GEP soluções em Compliance

CONHEÇA OS 5 PRINCIPAIS DESAFIOS DE UM DPO

E SAIBA COMO SUPERÁ-LOS

ORIENTAÇÕES DE USO DO E-BOOK

Este e-book conta com interações para deixar o documento mais dinâmico para você.

No rodapé, você encontrará links para acessar o site e as redes sociais da GEP. O sumário do e-book permite, também, o acesso direto a cada um dos tópicos.

SUMÁRIO

Introdução: O papel do DPO na LGPD 4

Ah...E o principal de tudo: este e-book é fruto da nossa experiência como DPO as a Service em inúmeras empresas, o que nos traz muita alegria e segurança em compartilhar todos esses desafios com vocês!

Divirta-se!

SOBRE OS AUTORES

MAURÍCIO ROTTA

sócio-fundador da GEP Soluções em Compliance

- Advogado e Cientista da Computação
- Doutor e Mestre em Engenharia e Gestão do Conhecimento – UFSC
- Especialista em Desenvolvimento de Sistemas Web
- Certificação em Governança em Privacidade e Proteção de Dados – Nymity/CIS Controls
- Certificação em Lead Implementer e Internal Auditor da ISO 27701 – ABNT

BRUNO BASSO

sócio-fundador da GEP Soluções em Compliance

- Advogado e Procurador de carreira do Munícipio de Florianópolis
- Coordenador do Comitê de Auditoria Estatutário da SCPAR
- Especialista em gestão de riscos e compliance
- Certificação Profissional em Compliance Anticorrupção – “CPC-A” – LEC
- Certificação Internacional em Information Privacy Professional/Europe (CIPP/E) – IAPP
- Certificação em Lead Implementer e Internal Auditor da ISO 27701, ISO 37001 e ISO 37301 – ABNT

SUMÁRIO

Introdução: O papel do DPO na LGPD 5

1º Desafio: Ter uma visão multidiciplinar da LGPD 8

2º Desafio: Saber se relacionar com diversos stakeholders 10

3º Desafio: Lidar com a falta de maturidade organizacional 12

4º Desafio: Reagir rapidamente a situaçõesde alta complexidade 15

5º Desafio: Desenvolver uma nova cultura na organização 17

Bônus: 3 passos essencias para o projeto de adequação à LGPD 19

Conclusão 22

INTRODUÇÃO: O PAPEL DO DPO NA LGPD

O DPO (Data Protection Officer), também conhecido como Encarregado pelo Tratamento de Dados Pessoais, é o principal responsável por manter a conformidade das organizações com a LGPD, sendo considerado o verdadeiro guardião do Programa de Governança em Privacidade.

Segundo a Lei Geral de Proteção de Dados Pessoais (LGPD), o DPO deve ser uma pessoa, natural ou jurídica, indicada pelo controlador, para atuar, principalmente, como um canal de comunicação entre o agente de tratamento, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

CURIOSIDADE

A função de DPO não foi criada pela Lei Geral de Proteção de Dados Pessoais (LGPD), nem, tampouco, pelo Regulamento Geral sobre Proteção de Dados da União Europeia (GDPR). Ela, na realidade, já se encontrava prevista na Diretiva 95/46/CE, ainda que de forma tímida e ainda muito simplificada.

Cabe ao DPO, dentre outras atribuições, apoiar a empresa no desenvolvimento das seguintes atividades:

- Formular regras de boas práticas para o bom funcionamento do Programa de Governança de Privacidade
- Elaborar o mapeamento do ciclo de vida dos dados pessoais
- Determinar e documentar a base legal utilizada para o tratamento de dados pessoais
- Avaliar as atividades que geram riscos à organização e aos titulares de dados
- Entender quais são as normas de privacidade e proteção de dados aplicáveis à empresa
- Definir as medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais
- Monitorar a conformidade da organização com a LGPD
- Elaborar Registros das Operações de Tratamento de Dados Pessoais e Relatórios de Impacto de Proteção de Dados Pessoais
- Realizar treinamentos e capacitações aos colaboradores

