Crowe

Checklist

Assessing your privacy and data protection programs

Crowe

Privacy affects every organization differently, because every organization is different.

But privacy and data protection is one of the most complex issues your organization will tackle. This brief checklist can help you identify areas where your organization can build a more effective program.

☐ **1.** Has a named individual been identified as program leader across the organization's footprint?

If your answer is no, consider identifying an individual to lead the program.

Depending on the size of the organization, geographies where business is conducted, scope of work, and industry, some organizations might be able to combine privacy-related responsibilities with other activities.

However, many organizations will need to have a leader fully engaged in privacy to address relevant regulatory requirements and support business objectives.

☐ **2.** Has a risk appetite been established related to processing personal data?

If your answer is no, consider identifying how much privacy and data protection-related regulatory risk the organization is willing to take.

Factor in issues including the privacy and data protection regulations that apply to the organization, the volume of personal data and information processed, where data subjects providing that information reside, the information security protections placed around personal data, and if personal data is transferred across country borders.

☐ **3.** Is the level of risk associated with processing personal data periodically assessed?

If your answer is no, consider beginning periodic assessments to better understand and remediate gaps that create risk beyond the organization's risk appetite.

☐ **4.** Are policies and procedures related to processing personal data documented to help employees understand the risk appetite?

If your answer is no, consider documenting a privacy policy that provides employees with information about the organization's expectations regarding privacy and data protection.

Procedures can be added over time as the privacy program matures.

☐ **5.** Are employees regularly trained on privacy and data protection procedures? Do employees with specific responsibilities for protecting personal data receive additional training beyond what is provided to all employees?

If your answer is no, consider starting with high level training on the organization's privacy policy. Include information about why privacy protection matters to the organization and its stakeholders.

For employees specifically tasked with protecting personal data, provide information about what is expected and, where applicable, how they should accomplish meeting expectations.

☐ **6.** Are policies and procedures shared with the appropriate groups who interact with personal data collected?

If your answer is no, consider either sharing policies and procedures with third parties processing personal data on behalf of the organization or creating and sharing a separate document that notes the expectations of those third parties.

☐ **7.** Have processes been designed that address requests from data subjects in a timely, accurate, and confidential manner?

If your answer is no, consider if the organization is subject to regulations that require specific responses to data subject inquiries.

If not, it is still a best practice to respond to inquiries. Here are two sample responses:

- We have received your request and will address it as timely as possible.
- We have received your request and cannot address it for the following reason.

If the organization is subject to regulations that require specific responses, consider designing a process that allows the organization to verify the identity of the requester and that includes mechanisms for effective, efficient identification and collection of relevant data responsive to the specific request, along with the secure transfer of responsive data to the verified data subject. In addition, create a process for documenting request receipts and responses.

☐ **8.** Have processes been designed and implemented so they support the Privacy by Design approach?

If your answer is no, consider building such a process. Once built, pilot the process to identify ways to make it more efficient and more effective. Implement once tested.

☐ **9.** Are data protection impact assessments leveraged to assess the risk of harm to individuals who provide personal data?

If your answer is no, consider building a process that assesses the potential risk of harm to individuals associated with a specific data collecting process. For example, a new website designed to provide users with the ability to track their health-related information.

For identified risks, develop and track mitigations that reduce the risk of harm.

☐ **10.** Are organizational and technical measures used to protect personal data from loss, destruction, theft, and misuse?

If your answer is no, consider conducting a security-focused gap assessment to determine the current state of data protection across the organization.

Remember to consider physical security-related requirements when conducting gap assessments.

☐ **11.** Are data maps and records of processing accurately prepared and maintained to include the specific type of personal data stored, the storage location, the business use associated with collection, and the legitimate means of processing the data?

If your answer is no, consider building data maps and records of processing that document information relating to the personal data held by the organization.

If data maps and records of processing exist but are not current or haven’t been reviewed and updated for more than 12 months, consider making updates.

☐ **12.** Does a data retention policy and associated data retention schedule exist that specifies the length of time personal data and information should be stored? Are employees trained on the policy and follow it?

If your answer is no, consider:

a. Preparing a data retention policy that reflects requirements from regulators (data protection-related and others)

b. Establishing a data retention schedule by data type and purpose for collection

c. Training employees periodically on the data retention policy and associated data retention schedule

d. Monitoring compliance

☐ **13.** Are transfer impact assessments appropriately conducted from locations with robust privacy and data protection laws to locations without robust privacy and data protection laws before an international transfer of personal data is executed?

Is the appropriate legal documentation leveraged to support international data transfers, including standard contractual clauses and, where applicable, data processing agreements?

If your answer is no and personal or sensitive personal data is transferred between countries, consider conducting transfer impact assessments to determine the risk associated with the specific international data transfer.

