guia prático · guia prático ·

Programa de Governança em Privacidade

ZOOX
SMART DATA

Expediente

Autoria: Daniela M. Monte Serrat Cabella, CIPM

Zoox Smart Data
Rio de Janeiro, 15 de dezembro de 2020.

índice · índice · índice · índice

ZOOX SMART DATA

INTRODUÇÃO

Um “Privacy Program” ou “Programa de Privacidade” é, pela própria definição de “program”, “um conjunto de medidas ou atividades relacionadas com um objetivo específico de longo prazo”. É por essa razão que se define o conjunto de atividades relacionadas à Privacidade como um “programa” (na tradução direta do termo em inglês), pois são atividades relacionadas com um objetivo de longo prazo.

Nessa linha, um Programa de Governança em Privacidade deve apresentar uma estrutura que dá base para o profissional de privacidade e proteção de dados atuar com segurança de modo a direcionar a organização para ir além da simples conformidade à legislação e contribuir para o bem comum. Essa estrutura deve levar em consideração toda e qualquer legislação de proteção de dados que incida sobre a operação da organização, e deve incorporar a privacidade desde a concepção e por padrão. Quando implementado de forma adequada, contribui para a gestão e longevidade da organização, maior eficiência operacional e fidelização de clientes, e ainda lhe agrega valor, quase como um ativo à parte.

Vivemos um momento de transição para uma nova cultura, de uso sustentável dos dados pessoais. A implementação e melhoria contínua de um Programa de Governança em Privacidade para que essa nova cultura se torne, de fato, uma realidade envolve diversas atividades e demanda um grande esforço e investimento por parte da organização. Conhecendo o tamanho do desafio e sua complexidade, e tendo recebido diversas solicitações de clientes e parceiros para que compartilhássemos a forma como estruturamos o Programa dentro de casa, resolvemos publicar uma versão resumida, no formato de um guia prático, para contribuir com o mercado e facilitar a implementação do mesmo tipo de Programa nas mais diversas organizações.

GESTÃO DO PROGRAMA

O ideal é que a Gestão do Programa de Governança em Privacidade seja realizada pelo Data Protection Officer (DPO), Encarregado pelo Tratamento de Dados Pessoais de uma organização ou Chief Privacy Officer (CPO), com o apoio de uma área dedicada, de forma exclusiva, ao tema de privacidade e proteção de dados pessoais e que responda diretamente ao CEO. É fundamental garantir que, dentro do cenário específico da operação, o Gestor do Programa e a área que o apoia tenham:

1. Acesso para comunicação direta com o(s) responsável(eis) pelas tomadas de decisão estratégicas da organização, garantindo que não haja nenhuma espécie de "filtro" nem "atraso" (intencional ou não) em relação às comunicações em matéria de privacidade e proteção de dados;

2. Autonomia concreta para a condução do Programa de Governança em Privacidade, e

3. Isenção de quaisquer conflitos de interesse relacionados à sua posição na organização.

PRINCÍPIOS

Todas as ações e atividades do Programa de Governança em Privacidade devem ser pautadas pelos sete princípios do framework de *Privacy by Design*, criado por Ann Cavoukian, quais sejam:

I. Proativo e não reativo; preventivo e não corretivo

II. Privacidade como padrão (by default)

III. Privacidade incorporada ao Design

IV. Funcionalidade total (soma positiva)

V. Segurança de ponta-a-ponta

VI. Visibilidade e transparência

VII. Respeito pela privacidade do usuário

OBJETIVOS

Os objetivos do Programa de Governança em Privacidade são:

1. COMPLIANCE - Monitorar e melhorar continuamente o nível de compliance em Privacidade e Proteção de Dados Pessoais, propor medidas para ir além do simples cumprimento da legislação e agregar valor ao consumidor final e à própria organização;

2. RISCO - Realizar análise e gestão de risco à privacidade e proteção de dados pessoais de forma eficaz, de acordo com melhores práticas internacionais consolidadas e levando em consideração aspectos éticos envolvidos no tratamento de dados pessoais;

3. PRIVACY BY DESIGN - Promover a privacidade desde a concepção (privacy by design) e por padrão (privacy by default) nos produtos e serviços da organização;

4. GOVERNANÇA - Elaborar, revisar, implementar, divulgar, atualizar e monitorar o nível de aderência a Políticas, Normas e Procedimentos de Proteção de Dados Pessoais, incluindo os relacionados à Segurança da Informação, de modo a contribuir para que a organização esteja preparada para responder, de modo eficaz e em tempo hábil, a eventuais incidentes com dados pessoais, bem como às requisições de titulares de dados pessoais e de autoridades públicas, e

5. COMUNICAÇÃO E CULTURA - Contribuir para a criação e fortalecimento de uma cultura de privacidade e segurança da informação tanto interna como externa à organização (mercado).

