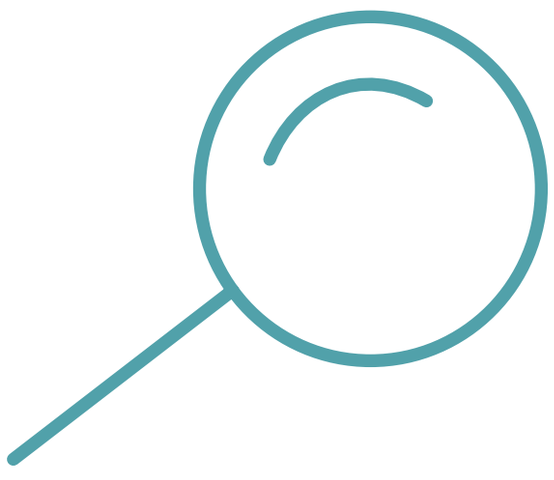
iapp

Checklist: Expedited Vendor Privacy and Security Assessment

As companies, educational institutions, governments and other organizations shift to remote work environments during the COVID-19 pandemic, the need for technologies to facilitate engagement has exploded. Video conferencing, chat platforms and virtual classrooms are necessities. The immediate need for these tools is expediting privacy and security assessments of vendors.

Below are key questions for privacy professionals to consider as they navigate this process:

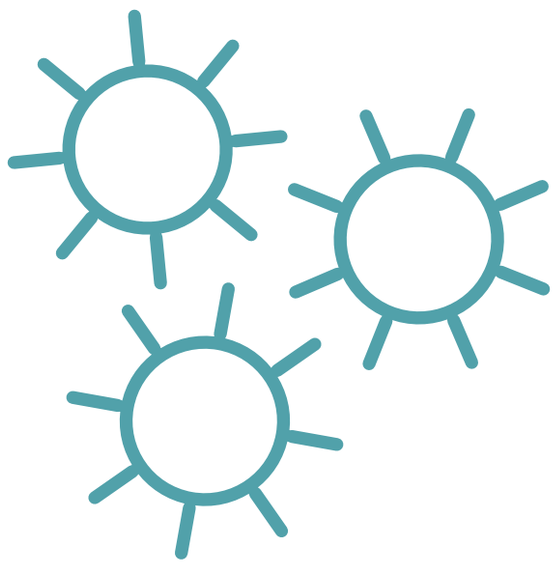


NARROW THE FIELD

- ☐ Is there robust, publicly available privacy documentation you can review?
- ☐ Does the vendor have verifiable privacy certifications or trust marks?
- ☐ Does a quick online search reveal credible concerns (e.g., recent incidents) about the vendor's privacy or security practices?
- ☐ Is anything about the vendor's platform or service overly intrusive or "creepy"?
- ☐ Does the vendor have privacy professionals on staff?

DUE DILIGENCE

- ☐ What type of data will be shared with, collected by or accessed by the vendor?
- ☐ What is the vendor permitted to do with the data?
- ☐ Where will the vendor store the data?
- ☐ How long will the data be kept, and what are the protocols around deletion?
- ☐ What security controls does the vendor have in place?
- ☐ Does the vendor have good privacy-by-design so that default settings favor privacy?
- ☐ Does the vendor have an incident response and recovery plan?



STREAMLINE MECHANICS

- ☐ Can you streamline your vendor assessment questionnaire and the sign-offs required?
- ☐ Can you leverage privacy technology in the vendor assessment process or outsource it to speed things up?
- ☐ Do you have a standardized data processing agreement that you can put in place?

REASSESS WHEN TIME ALLOWS

Consider moving up the reassessment time frame for vendors that had an expedited review.