Auxiliar na condução de incidentes de segurança da informação

No Brasil, a função de DPO já se encontra regulamentada pelo Ministério do Trabalho, por meio da **Classificação Brasileira de Ocupações (código 1421-35)**, cabendo ao Encarregado de Proteção de Dados Pessoais:

- Planejar processos de riscos e de proteção de dados pessoais e privacidade
- Participar da implementação do programa de governança em privacidade
- Monitorar e avaliar o cumprimento das políticas do programa de governança em privacidade
- Participar da identificação de situações de riscos e propor ações para mitigação deles
- Prestar atendimento ao cliente e/ou cooperado e/ou titular de dados pessoais

Como se vê, o DPO precisa estar preparado para lidar com uma série de desafios. Neste e-book, vamos compartilhar apenas cinco deles...

Está preparado? Então, vamos nessa!

1º DESAFIO: TER UMA VISÃO MULTIDISCIPLINAR DA LGPD

Antes de mais nada, tenha cinco questões fundamentais em mente:

1 A LGPD é uma lei que precisa ser interpretada por meio de uma visão multidisciplinar.

2 O Encarregado de Dados Pessoais não precisa, necessariamente, ter formação jurídica, mas, sim, conhecimentos, habilidades e atitudes.

3 Não é necessária qualquer certificação ou formação específica para você ser um DPO.

4 O foco deve estar, principalmente, nas pessoas e não apenas na implementação de controles.

5 Acima de tudo, o DPO é construtor de pontes, não de muros!

Na realidade, o mais importante é que o DPO tenha uma visão global da organização e conhecimentos multidisciplinares em privacidade, proteção de dados pessoais e segurança da informação, além, claro, de conhecimentos em gestão de riscos.

O desafio do DPO, portanto, não é apenas ser o de ser um profissional com uma determinada formação, mas, sim, o de ter uma visão holística de várias áreas e um conhecimento multidisciplinar.

Isso quer dizer que o DPO deve ser um apaixonado pelo tema e, antes de mais nada, ser um conhecedor de processos, um profissional habilidoso na gestão de pessoas, além de ter que possuir uma visão analítica e inovadora, apresentar rápida capacidade de aprendizado sobre as diversas áreas de negócio e, em alguns casos, entender muito bem sobre os conceitos de Privacy by Design.

De fato, o DPO precisa ser um verdadeiro “generalista especialista”!

E, daí, achou que seria fácil ser um DPO? Então, prepare-se, porque só está começando!

2º DESAFIO: SABER SE RELACIONAR COM DIVERSOS STAKEHOLDERS

Stakeholders ou Partes Interessadas são aquelas pessoas que, de alguma forma, se relacionam com a sua organização, como, por exemplo, os colaboradores, os prestadores de serviço e os próprios parceiros de negócio.

Dentre as principais parte interessadas que se relacionam com a sua organização podemos mencionar os Titulares de Dados Pessoais, as clientes, controladores de dados pessoais, operadores de dados pessoais e órgãos de fiscalização, como o Ministério Público e o Procon.

Nesse contexto, o grande desafio do Encarregado de Dados Pessoais é justamente o de ter que lidar - muitas vezes ao mesmo tempo - com as legítimas expectativas de todos esses stakeholders. Não é por outro motivo, aliás, que o DPO precisa vestir vários “chapéus”.

O DPO, na realidade, precisa não apenas mapear as partes que têm interesses ou responsabilidades associadas ao tratamento de dados pessoais, ou seja, aquelas que possam afetar, ser afetada ou perceber que são afetadas por uma decisão ou atividade relacionada ao tratamento de dados pessoais, como, principalmente, entender as suas necessidades e expectativas.

Sob esse olhar, é evidente que a principal dificuldade para o DPO é a de ter que buscar "equilibrar esses pratos" dentro do que a legislação impõe em termos de prazo e de cumprimento de obrigações de *compliance*

Em outras palavras, o DPO precisa não apenas desenvolver as suas atividades, como buscar estar atento a todas as atividades que possam estar relacionadas ao tratamento de dados pessoais e que, de alguma forma, afetem os interesses das partes interessadas.

Por isso, antes de exercer a função de DPO, procure conhecer as partes interessadas e formar um time de privacidade que possa ajudá-lo no dia a dia. Sem isso, você estará correndo muito mais riscos do que o necessário!

