SUMÁRIO

POLÍTICA DE DIREITO DOS TITULARES..... 2
POLÍTICA DE PRIVACIDADE..... 3
POLÍTICA DE COOKIES..... 4
POLÍTICA DE RETENÇÃO DE DADOS..... 5
POLÍTICA DE REVISÃO DE CONTRATOS..... 6
POLÍTICA DE RESPOSTA A INCIDENTES..... 7
POLÍTICA DE GOVERNANÇA DE DADOS, INFORMAÇÃO E CONHECIMENTO..... 8
POLÍTICA DE SEGURANÇA DE INFORMAÇÕES E SIGILO DE DADOS..... 9
PROCEDIMENTO DE ATENDIMENTO À REQUISIÇÕES DE TITULARES..... 10
REGISTRO DAS OPERAÇÕES DE TRATAMENTO DE DADOS (ROPA)..... 11
RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS (RIPD OU DPIA)..... 12
IMPLANTAÇÃO DE PRIVACY BY DESIGNER..... 13

POLÍTICA DE DIREITO DOS TITULARES

Conceito: Estabelece direitos que podem ser exercidos pelos titulares de dados pessoais perante o controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição.

Principais entregas em relação ao documento e aos direitos dos titulares:

- Breve introdução (conceitos, confirmar existência de tratamento, quais dados são tratados);
- Art. 18, I, da LGPD - Confirmar a existência de tratamento de dados (forma imediata ou complexa)
- Art. 18, II, da LGPD - Direito de obter o acesso e cópia dos dados que foram colhidos (forma imediata ou complexa);
- Art. 18, III, da LGPD - Solicitar correção de dados pessoais;
- Art. 18, IV, da LGPD - Solicitar anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade, salvos os dados necessários para cumprimento de obrigação legal ou regulatória, bem como dados financeiros e outros tratados com finalidade legítima que transcende a vontade do titular;
- Art. 18, IV, da LGPD - Solicitar portabilidade de dados para outro fornecedor de serviço/produto, para que esse terceiro possa oferecer esses produtos ao titular;
- Art. 18, VI, da LGPD – Direito à eliminação de dados, ao menos que o controlador tenha justificativa para manutenção.
- Art. 18, VII, da LGPD - Saber se há compartilhamento com terceiros e, se há, com quem ocorre;
- Art. 18, VIII, da LGPD - Informações sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa.
- Art. 18, IX, da LGPD - Revogar o consentimento;
- Como pode exercer os direitos? Através de qual meio?

Eventuais modelos (Ctrl+clique para ir até a página):

- CIEE
- Carrefour Seguros e Serviços
- InfraNewsTelecom

POLÍTICA DE PRIVACIDADE

Conceito: é o documento que contém as práticas e medidas de Privacidade e Segurança adotadas por determinada organização. Seu objetivo é fornecer informações sobre como a empresa obtém, utiliza, armazena e protege os dados pessoais que coleta, a fim de levar transparência aos donos dos dados pessoais que possui.

Principais entregas em relação ao documento:

- Introdução, infos gerais sobre a empresa e sobre o tratamento de dados;
- art. 6, V, LGPD - Quais dados pessoais são coletados, inclusive os não informados (IP, localização etc.), onde, como e por que esses dados são coletados;
- Onde os dados ficam armazenados, e por quanto tempo;
- Utiliza cookies ou tecnologias semelhantes? Como e quais? (várias empresas colocam a política de cookies dentro da política de privacidade)
- Informações sobre coletar dados de conhecidos do usuário, através de indicações, por exemplo.
- Com quem seus dados são compartilhados (fornecedores de serviços, afiliadas, parceiros de marketing, autoridades públicas/governamentais, operações comerciais, transferência comercial, fusão de empresa etc.)
- Informações sobre medidas de segurança adotadas pela empresa (como mantem os dados seguros, quem pode acessar os dados, medidas tomadas pela empresa, medidas tomadas pelo usuário (senha fraca) etc);
- Informações sobre exercícios de direitos (pode citar a política de direitos ou implementá-la aqui) e de como o titular pode exercê-los;
- Informações de contato do DPO ou do encarregado;
- Alterações da política.
- Algumas empresas colocam um tópico sobre "Incidentes", que explica o que se prossegue quando ocorre algum incidente com vazamento de dados.

