WSJ PRO

AI, Growing Data Risks Expand the Role of Chief Privacy Officer

Many chief privacy officers now help make AI and cybersecurity decisions on new products and services

By Catherine Stupp

Sept. 5, 2024 12:01 pm ET | WSJ PRO

A GE HealthCare plant outside Paris. Lara Liss, chief privacy and data trust officer, says she is now involved in the development of products earlier in the process to ensure privacy concerns are addressed at the design phase. PHOTO: AGENCE FRANCE-PRESSE/GETTY IMAGE

Privacy executives are taking on new responsibilities in artificial intelligence and cybersecurity as companies expand their use of emerging technologies and regulators more closely watch what businesses do with data.

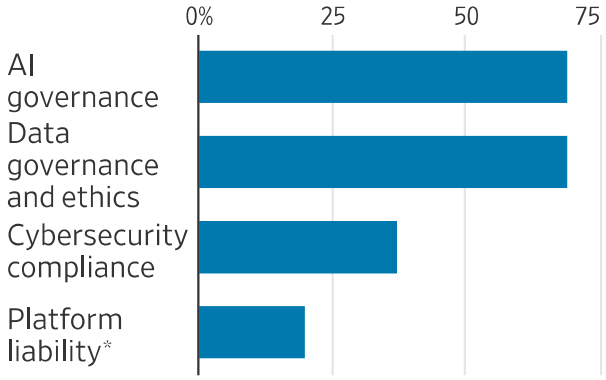
Chief privacy officers have been responsible for managing compliance with a web of laws in U.S. states and other countries where the company may operate. CPOs have also had a hand in setting ethical policies on the company's use of information.

Now, corporate privacy executives are adding new areas to their remit. Over 80% of privacy teams now do additional work in areas such as AI and data governance, according to a forthcoming survey of 671 privacy executives from the International Association of Privacy Professionals. The report is due out Friday.

Spreading Scope

The job of the chief privacy officer is expanding as AI, data governance and cybersecurity increasingly overlap

Areas CPOs recently added to their duties



* Refers to laws in Europe and other jurisdictions that require companies to police harmful content

Source: Survey of 671 privacy executives from the International Association of Privacy Professionals

Chief executives and boards, taking note of rising technology risks worldwide, are getting their CPOs to help navigate new laws governing data-security breaches and the development and use of AI, said Caitlin Fennessy, vice president and chief knowledge officer at IAPP, a trade group based in Portsmouth, N.H.

"They're looking at approaching these things more holistically," Fennessy said, by handing additional tasks to the chief privacy officer rather than having oversight siloed in different tech-focused areas.

At GE HealthCare, Chief Privacy and Data Trust Officer Lara Liss leads the company's work on "responsible AI," an industry term for making sure AI respects privacy, ethical and cybersecurity guidelines. She shares that obligation with the company's chief AI officer and vice president of AI.

Liss, a lawyer who also holds an M.B.A., said part of her job is to assess the risks of new products and help GE Healthcare comply with evolving AI regulations. She is now involved in the development of products earlier in the process, she said, to ensure privacy concerns are addressed at the design phase.

In healthcare, high-quality data is now the priority, compared with a few years ago when companies aimed to collect large quantities of data, Liss said. Today, her privacy team works with business units to make sure they gather just the minimum amount of data they need.

“We learned in healthcare that more data didn’t always result in more accurate treatment,” she said.

The rise of huge data breaches that can do lasting damage to a company’s reputation, coupled with a maze of AI and privacy laws, has put a spotlight on corporate privacy officers, said Dan Linton, global data privacy officer at Real Chemistry, a healthcare-focused marketing company.

Last week, California lawmakers passed a controversial bill to regulate AI, which Gov. Gavin Newsom, a Democrat, has until Sept. 30 to sign or reject. Hundreds of other AI bills are in state legislatures, while the world’s first comprehensive AI legislation took effect last month in the European Union.

Data regulations are picking up steam as well. At the beginning of this year, 12 U.S. states had already passed comprehensive data privacy laws. Seven more have done so since then.

Caroline Louveaux, chief privacy and data responsibility officer at Mastercard. PHOTO: CHRISTINNE MUSCHI/BLOOMBERG NEWS

For Linton, a lack of legal precedent on how AI models use personal data has forced him to work more closely with data and cybersecurity teams to understand technical processes. “I’m getting more involved at the strategic level than I was several years ago,” he said.

Caroline Louveaux, Mastercard’s chief privacy officer, added data responsibility officer to her title last year. The company’s privacy and data strategy teams work together on AI development, she said.

Based in Brussels, Louveaux stays on top of European regulatory moves in privacy and data areas. After the EU’s General Data Protection Regulation, the broad privacy law, took effect in 2018, Louveaux said she and her privacy team saw that policymakers in Europe and beyond wanted to address AI rules next. So she and her team took up the topic with representatives from the bloc and other countries, including Singapore, she said.

Privacy officers are well-trained in parsing out the various, and sometimes competing, demands that come up in new privacy and data laws as they touch on cybersecurity, transparency and protecting personal data, she said.

“These skill sets are going to be more and more important for the future because we see more and more of these tensions between different digital rules,” she said.

Write to Catherine Stupp at catherine.stupp@wsj.com