3º DESAFIO: LIDAR COM A FALTA DE MATURIDADE ORGANIZACIONAL

Quando tratamos de um assunto tão novo, complexo e desafiador, como se trata da adequação de uma empresa à LGPD, é natural que muitas dificuldades surjam no decorrer do processo.

A principal delas, nós diríamos, são as objeções criadas por muitos colaboradores em relação ao tema. É muito comum o DPO ouvir expressões como “a lei não vai pegar”, “mais uma burocracia”, “a empresa vai quebrar”, entre outras. Isso, por óbvio, se deve ao fato de o assunto ainda estar pouco difundido no Brasil quando em comparação com o cenário mundial.

Este, portanto, é um dos principais desafios do DPO: lidar com a falta de maturidade organizacional com relação à privacidade, proteção de dados pessoais e segurança da informação.

Lembre-se, também, de que o nível de maturidade pode variar, inclusive, de “setor para setor” e de “pessoa para pessoa” mesmo dentro da sua organização.

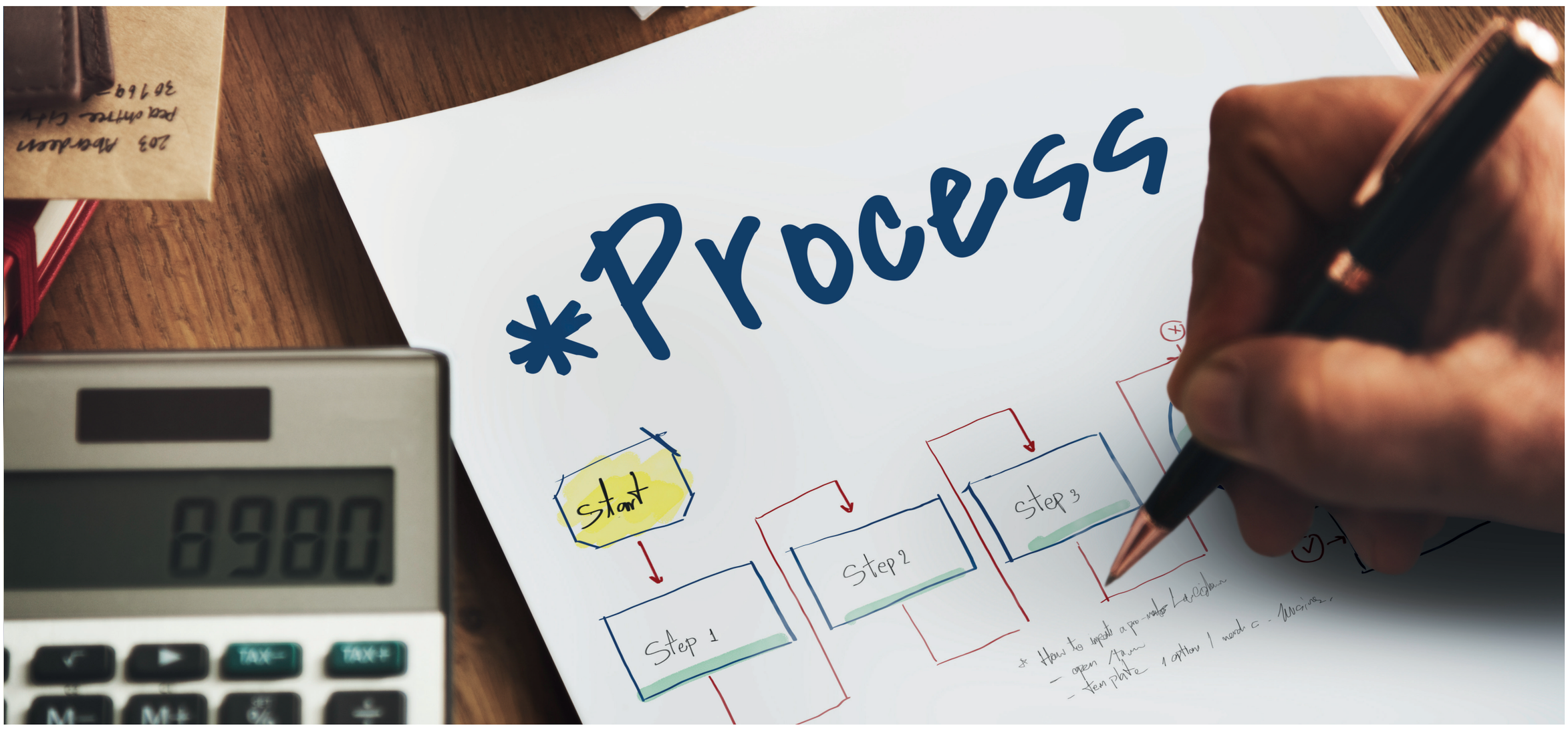
Por isso, além de entender as necessidades e

