treated as "sensitive" for security purposes. Check with the RRA Legal Team if you are unsure.