COVID-19 | Cyber Security and Privacy

Restaurando a conformidade com a privacidade

A pandemia do COVID-19 exigiu que as empresas rapidamente adpatassem seus modelos de negócio, às vezes, às custas de regras envolvendo privacidade. Que medidas práticas podem ser tomadas para resolver essa deficiência e recuperar o Compliance com a privacidade?

As áreas de suporte de risco e compliance sofreram um golpe duplo da pandemia. As empresas aceleraram a aprovação de novas tecnologias e processo para lidar com o novo modelo de negócio, deixando o compliance com privacidade e proteção de dados em segundo plano.

Além disso, a pandemia tornou o trabalho de incorporação, monitoramento e aplicação de controles de privacidade muito mais difícil, tanto no âmbito técnico quanto no de governança.

À medida em que os funcionários se acostumam com o trabalho remoto, as empresas começam a ter um tempo maior para se reorganizarem e dar um passo atrás para pensar de maneira mais estratégica. Desta forma, as atividades de risco e compliance voltam para a mesa de discussões.

Nesse contexto, como as empresas podem avaliar e sanar as inconformidades relacionadas à privacidade?

Comece com governança

- Como o escritório de privacidade está gerenciando o trabalho remoto? Certifique-se que seu time tenha acesso às ferramentas e tecnologias adequadas para se comunicar e trabalhar de maneira mais eficiente e com segurança. Envolva seu time de TI para auxiliar nessa análise.
- Defina como você pode apoiar a resiliência, agindo de modo mais flexivel com o negócio – outras áreas estão sob tensão e precisam de seu suporte para garantir a continuidade das atividades.
- Considere adaptar o trabalho dos funcionários – eles tem filhos para cuidar e precisam trabalhar em horários diferentes? Eles têm privacidade na casa deles para discutir e tratar dados ou reclamações confidenciais?
- Garanta que, ainda que a LGPD não esteja em vigor, a equipe tenha consciência sobre o cumprimento de direitos lá estabelecidos e que os fluxogramas internos que auxiliarão neste atendimento sejam seguidos.
- Reveja políticas e padrões organizacionais à luz dos novos modelos de trabalho e acordos de atendimento ao cliente.
- Fique de olho nas orientações dos reguladores e garanta que as interações regulatórias estejam sendo rastreadas e gerenciadas consistentemente durante este período. Garanta a existência de fortes linhas de comunicação com sua equipe jurídica e/ou acesso a serviços jurídicos.
- Reimplemente o privacy by design, considerando como executar, remotamente, avaliações de impacto para tecnologias e processos novos e antigos que sofreram mudanças nos fluxos de dados e nas formas de trabalho.
- Faça ajustes nos cronogramas de auditoria externa e interna e de privacidade, conforme necessidade - certifique-se de documentar as lacunas relacionadas a capacidade de avaliação e mantenha informados os conselhos e comitês regularmente.
- Ajuste métricas de compliance e relatórios de KPI para novas práticas de trabalho remoto – alguma delas dependem de estar fisicamente no escritório, por exemplo, revisões de política de mesa limpa?
- Monitore o efeito que a pandemia teve na disponibilidade de recursos e na capacidade de tratar processos críticos de privacidade em toda a Organização. Como o RH e a TI estão lidando com a demanda - o que eles tiveram que abandonar ou se adaptar?

Garanta a comunicação

- Adapte as campanhas de comunicação e conscientização para se adequar à nova maneira de trabalhar.
- Informe os funcionários sobre suas obrigações relacionadas a privacidade ao trabalhar remotamente, especialmente aqueles que lidam com dados confidenciais, por exemplo, em atendimento à clientes.
- Garanta que os funcionários, que podem ser solicitados a trabalhar com dados pessoais e informações confidencias no período de pandemia, tenham acesso a guias e materiais de treinamento relevantes para desempenhar suas funções.

Proteja os direitos de seus funcionários e clientes

- Revise os processos de monitoramento de funcionários e de coleta de dados para métricas de risco da equipe. Como devem ser adaptados – continuam razoáveis, adequados e transparentes?
- Identifique os funcionários em transferências internacionais e transfronteiriças e verifique se o manuseio de seus dados pessoais está em conformidade com as normas locais. Para funcionários isolados ou que trabalham no estrangeiro, garanta que seu acesso aos dados pessoais esteja de acordo com a política.
- Quais medidas foram aplicadas para confirmar que os funcionários possam estabelecer um equilíbrio adequado entre o trabalho e a vida pessoal – há respeito pela vida privada nos métodos de trabalho remote?
- Seja transparente com os clientes sobre quaisquer mudanças em como seus dados pessoais que serão processados para garantir a continuidade do negócio e atualize as políticas de privacidade externas relevantes.
- Gerencie os dados de saúde dos funcionários e processos de teste,

para que estejam em conformidade com as normas e leis.