expectativas das principais partes interessadas, é preciso que o DPO consiga mapear os pontos fortes e fracos da organização e o seu contexto, levando em consideração fatores como:

1. Tamanho, estrutura e delegação de autoridade para tomada de decisão da organização
2. Localizações e setores de atuação da organização
3. Natureza, escala e complexidade das operações e atividades da organização
4. Modelo de negócio da organização
5. Entidades sobre as quais a organização tenha controle e entidades que exerçam controle sobre a organização
6. Parceiros de negócio da organização, clientes e outras partes interessadas
7. Obrigações e deveres estatutários, regulatórios, contratuais e profissionais aplicáveis.

Pode-se pensar, também, em utilizar métricas para medir o nível de maturidade organizacional em relação ao

tema, entrevistar os pontos focais da organização e, até mesmo, realizar dinâmicas para entender melhor o nível de compreensão das pessoas.



É recomendável ao DPO, portanto, sempre buscar estruturar uma governança em privacidade adequada ao modelo de negócio da sua organização, para suportar e alavancar o processo de adequação à LGPD.

4º DESAFIO: REAGIR RAPIDAMENTE A SITUAÇÕES DE ALTA COMPLEXIDADE

O DPO precisa agir, rapidamente, em situações de alta complexidade e difícil resolução.

IMAGINE A SEGUINTE A SITUAÇÃO

Um colaborador salva alguns dados pessoais que estão sob a posse da organização em um pendrive. Esse dispositivo móvel é pessoal e acabou de ser furtado do colaborador. O colaborador comunica o fato apenas trinta dias após o ocorrido ao DPO. O que você faria?

É preciso agir rapidamente e adotar uma série de decisões. Será que o colaborador podia ter copiado os dados pessoais para o pendrive? Será que o colaborador foi devidamente instruído sobre a proibição? Há política dispondo sobre a utilização de dispositivos móveis pessoais na organização? Os dados pessoais estavam criptografados? Quais tipos de dados pessoais foram furtados? O ocorrido é caracterizado como um incidente de segurança da informação? Se for um incidente de segurança da informação, ele tem potencial de causar prejuízos a seus titulares? Mesmo após ter transcorrido o prazo de

SUMÁRIO

legal, a organização tem a obrigação de comunicar à ANPD? Preciso acionar o departamento jurídico e/ou o de segurança da informação? E por aí vai....

Percebam que o DPO necessita, com a maior brevidade possível, tomar decisões um tanto quanto complexas, o que, por certo, pode levá-lo a adotar atitudes inadequadas.

IMAGINE UMA OUTRA SITUAÇÃO

O setor de segurança da informação da sua organização acaba de comunicar a ocorrência de um incidente com o vazamento de milhares de dados pessoais de crianças. Não se tem ainda a dimensão da gravidade, mas há possibilidades de terem sido furtados por um hacker. O que você faria como DPO?

Tentaria entrar em contato com o hacker diretamente? Acionaria as autoridades competentes? Solicitaria a realização de uma investigação interna? Faria tudo ao mesmo tempo? O que você priorizaria?

Como se vê, o DPO, além de ter que agir preventivamente, precisa apoiar a organização a mitigar eventuais impactos negativos de situações indesejadas, auxiliar na apuração e, acima de tudo, resguardar os interesses da organização.

