KPMG

COVID-19 | Privacy

Restoring privacy compliance

The COVID-19 pandemic has required businesses to rapidly adapt their working models, sometimes at the cost of privacy rights. What practical steps can you take to address the deficit and restore privacy compliance?

The second line risk and compliance function has taken a double hit from the pandemic. Businesses have expedited the approval of new technologies and processes to cope with the new working model, leaving privacy compliance as an afterthought.

Also, the pandemic has made the job of embedding, monitoring and enforcing privacy controls much harder, both at a technical and a governance level.

As employees get used to remote working, businesses now have a moment to breathe and take a step back and think more strategically. With the second line looped back into discussions, how can you assess and remediate the privacy compliance gap?

Start with governance

— How is the privacy office managing with remote working? Ensure that your team has access to the right collaboration tools and technologies to communicate and work more efficiently.

— Establish how you can support resilience efforts by working flexibly with the business — they're under strain, and they need an agile and supportive second line team to deliver continuity of services, and manage under financial pressure.

— Consider employee working arrangements — do they have children to look after and need to work new hours? Do they have privacy in their homes to discuss and process data or sensitive complaints?

— Arrange for staff to be able to fulfill data subject access rights — are requests still being processed on time and in line with legal requirements?

— Review organizational policies and standards in light of new working models and customer service arrangements.

— Keep an eye out for guidance from regulators, and ensure regulatory interactions are still being tracked and managed consistently during this time. Ensure you have strong communication lines with your legal team, and access to legal services.

— Re-embed privacy by design by considering how to remotely re-perform impact assessments for both new and old technologies and processes that have seen changes to data flows and ways of working.

— Make adjustments to external and internal audit schedules and privacy audits as required — make sure to document assessment capability gaps and keep relevant boards and committees informed regularly.

— Adjust your compliance metrics and KPI reporting to new remote working practices — are any of them dependent on physically being in the office, e.g. clear desk reviews?

— Monitor the effect COVID-19 has had on resource availability and the ability to operate critical privacy processes in every department. How are HR and IT coping with demand — what have they had to drop?

Make sure you're communicating

— Adapt communications and awareness campaigns to fit the new way of working.

— Make employees aware of their privacy obligations when working remotely, especially those handling sensitive data, e.g. in call centers.

— Ensure employees, who may be required to handle data for the pandemic period, have access to relevant training guides and materials to perform their roles.

Look after your employees and customer rights

— Review employee monitoring processes and data collection for staff risk metrics. How should they be adapted — are they still fair, adequate and transparent?

— Identify employees on international and cross-border transfers and verify the handling of their information complies with local regulations. For employees stranded or working from overseas, ensure their access to data is policy compliant.

— What measures have been put in place to confirm employees can establish a clear work-life balance — is there respect for privacy in current ways of working?

— Be transparent with customers over any changes in the way their data is processed for the sake of business continuity and update relevant external privacy notices.

— Manage employee health data and testing processes, so they comply with regulation.

Work with your technology and security teams

— Ensure your security team is monitoring the implementation of security and privacy controls in the builds of any new assets acquired to support remote working, e.g. newly acquired laptops and conferencing collaboration solutions.

— Keep an eye on the security compliance deficit too — what workarounds do they have to address? Are staff using their own devices to access work data? Is this being managed in line with BYOD policies?

— Work with IT to understand how their data monitoring controls have been affected. What are they struggling to do, and how can you mitigate risks?

— Your development teams may have been under pressure to roll out applications that support customers. Have they been able to embed privacy controls and data loss prevention controls effectively, and can you retroactively assess their privacy controls and implement any changes required?

Third party oversight

— Verify that emergency contractors or suppliers onboarded to support COVID-19 have undergone privacy due diligence. Are they still able to provide relevant information? Can you conduct assessments remotely?

— Are changes to ways of working reflected in contractual privacy clauses (i.e. update data flow arrangements and security safeguards). Is any data flowing internationally?

— Has your third party supply chain privacy risk been heightened due to the loss of suppliers. Do you need to use alternative providers?

Monitor your data assets and lifecycle

— Review data flow diagrams and make any changes to where data is stored, accessed in new locations or used in different ways. Also, record changes in your data inventories and privacy notices.

— Make certain employees have the proper equipment to manage personal data and privacy from their homes (i.e. shredders, scanners).

— Verify that governance and records management policies take into account the increased flow and volumes of data use across the network.

Incident management

— Work with the security team to review incident response plans in light of remote working — can they still respond to incidents at the same speed?

— Keep up-to-date on the cyber threat and your risk landscape. Has there been an uptick in incidents or data breaches as a result of the change in working?

— Are you still able to track near-misses and incidents efficiently — can you maintain response rates and capabilities?

Make sure to document your lessons learned — they might be useful as your organization recovers and adjusts to the new, post-pandemic reality. And in the face of pressure to reduce expenses, it's worth asking what technologies are out there that can let you automate privacy compliance processes and make them efficient?

Contacts

Michael Daughton
Partner, Head of Risk and Regulatory Consulting
KPMG Ireland
E: michael.daughton@kpmg.ie

Tom Hyland
Associate Director, Risk Consulting
KPMG Ireland
E: tom.hyland@kpmg.ie

Mark Thompson
Global Privacy Advisory Lead
KPMG International
E: mark.thompson@kpmg.co.uk

home.kpmg
home.kpmg/socialmedia

Publication date: May 2020