Trabalhe com seus times de segurança e tecnologia

— Garanta que seu time de segurança está monitorando a implementação dos controles de segurança e privacidade no desenvolvimento de quaisquer novos recursos adquiridos para dar suporte ao trabalho remoto, como por exemplo notebooks e soluções para conferência recentemente adquiridos.

— Fique atento ao déficit de conformidade de segurança também – quais alternativas eles precisam abordar? Os funcionários estão utilizando seus próprios dispositivos para acessar dados do trabalho? Isso está sendo tratado de acordo com as políticas de BYOD ("Bring Your Own Device")?

— Trabalhe com TI para entender como os controles de monitoramento de dados pessoais estão sendo afetados. Quais são as dificuldades e como mitigar os riscos?

— Suas equipes de desenvolvimento devem estar sob pressão para implementar aplicativos que auxiliam os clientes. Foi possível incorporar controles de privacidade e de prevenção de perda de dados pessoais de forma efetiva? É possível avaliar retroativamente os controles de privacidade e implementar as alterações necessárias?

Gerencie os terceiros

— Verifique se os contratantes ou terceiros emergenciais relacionados às atividades de suporte ao COVID-19 passaram pela due dilligence de privacidade. Eles ainda são capazes de fornecer informações relevantes? É possível realizar avaliações remotamente?

— As mudanças nas formas de trabalho estão englobadas nas cláusulas contratuais de privacidade (por exemplo na disposição do fluxo dos dados pessoais e nas salvaguardas de segurança)? Há algum dado circulando internacionalmente?

— O risco de privacidade relacionado a cadeia de suprimentos de seus terceiros aumentou devido à perda de fornecedores? Há a necessidade de uso de fornecedores alternativos?

Monitore os ativos de informação e ciclo de vida

— Revise os diagramas de fluxos de dados e faça alterações nos locais onde os dados são armazenados, acessados em novos locais ou usados de maneiras diferentes. Ainda, registre as alterações em seu inventário de dados e nas anotações de privacidade.

— Garanta que seus funcionários tenham equipamentos adequados para gerenciar dados pessoais e da vida privada de suas casas (por exemplo trituradoras e scanners).

— Verifique se as políticas de governança e de gestão de registros levam em consideração o aumento do fluxo e volume de dados pessoais.

Gerencie incidentes

— Trabalhe com a equipe de segurança para revisar planos de resposta a incidentes à luz do trabalho remoto – é possível responder à incidentes na mesma velocidade?

— Atualize as novas ameaças cibernéticas e seu cenário de riscos. Houve um aumento nos incidentes ou na violação de dados por conta da mudança no modo de trabalho?

— Ainda é possível rastrear incidentes de forma eficaz – é possível manter as taxas de resposta e competências?

— Certifique-se de documentar suas lições aprendidas – elas podem ser úteis enquanto sua empresa recupera-se e adapta à nova realidade pós-pandemia. E com relação à pressão na redução das despesas, é viável questionar quais são as tecnologias que permitem automatizar a conformidade de processos de privacidade e fazê-las eficientes?

Como se prevenir contra Fraudes e Golpes

— Certifique-se de aumentar o nível de conscientização de seus colaboradores neste período para fraudes e golpes relacionados à pandemia ou situações de vulnerabilidade do trabalho remoto, dos quais destacamos:

— Phishing: páginas fraudulentas de agências de saúde, hospitais e organizações de combate ao COVID podem mirar colaboradores não atentos.

— E-mails Corporativos Infectados: preste atenção em e-mails sobre updates acerca da crise (novas vacinas, condições de isolamento e outros títulos chamativos). Colaboradores devem ser instruídos a sempre verificar a autenticidade de domínios.

— Caso os colaboradores tenham informações corporativas (como e-mail e calendário) em seus dispositivos pessoais, divulgue recomendações sobre a instalação apenas de aplicativos confiáveis, principalmente em tempos incertos onde a atividade criminosa é majorada.

Fale com o nosso time

Leandro Augusto
Sócio-líder de Cyber & Privacy
lantonio@kpmg.com.br

Rodrigo Milo
Sócio de Cyber & Privacy
rodrigomilo@kpmg.com.br

Samara Schuch
Sócia-diretora de Cyber & Privacy
samaraschuch@kpmg.com.br

Isabella Becker
Gerente de Cyber & Privacy
isabellabecker@kpmg.com.br

Ser criativo
transforma negócios.

#KPMGTransforma

Baixe o APP
KPMG Brasil

kpmg.com.br
/kpmgbrasil

Projeto gráfico e diagramação: Gaudí Creative Thinking