5º DESAFIO: DESENVOLVER UMA NOVA CULTURA NA ORGANIZAÇÃO

Um dos maiores desafios para qualquer profissional, é conceber algo do “zero”. Imagine quando passamos a falar de um novo conceito, de situações inéditas e de estruturas completamente inovadores.

Não há dúvidas de que esse é um grande – senão o principal – desafio de um DPO. É o que muitas vezes chamamos de “pregar no deserto”!

De fato, cabe ao DPO enfrentar o desafio de ser o precursor da mudança de mentalidade e da criação de uma cultura voltada à privacidade e à proteção de dados pessoais, o que será vital para que a organização atinja níveis aceitáveis de conformidade com a LGPD e se mantenha em compliance com a legislação.

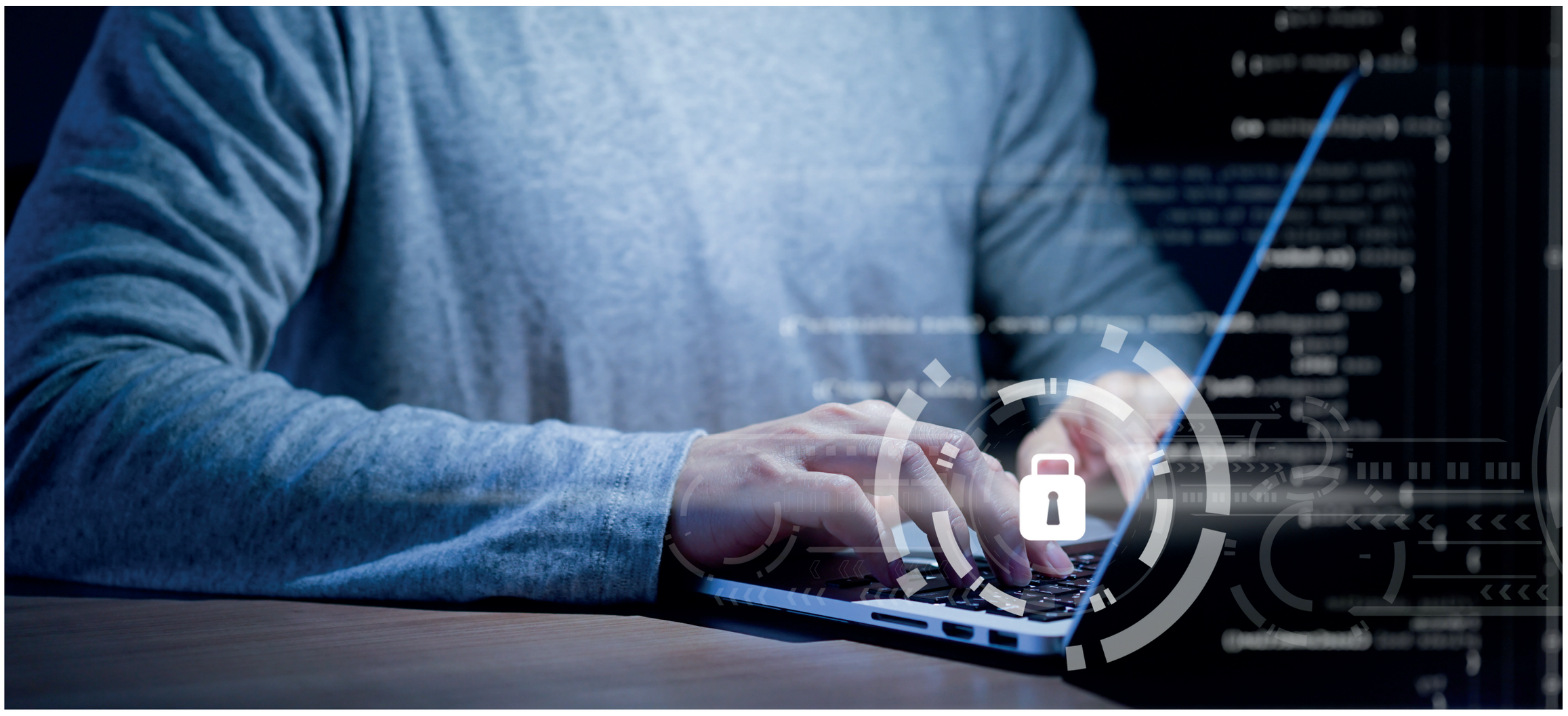
E todos sabemos que não se muda a cultura de uma organização “da noite para o dia”. É preciso comunicar, treinar e, acima de tudo, buscar engajar as pessoas em relação ao tema, o que, claro, é muito desafiador.