Eventuais modelos (Ctrl+clique para ir até a página):

- NuvemShop (gerador de política de privacidade)
- Ambev (Resumo da política)
- DocuSign (plataforma de assinatura de documentos)
- Globo
- Nestle

POLÍTICA DE COOKIES

Conceito: é um documento complementar à Política de Privacidade. Aqui, você encontrará informações objetivas e claras sobre o que são Cookies, quais Cookies utilizamos em nossas aplicações, qual papel desempenham e como configurá-los.

Principais entregas em relação ao documento:

- Introdução explicando sobre Cookies;
- Quais os tipos de cookies são utilizados e de que forma cada um deles funcionam? Exemplo: Cookies essenciais/estritamente necessários, de desempenho, funcionais, de segmentação e rastreamento etc.
- Por que cada um desses cookies é utilizado e qual é o tempo de vida de cada cookie (por quanto tempo eles permanecem válidos, armazenando as infos do usuário)?
- São utilizadas ferramentas analíticas (Google Analytics, por exemplo)?
- Existem cookies de terceiros? Por exemplo, se há um vídeo do youtube no site, o youtube pode oferecer algum cookie para o usuário.
- Como excluir, bloquear ou revogar o consentimento de cookies?
- Atualizações da política;
- Contato

Eventuais modelos (Ctrl+clique para ir até a página):

- Shell
- LegalCloud (gerador de política de cookies)
- Google
- Infomoney (bem completo)
- Volkswagen

POLÍTICA DE RETENÇÃO DE DADOS

Conceito: Essa política estabelece os princípios fundamentais que devem ser adotados ao considerar a retenção e proteção de registros. Além disso, define os tipos de registros mantidos e seus requisitos gerais antes de discutir a proteção, destruição e gerenciamento de dados. A exclusão de dados vem da necessidade de liberar espaço nos servidores, e torná-los mais rápidos e eficientes.

Principais entregas em relação ao documento:

- Quais dados são retidos, por quanto tempo, e em qual nuvem/plataforma/mídia? Obs: Citar qual data é considerada, pois a data de inserção de dados pelo usuário pode ser diferente da data de recebimento de dados pela empresa.
- Sobre a plataforma utilizada para retenção/armazenamento de dados, ela funciona online 24h/dia? Para maior proteção dos dados retidos, é preciso que seja online 24/7.
- E se for solicitada a exclusão, alguns dados ainda serão retidos? Por quanto tempo e para qual finalidade?
- Em relação à essa exclusão, deve ser garantido que os dados excluídos não poderão ser mais usados. O procedimento de destruição deve ser arquivado para que a eliminação possa ser comprovada;
- Algum dado pode ser arquivado para posterior recuperação?
- Cópia de dados do usuário para o usuário antes que sejam excluídos;
- Contato/Encarregado de proteção de dados;
- Art. 16. LGPD - Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades: Cumprimento de obrigação legal/regulatória pelo controlador; estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

Eventuais modelos (Ctrl+clique para ir até a página):

- Adobe
- Cobmais
- Ribeiro Lourenço Advogados (completa)

POLÍTICA DE REVISÃO DE CONTRATOS

Conceito: Contratos não revisados podem estar colocando sua empresa em grande risco. Por isso, é preciso fazer uma revisão periódica deles. A revisão de contratos é uma prática adotada para conferir todas as cláusulas do contrato, e verificar a sua validade e os seus benefícios, de acordo com a legislação.

Principais entregas em relação ao documento:

- Não há um documento exigido por lei de política de revisão de contratos, porém parte da empresa saber e relatar em algum documento como será feita a revisão de contratos, por quem será feita (normalmente um advogado especializado na área.), com qual periodicidade e de quais contratos será a revisão;
- Caso o contrato esteja beneficiando demais alguma parte, se há algo errado com alguma cláusula, vírgulas erradas em números etc., isso pode causar problemas para a empresa.