ROTEIRO DE IMPLEMENTAÇÃO

Seguem, abaixo, as principais atividades a serem implementadas para garantir a eficiência tanto da gestão do Programa como da implementação de cada um dos cinco objetivos propostos acima.

Fundamentos e Gestão

- Nomear DPO da organização.
  - Assinatura do Termo de Nomeação com a descrição objetiva das responsabilidades, obrigações, atividades, garantias e limitações da função, bem como menção à cobertura de sua atuação (organização apenas ou grupo, território nacional ou internacional), a ser assinado pelo CEO ou função equivalente na organização.
  - Divulgação interna da nomeação, mediante comunicado. O ideal é utilizar tanto o modo informal (que costuma ser mais direto e eficaz) como formal (que documenta a ação de divulgação oficial).
  - Divulgação externa, que deve incluir a menção do DPO no site da organização (na Política de Privacidade, por exemplo), bem como outras formas de comunicação ao mercado e às autoridades.

- Garantir que a Privacidade e a Proteção de Dados sejam inseridas como Valores da organização.

- Garantir que a Privacidade e a Proteção de Dados sejam inseridas no Planejamento Estratégico e se tornem Estratégias “core” da organização.

- Inserir diretrizes de privacidade e proteção de dados no Código de Ética e Conduta da organização.

- Garantir que haja recursos financeiros e humanos (equipe) suficientes para o desempenho das atividades do Programa (é responsabilidade da organização prover tais recursos).

- Criar sistema de gestão de demandas. Como a implementação do Programa exige contato frequente com todas as áreas da organização e que elas mesmas demandem o DPO e a área de Privacidade e Proteção de Dados, é necessário ter uma forma organizada e estruturada para receber e responder às demandas. É recomendável a utilização de softwares específicos para gestão de demandas como o Monday, Jira, Trello ou Notion, por exemplo.

- Aplicar metodologia ágil para a gestão de atividades e demandas relacionadas ao Programa. Sempre haverá muito trabalho a ser feito ou revisado e melhorado, portanto é recomendável adotar sprints de uma semana e as matrizes RUT e RICE para apoio à priorização das atividades e demandas. No Anexo I, há maiores informações sobre essas matrizes e sua adaptação para a gestão pela área de Privacy & Data Compliance da Zoox, feita pelo Marcelo Martins, Scrum Master e Gerente de Projetos, e Daniela Cabella, DPO e Head of Privacy & Data Compliance.

- Estabelecer Comitê de Privacidade e Proteção de Dados Pessoais, com Regulamento próprio, para a tomada de decisão colegiada nos casos pertinentes.

Compliance

- Mapear todos os dados pessoais e operações de tratamento, tanto para dados de usuários de produtos e/ou serviços da organização, como de não usuários, ou seja, funcionários, representantes de clientes, parceiros e fornecedores, ou terceiros.
    - Desenhar o fluxo da operação, que pode ser feito nos moldes do modelo da ISO 29134 ou de forma customizada.
    - Criar ou revisar o inventário de dados pessoais e operações de tratamento.
- Mapear a legislação incidente na operação e o nível de compliance para cada controle legal ("implementado", "documentado" e "monitorado", como nas auditorias de segurança da informação). O controle de compliance à legislação pode ser realizado por meio do uso de softwares, planilhas ou de outras formas - o que importa é que haja um controle efetivo e completo do nível de compliance e que se consiga extrair dados para tomadas de decisão e métricas para quantificar a evolução do Programa.
    - Para o controle de cumprimento do Regulamento n. 2016/679 (General Data Protection Regulation, ou GDPR), há um excelente modelo de controle publicado pela ICO, autoridade de proteção de dados do Reino Unido (*Information Commissioner's Office*).

- Para a Lei Geral de Proteção de Dados Pessoais brasileira (Lei n. 13.709/2018, LGPD), é importante adotar um controle que cubra "cada vírgula" da lei. Adotamos um modelo de controle da Complete Privacy que agrega todos os controles da LGPD em cinco pilares (Fundamentos, Princípios, Direitos do Titular, Obrigações e Governança) e se soma ao controle de Segurança da Informação.