A transformação cultural, portanto, vai envolver um grande esforço por parte do DPO, cabendo a ele introduzir esses novos conceitos por meio de exemplos que façam sentido para cada um dos setores da organização. É, em outras palavras, a adoção do famoso walk the talk.

Não basta, assim, simplesmente impor controles sem explicar o real motivo para as pessoas envolvidas com o tema. É preciso transformar o as pessoas, para, só assim, promover a transformação cultural em relação tema de forma efetiva e prática!

Esse desafio é osso duro de correr...então, respire fundo e avance!

BÔNUS: 3 PASSOS ESSENCIAIS PARA O PROJETO DE ADEQUAÇÃO À LGPD



Separamos aqui 3 passos essenciais para o projeto de adequação à LGPD, que dever ser seguidos pelo DPO.

Primeiro Passo: entender o contexto da organização

Antes de mais nada, é preciso entender o contexto da organização, conhecer as principais partes interessadas, formar o time de privacidade e sensibilizar os colaboradores.

É que sem engajar a todos, a LGPD torna-se apenas mais uma ferramenta burocrática dentro da organização. E lembre-se: não há um modelo único, por isso é necessário ter visão acerca das principais obrigações de compliance que a empresa, mandatoriamente ou voluntariamente, precisa cumprir.

Nessa fase, por exemplo, você pode definir quais serão as pessoas diretamente envolvidas com o projeto, levantar as principais preocupações da organização em relação ao tema e promover palestras de sensibilização na sua

empresa.

Não se esqueça, também, de ter bem clara a definição de papéis e responsabilidades, especialmente, em relação ao exercício da função de encarregado pelo tratamento de dados pessoais.

Segundo Passo: realizar a avaliação de riscos de compliance

Este passo vai exigir de você um pouco mais de tempo, esforço e conhecimento técnico, em razão da necessidade de se buscar as principais fontes de riscos ligados à proteção de dados pessoais e segurança da informação dentro da sua empresa.

A avaliação de riscos de compliance envolve as etapas de identificação, análise, avaliação, tratamento e comunicação dos riscos, por meio da análise de documentos e realização de entrevistas pessoais com os pontos focais da organização.

É nessa fase também que você deve fazer o mapeamento do ciclo de vida dos dados pessoais da sua organização, com o objetivo de entender como ocorre a coleta, o processamento e o arquivamento de dados pessoais dentro da sua empresa.

Como se percebe, este é um passo fundamental para o sucesso do compliance dentro da sua empresa.

Terceiro Passo: implementação dos planos de ação

O terceiro passo corresponde à implementação dos planos de ação levantados na etapa anterior. É chegada a hora de "botar a mão na massa", para dar início à elaboração da Política de Privacidade, da Política de Segurança da Informação e à adequação dos processos e procedimentos relacionados.

Por fim, e não menos importante, você deve realizar treinamentos e capacitações a todas as partes interessadas, com o objetivo de engajar cada vez mais as pessoas responsáveis pelo dia a dia da sua empresa.

CONCLUSÃO

Ser um DPO não é apenas cumprir com uma obrigação legal, mas, uma verdadeira oportunidade de melhoria da cultura organizacional relacionada ao tema. É que o Encarregado pelo Tratamento de Dados Pessoais é, de fato, o guardião da efetividade do Programa de Governança em Privacidade de Dados.

Antes de definir se você está preparado para ser um DPO, pense se você está preparado para pensar fora da caixa. Não há soluções simples ou lógicas, mas holísticas e amplas.

Lembre-se de que o DPO deve ser um verdadeiro porta-voz da cultura de proteção de dados, cabendo a ele agir de maneira preventiva, detectiva e responsiva!

Esperamos que você tenha aproveitado a leitura e os insights deste e-book!