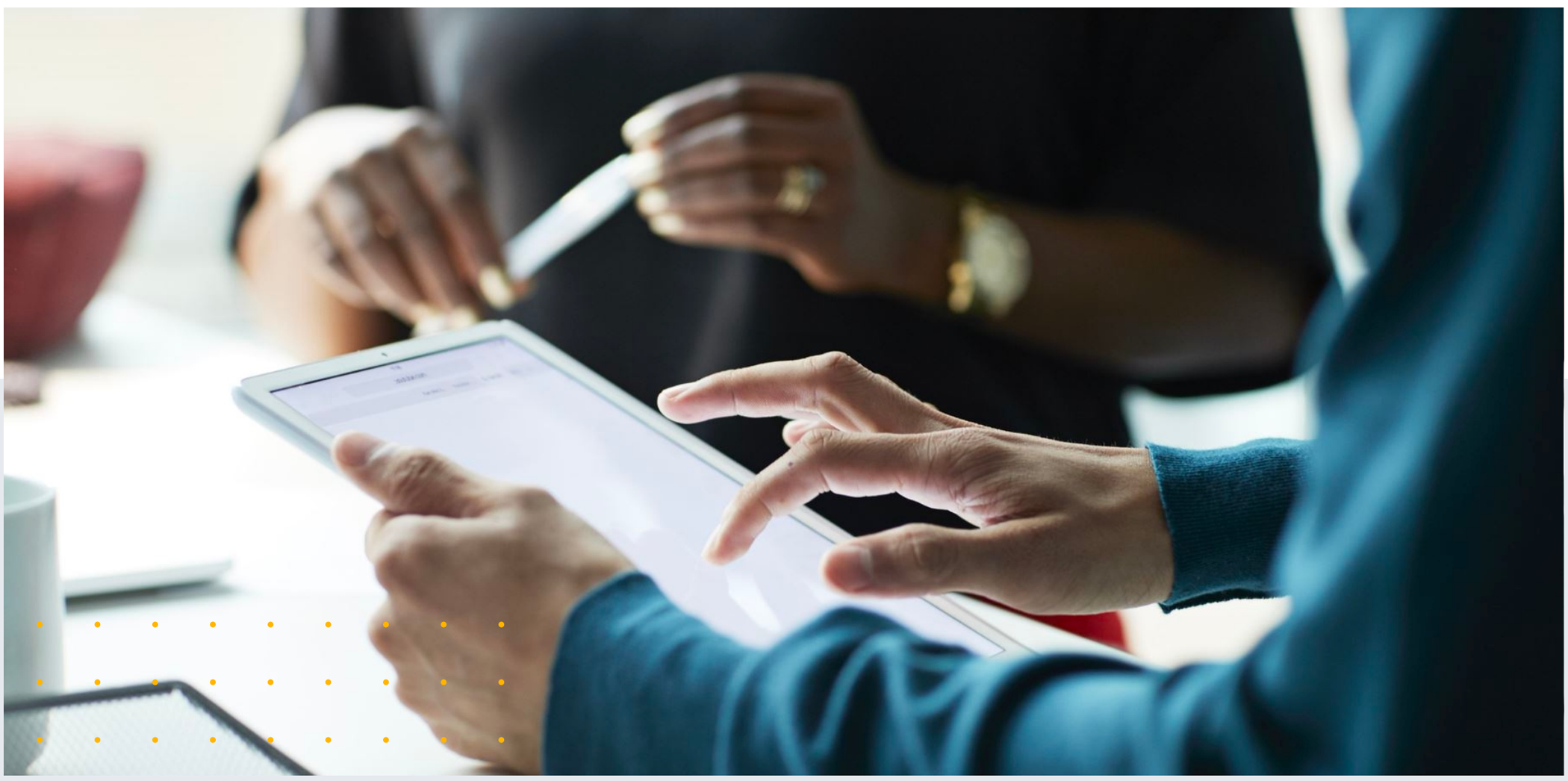
Determine if the transfer of data should be stopped until related risks are appropriately addressed and, if necessary, legal agreements are in place related to the data transfer. Remember that data might not need to physically change locations for a transfer to have occurred.

☐ **14.** Is the processing of personal data appropriately registered where necessary?

If your answer is no, consider reviewing country-specific requirements associated with registration. Follow up where necessary.

☐ **15.** Is the organization lawfully processing personal data by obtaining explicit consent where necessary or by operating under another legal means of processing as specified in applicable regulations?

If your answer is no, evaluate options for aligning the processing of personal data with regulatory requirements.



Let’s talk

Regardless of how you assess the current state of your organization’s privacy and data protection program, there might be opportunities to increase efficiency and effectiveness. We can help put your privacy program on a path that works for your organization.

Pam Hrubey
Principal
+1 202 552 8058
pam.hrubey@crowe.com

Learn more about our privacy solutions

Visit crowe.com

CLS2299-002G