General Data Protection Regulation (GDPR) Checklist Items

Many of the privacy requirements within the USG Business Procedures Manual (BPM), Section 12 include practices that are in alignment with many privacy and data protection laws and regulations, even if the USG is not subject to such laws or regulations. The USG takes the privacy and data protection of our stakeholders very seriously, thus we have put baseline best practices into our policies.

Your institution has complied with many of those practices in the completion of the USG Privacy Checklist. However, for those institutions that are working with a large volume of data subjects from the European Union (EU), further compliance is necessary in alignment with the additional GDPR Checklist.

GDPR Criteria

Review the following criteria if you are uncertain and complete the GDPR checklist if your institution has any of the following:

1. Your institution handles (collects, retains, processes, etc.) a large volume of personal data of students and/or employees who are data subjects* of the European Union (EU).

OR

2. Your institution has a campus/location within the EU.

GDPR Checklist

1. Has the institution identified and documented all instances of Personal Data within the scope of business activities, processes and supporting systems (including third-party vendors)?

    1a. Having identified and documented these instances of Personal Data, has the institution initiated and completed a Record of Processing Activities (RoPA), including determining the appropriate legal basis for the processing of Personal Data?

2. Has the institution identified “special categories” of personal data that require additional controls?

3. Has the institution updated the institutions' Data Policy to include GDPR verbiage?

4. Has your institution reviewed whether or not you are required to have a Data Protection Officer (DPO) per GDPR guidelines?

    4a. If you have and it was determined your institution does require a DPO, is there a plan in place to appoint one or has one been appointed?

5. Does the institution have procedures in place to process data subject requests (DSRs), including modification to, deletion of or access to data collected?

6. Does the institution have a mechanism in place to effectuate the legal transfer of data across borders?

7. Does the institution provide training to appropriate personnel regarding the requirements of GDPR?

8. Does the institution have in its breach protocols the appropriate procedures for notifications in a timely manner and to the appropriate organizations and/or regulatory bodies?

9. Does the institution have data minimization and appropriate data retention processes in place?

10. Does the institution have controls in place related to the confidentiality, availability, and integrity of personal data including appropriate technical and security measures like anonymization, tokenization, personnel training, etc.?

11. Has the institution documented uses of Artificial Intelligence or Machine Learning occurrences?