- Para o controle de Segurança da Informação, recomenda-se a adoção de melhores práticas reconhecidas internacionalmente, como os frameworks da ISO 27001 ou NIST, por exemplo.

- Importante registrar os pontos em que a organização vai além do simples compliance e contribui para o bem comum.

- Utilizar os controles mapeados para apoiar as tomadas de decisão e elaborar Planos de Ação.

- Mapear todos os contratos vigentes e realizar a inclusão ou revisão das cláusulas de proteção de dados pessoais e privacidade.

- Elaborar, revisar ou atualizar cláusulas padrão de proteção de dados customizados para o modelo de negócio.

- É possível criar modelos de cláusulas ou Acordos de Tratamento de Dados Pessoais inspirados nos modelos de Standard Contractual Clauses (SCC) que a Comissão Europeia publicou ou com base em Data Processing Agreements (DPAs) publicamente disponíveis de organizações reconhecidas por seus esforços em proteção de dados pessoais, como o do ProtonMail, realizando apenas a adaptação para a legislação local (quando aplicável) e para o modelo de negócio da organização. Não se pode ignorar que há diversos países e organizações internacionais que já têm experiência nos temas de privacidade e proteção de dados por muito mais tempo do que o Brasil, sendo recomendável aprender com os acertos e melhores práticas já consolidadas. A semelhança de abordagem do tema, ou até mesmo uma certa padronização, facilita os negócios, pois, como frequentemente se diz, "os dados não veem fronteiras" e, por vezes, acabam atraindo para a organização a incidência de diversas normas de proteção de dados e privacidade de uma só vez.

- Documentar medidas técnicas e administrativas que comprovam o cumprimento dos sete princípios de *Privacy by Design.*

- Realizar auditorias (internas, em parceiros e em clientes), para verificar o nível de proteção de dados e privacidade que é aplicado em toda a cadeia de tratamento dos dados pessoais.

Risco

- Estabelecer um programa de Gestão de Riscos. Diante de diversos frameworks de melhores práticas para a gestão de riscos, adotamos o da ISO 31000 conjugado com os sete princípios de *Privacy by Design.*

- Realizar análise de risco à privacidade (ISO 29134) e à proteção de dados pessoais (template de Data Protection Impact Assessment (DPIA) da ICO e modelo de Relatório de Impacto do MPDFT).

- Considerar aspectos éticos do tratamento de dados pessoais como medida que vai além do mero compliance.

- Analisar a necessidade de contratação de seguro cyber, e, em caso positivo, contratar o mais adequado.

Privacy by Design

- Construir materiais de apoio para a equipe de Produto (ou equivalente), como a elaboração de Persona, e Jornada do Usuário com aspectos de privacidade, para apoiar a na criação de novos produtos, funcionalidades ou serviços que sejam *privacy by design e by default.*

- Integrar com equipe de Produto (ou equivalente) não apenas de forma orgânica, mas também estruturada, com a criação de processos e adoção de ferramentas que possibilitem maior integração entre essa área e o DPO/equipe de Privacidade e Proteção de Dados no fluxo de desenvolvimento de novas soluções.

Governança

- Mapear quais Políticas ("diretrizes"), Normas ("regras") e Procedimentos de Proteção de Dados e Segurança da Informação já foram elaborados, aprovados e divulgados e quais ainda não o foram. Utilizar uma lista de apoio, como o exemplo do Anexo II.

- Elaborar Plano de Ação para redigir, aprovar, divulgar, revisar e monitorar a aderência a todos os documentos de Governança de Proteção de Dados e Segurança da Informação.

Comunicação e Cultura

- Construir um Plano de Comunicação que garanta a frequência e eficiência necessárias para o desenvolvimento das atividades do Programa.

    - Plano de Comunicação Interno para a conscientização sobre o tema de privacidade e proteção de dados pessoais, para contribuir com o compliance, mitigar falhas humanas, e fortalecer a cultura da organização nesses aspectos

    - Plano de Comunicação Externo, como medida que vai além do compliance. No Brasil, a legislação específica de proteção de dados pessoais é recente, o que significa que precisamos contribuir para (i) que o usuário ou consumidor final titular dos dados (de modo geral, a sociedade) entenda que ganhou novos direitos, o que eles significam e como exercê-los, bem como para (ii) colaborar com o compartilhamento de melhores práticas, de modo a elevar o nível geral de conhecimento aplicado sobre proteção de dados e privacidade em todo o mercado, prática que não apenas valoriza os negócios que aplicam tais medidas, como também contribui para o uso sustentável de dados pessoais.

