hopkins carley

The information contained below is provided for high-level, general informational purposes only. No information provided below should be construed as legal advice from Hopkins & Carley (or the individual author), nor is it intended to be a substitute for legal counsel on any subject matter. Please do not act or refrain from acting on the basis of any information included below without seeking the appropriate legal or other professional advice on the particular facts and circumstances at issue.

Brief Overview of Data Mapping / Vendor & 3rd Party Risk

Data Mapping

In order to effectively comply with an increasing number of data protection laws, including CCPA and GDPR, organizations must first ascertain what personal information is collected, as well as how and why it is being processed, shared/disclosed, stored and secured. In order to do so, organizations should conduct a data mapping exercise, which is considered the foundation of any privacy program.

Regardless of how it is accomplished (i.e., via automated tool or manual questionnaire), data mapping requires a current and detailed understanding of:

- The collection points and sources of personal information – when and how is data collected?
- The general location (region/country) of individuals whose data is processed – whose data is collected and where are the individuals located?
- The Purpose of collection/processing – why is the data processed?
- Storage – where is the data stored?
- Third-party sharing of personal information – to whom is personal data disclosed? Note: data mapping exercises frequently reveal secondary or tertiary downstream processing activities that may not be apparent to the organization driving the collection of data, but of which both said organization and consumers must be informed. Your mapping should therefore allow you to determine where your organization stands in the "supply chain" and how/why data is disclosed to third-parties (including security practices).
- Data retention periods – how long are different categories of data retained and why?
- Security – how is personal data secured? Note: this should include a classification of data to assess criticality.

Some organizations also prepare a visual depiction of the lifecycle of each type of personal information through a defined process, including the applications, systems, databases and third parties to which the data flows.

Prior to beginning any data mapping, please note that:

- The definition of "**personal information**" or "**personal data**" is increasingly broad under recent legislation:
  - → Personal information that identifies, relates to, describes, is capable of being associated with, or may reasonably be linked, directly or indirectly, with a particular individual or consumer, including names, emails etc. as well as inferences.
  - → Identifiers, IP addresses, location information, and data collected via cookies and tracking technology.
  - → Fully anonymized or de-identified data is generally excluded.

- "**Collecting**", "**sharing**" or "**processing**" personal data is also very broad and, depending on the law, includes buying, renting, gathering, selling, obtaining, receiving, accessing, transmitting, recording, and consulting.
- Personal information may be collected in many ways: directly from individuals, indirectly through automated technologies such as cookies (SDKs etc.), or from third parties. In all cases, this should be included in the data map in order to ensure sufficient transparency and proper compliance assessments.

Vendor and 3rd Party Risk Assessments

Knowing where your organization stands in the data supply chain or ecosystem is key, and determining vendor or third-party compliance with privacy laws, including GDPR, equally as important. Blindly outsourcing the responsibility of data governance and privacy/security compliance to vendors is not sufficient. Under GDPR, companies have an obligation to conduct due diligence, implement appropriate contract terms, and routinely monitor vendors (and their own vendors) in order to ensure to that data is always processed in accordance with applicable data protection laws. If there is a violation or data breach caused or enabled by a vendor, your organization may be liable.

- First, as part of your data mapping (above), determine (i) what data you provide or share with third parties or vendors, (ii) whether it is personal data that is covered by GDPR or other privacy laws, and if so what requirements are associated with that type of data.
- Know what vendors your vendors use, all the way down the supply chain!
- Reviewing all vendor agreements is very important. Before assuming that none exist, many are automatically included as part of standard terms of service and can be found online. Many will be non-negotiable.
- Once identified, vendor contracts should be updated or modified to include new language to define vendors' roles, liability, and obligations – as well as their vendors (also known as sub-processors). This is often known as a data processing agreement (Article 28 GDPR), but can come in different shapes and forms. In some cases, you may partner with another company that is more than just a service provider and may be deemed a joint or separate controller under GDPR, in which case we recommend an agreement allocating responsibilities.
- For new vendors or third parties, include a formal intake process, and understand their security and privacy compliance. If they refer you to their website for inquiries on compliance, keep any records/screenshots of standard FAQs or "we comply with XX privacy laws" that they may provide online!
- Create a centralized system or repository that will not only track vendor contracts, but will also flag vendors who process personal data and alert your stakeholders of contract terms and renewal dates.
- Many breaches occur via vendors. In some cases, it may result from vendors' own employees, in other cases vulnerabilities in vendor systems. The fall-out from Target's highly publicized data breach several years ago, in which an HVAC vendor was exploited by hackers to access customer data, should stand as a reminder that a chain is only as strong as its weakest link: ensuring that your vendors (or your vendors' vendors) are secure and comply with privacy requires a thorough and methodical approach.
- Review other laws (e.g., CCPA), that require you to keep track of your vendors or service providers. When you entrust third parties with your users' personal data – or your customers' users' personal data – you should always ensure that they are trustworthy!

Hopkins & Carley provides complete and comprehensive Data Questionnaires/Assessments to existing clients. For more information, please contact Celine Guillou, CIPP/E (cguillou@hopkinscarley.com) or Chiara Portner, CIPP/US (cportner@hopkinscarley.com).

For more information about the firm, please visit us at www.hopkinscarley.com.