GLOBAL PRIVACY PRINCIPLES SELF-CHECK

Whenever you collect, access, use or otherwise process personal data, ***always remember to apply these 6 basic privacy principles****. Compliance with these key principles enhances data protection and is a fundamental building block for honoring the privacy rights of our students, employees, alumni, visitors, and other individuals of whom we process their data.*

Purpose: To provide a quick guide for you to self-check your adherence to basic Privacy principles before reaching out to the CES Privacy Center. This will facilitate our reviews and conversations.

1. **Purpose Limitation** – we are clear about what the purposes for processing are from the start. These purposes are explicit and legitimate. We do not further process the data in a way incompatible with those purposes.

   ** Have you defined the specific purpose for processing data?*

2. **Data Minimization** – we confirm that the personal data we are processing is (i) adequate – sufficient to properly fulfil the stated purpose; (ii) relevant – has a rational link to that purpose; and (iii) limited to what is necessary. We do not collect or maintain more than we need for that purpose.

   ** Have you determined what data elements are strictly necessary to accomplish your defined purpose?*

3. **Lawfulness** – we verify that the collection and use of personal data is justified, legal, and is either (i) necessary for the performance of a contract, or (ii) pursues a legitimate interest, or (iii) is necessary for compliance with a legal obligation, or (iv) is based on consent.

   ** Have you determined your legal justification for collecting or using the personal data (often it is legitimate interest or performance of a contract)?*

4. **Transparency** – we are open and honest with people from the start about who we are, and how and why we use their personal data. We provide them with clear and intelligible information either through concise privacy notices or just-in-time statements.

   ** Have you provided appropriate Privacy notices to individuals before collecting any personal data and cookie banners if using a front-end website?*

5. **Protection** – we verify that we have appropriate security measures in place to protect the personal data we hold against unauthorized or unlawful processing and against accidental loss, destruction or damage.

   ** Have you applied role-based access controls to limit who has access to personal data to those with a legitimate business need?*

   ** Have you ensured that a Data Sharing Agreement (DSA) is in place before personal data is shared to other departments or outside the organization?*

   ** If using a vendor, have you made sure the vendor completed a Vendor Contract Security and Privacy Addendum?*

6. **Duration** – we do not keep personal data for longer than needed. After the original, defined purposes for which the data was collected are achieved, we securely destroy or de-identify the data in accordance with defined standards and policies.

   ** Have you determined the appropriate retention schedule necessary to fulfill your defined purpose and still be in line with any published standards and policies?*

   ** Have you designed or planned a way to delete the data when legitimate business purposes have been met?*