- Estabelecer a comunicação diária entre o DPO e a equipe de Privacidade e Proteção de Dados para garantir o alinhamento, a agilidade e a eficiência na realização das atividades do Programa.

- Estabelecer a comunicação direta com o CEO, no mínimo semanal, sobre os assuntos de Privacidade e Proteção de Dados.

- Garantir que haja comunicação livre e direta (também frequente) com todas as áreas (gestores e operação) para alinhamento de assuntos de Privacidade e Proteção de Dados Pessoais.

- Elaborar e aplicar treinamentos semestrais, ou de maior frequência, de Privacidade e Segurança da Informação para fortalecer a cultura de Proteção de Dados na organização, e medir o nível de absorção do conteúdo. Elaborar Plano de Ação para correção de baixa absorção do conteúdo de matérias específicas, se aplicável.

MELHORIA CONTÍNUA

A organização e o contexto em que se insere estão em constante mudança. Por isso, é fundamental manter um ciclo PDCA de melhoria contínua. Algumas atividades envolvidas nesse processo são:

- Monitorar o cenário legislativo para novos Projetos de Leis e Decretos relacionados à matéria e que possam afetar a operação.
- Monitorar o surgimento de novas melhores práticas de proteção de dados pessoais.
- Determinar o cronograma de revisão e atualização dos mapeamentos, fluxos, inventários, políticas, normas e procedimentos. Também realizar revisões e atualizações desses documentos caso haja alterações no modelo de negócio ou na operação, ou ainda no cenário societário ou legislativo.
- Realizar auditorias tanto interna como em fornecedores, parceiros e clientes.
- Elaborar plano para garantir o aprendizado contínuo da equipe de Privacidade e Proteção de Dados.
- Empenhar esforços para que tanto a organização como os profissionais que trabalham com o tema de privacidade e proteção de dados sejam certificados na matéria.

CONSIDERAÇÕES FINAIS

Cada organização pode e deve adaptar o Programa de Governança em Privacidade ao seu próprio modelo de operação, lembrando sempre de cobrir os cinco objetivos para garantir a solidez do Programa. Por fim, é importante lembrar que a própria documentação do Programa de Governança em Privacidade já é uma medida administrativa de Privacy by Design que cumpre o princípio de “proativo e não reativo, preventivo e não corretivo”, bem como o princípio da responsabilização e prestação de contas da LGPD.

ANEXO I

Priorização Ágil de Atividades e Demandas de Privacidade e Proteção de Dados

Por Marcelo Martins e Daniela Cabella

Matriz RUT

Para aplicar a matriz de "Relevância x Urgência x Tendência" (RUT) na priorização de atividades e demandas que envolvam a matéria de Privacidade e Proteção de Dados, recomendamos que o Gestor do Programa de Privacidade leia cada item da lista de pendências ("backlog"), esclareça dúvidas se necessário, e convide todos os membros da equipe de Privacidade e Proteção de Dados a votar (de 1 a 5), junto com ele, cada um dos três critérios, conforme a seguir:

VALOR	1	2	3	4	5
Relevância *(Qual o valor para o Programa de Privacidade?)*	Não faz parte do Programa de Privacidade. Seria bom ter, mas ficamos bem sem isso.	É relacionado ao Programa de Privacidade, seria bom ter.	Importante para o Programa de Privacidade.	Muito importante. O Programa de Privacidade fica desfalcado sem essa medida.	Não há Programa de Privacidade sem essa medida.
Urgência *(Qual é o timing?)*	Implementar agora não faz diferença. Dá para esperar.	Não é bom ficar sem, mas dá para esperar.	É desejável lançar em breve, na próxima Sprint talvez.	Teremos problemas se não estiver na próxima Sprint.	É imediato. Não podemos esperar a próxima Sprint.
Tendência *(Qual é a perspectiva da empresa?*	A primeira impressão não é boa, mas a empresa se acostuma com a ausência dessa medida.	Pode ser problemático para a empresa continuar sem isso.	É certo que a empresa será prejudicada sem isso.	O prejuízo para a empresa não só é certo, como também aumenta com o tempo.	Piora muito a cada dia, é extremamente desgastante para a empresa continuar sem isso.

A votação deve ocorrer ao mesmo tempo para que ninguém seja influenciado na sua escolha de nota (o famoso “1, 2, 3 e já!”). Muito provavelmente não haverá consenso inicial na maioria das vezes, e isso levará a uma discussão organizada sobre os motivos pelos quais cada um escolheu determinada nota. O objetivo é que todos cheguem a um consenso final sobre a nota para cada um dos três critérios e depois os multiplique. Dessa forma, a pontuação de cada item do backlog terá entre 1 e 125 pontos, sendo que os de maior nota deverão ficar no topo da lista de pendências e os de menor nota ao final, como menos prioritários.

Conforme destaca Andressa Chiara em seu artigo, existe um grande valor nas discussões geradas para defesa das notas, pois muitas informações que emergem nesse momento dificilmente seriam reveladas de outra forma. Além disso, é possível gerar métricas de valor entregue por sprint e valor agregado, o que, na nossa visão, também é útil para a gestão de atividades e demandas de um Programa de Governança em Privacidade.

Matriz RICE

Após a atribuição de notas aos itens do backlog pela Matriz RUT, é comum que alguns deles fiquem com pontuação igual. Como critério de desempate, utilizamos a Matriz RICE (“Reach x Impact x Confidence x Effort”, ou seja, “Alcance x Impacto, x Confiança x Esforço”).

Alcance	Impacto	Confiança	Esforço	RESULTADO
Métricas	1 a 5	%	Pessoas / Sprint	A * I * C / E

O alcance deve ser pontuado conforme o número de pessoas que a atividade ou tarefa irá impactar ao final (exemplo: notificação sobre atualização da Política de Privacidade para “X" usuários do produto); o nível de impacto deve ser medido de 1 (baixo) a 5 (alto); o nível de confiança do Gestor e da equipe de Privacidade e Proteção de Dados deve ser medido em termos de porcentagem (quanto maior a porcentagem, maior a confiança), e o esforço deve refletir o número de pessoas envolvidas na realização da tarefa por sprint. Os quatro critérios devem ser equacionados da seguinte forma:

(Alcance x Impacto x Confiança) / Esforço

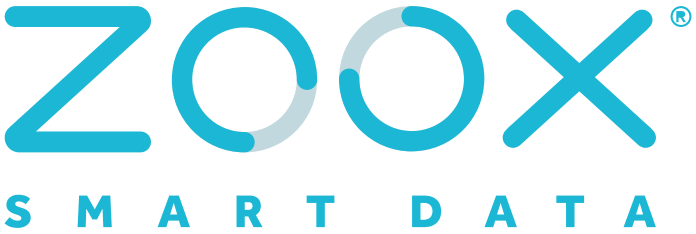
O valor resultante da Matriz RICE deverá ser utilizado, portanto, como critério de desempate para os itens com mesma pontuação pela Matriz RUT, sendo que os itens com score RICE maior devem ser priorizados.

ANEXO II

Lista Básica de Documentos de Governança

- Política de Segurança da Informação
- Política de Proteção de Dados Pessoais
- Política de Privacidade do Site
- Políticas de Privacidade dos Produtos ou Serviços
- Política de Gerenciamento de Riscos
- Norma de Classificação da Informação
- Norma de Gestão de Identidade e Acesso
- Norma de Acesso e Uso de Dados Pessoais
- Norma de Transferência e Armazenamento de Dados Pessoais
- Norma de Retenção e Eliminação/Anonimização de Dados Pessoais
- Norma de Atendimento a Requisições de Titulares
- Norma de Atendimento a Requisições de Autoridades
- Norma de Uso de Recursos de Tecnologia da Informação e
- Comunicação
- Norma de BYOD
- Norma de Uso de Controles Criptográficos

- Norma de Uso de Controles Criptográficos
- Norma de Cloud Computing
- Norma de Teletrabalho/Trabalho Remoto
- Norma de Utilização de Senhas
- Norma de Uso da Internet
-Norma de Uso de Wi-Fi
- Norma de Background check
- Norma de Uso de Rede Social Pública
- Norma de Treinamento em Proteção de Dados
- Norma de Contratação e Auditoria de Terceiros
- Norma de Elaboração e Registro de PIA e DPIA
- Plano de Resposta a Incidentes
- Plano de Continuidade de Negócio
- Procedimento de Atendimento a Requisições de Titulares
- Procedimento de Atendimento a Requisições de Autoridades
- Procedimento de Anonimização e Eliminação Segura de Dados Pessoais
- Procedimento de Notificação de Titulares Envolvidos em Incidente
- Procedimento de Notificação de Autoridades sobre Incidente


ZOOX®
SMART DATA