POLÍTICA DE RESPOSTA A INCIDENTES

Conceito: O Plano de Resposta a Incidentes de Segurança e Privacidade é essencialmente um processo. Descreve, em um documento acessível, a forma como a empresa vai responder às emergências e incidentes, de forma rápida. Na definição do art. 46 da LGPD, incidente de segurança de dados pessoais pode ser compreendido como quaisquer acessos não autorizados a tais informações, situações acidentais ou ilícitas que resultem na destruição, perda, alteração, comunicação dessas, ou, ainda, qualquer forma de tratamento desses mesmos dados de forma inadequada ou ilícita.

Principais entregas em relação ao documento:

- Formação do time de resgate a incidentes (TRI), geralmente é o TI, acompanhado da equipe de jurídico, de um encarregado de dados, de alguém da área de segurança ou de riscos etc. O TRI deve ter reuniões periódicas para definir melhorias neste plano, necessidades de preparo, treinamento do resto do time etc. O TRI deve documentar o incidente, e conduzir uma reunião de Lições Aprendidas.
- Já foi delimitado um time para responder, meios de comunicação e de alarmes eficientes, salvaguardas e mecanismos de controle para proteção de recursos da empresa?
- Haverá algum apoio externo, seja para responder aos incidentes, seja para compor o TRI?
- As autoridades competentes são acionadas? Os titulares dos dados são informados? Como e quando?
- Há um Plano de Resposta à Incidentes documentado e acessível, para que possa ser seguido à risca?
- Etapas do Plano de Resposta a Incidentes: Preparação de equipe, políticas e ferramentas; Identificação do incidente; Contenção do incidente; Erradicação da ameaça e restauração dos sistemas afetados; Recuperação dos sistemas; Lições aprendidas.
- Há algum plano de simulação de incidente de segurança (SIS)? A proposta é que a organização simule um episódio de incidente de segurança de dados pessoais, a fim de verificar se a programação de resposta (se ela for existente) é executada com a velocidade adequada;
- Há um mapeamento de riscos após o incidente? Vistorias/auditorias para identificar vulnerabilidades pós incidente?

Eventuais modelos (Ctrl+clique para ir até a página):

- StoneX
- UFRGS
- Secretaria da Educação de PE (bem completo)

POLÍTICA DE GOVERNANÇA DE DADOS, INFORMAÇÃO E CONHECIMENTO

Conceito: Gestão ou governança de dados é a gestão de políticas, processos, pessoas e tecnologias, de forma a estruturar os ativos de informação (dado/informação/conhecimento a que esteja associado um valor) dentro da organização.

Principais entregas em relação ao documento:

- Como é um conjunto de processos, pessoas, tecnologias e políticas, a governança de dados pode ser estruturada pela empresa, e passada para os titulares através de documentos de informações, como a política de privacidade. Nessa política, devem estar definidos os princípios que uma organização deve adotar, assim como as diretrizes, responsabilidades e como a estrutura organizacional irá conduzir e monitorar a governança;
- A governança de dados é digital? Os dados podem ser encontrados e validados de forma eficiente e prática?
- Como ocorre o armazenamento, acessos, permissões e eliminação dos dados? Como é a segurança dos dados, e quem está encarregado e/ou responsável por qualquer eventual problema? Como é o Plano de Resposta a Incidentes? Está documentado? Como posso encontrá-lo? Serei avisado? Quais são os meus direitos de titular? Onde posso encontrar esses documentos?
- Informações sobre o consentimento, descarte dos dados, solicitações de revisão interna do tratamento de dado;
- Há tratamento de dados de menores? Cuidado especial.

Eventuais modelos (Ctrl+clique para ir até a página):

- Embrapa (bem completo)
- FVA Sociedade de Advogados

POLÍTICA DE SEGURANÇA DE INFORMAÇÕES E SIGILO DE DADOS

Conceito: Uma boa PSI deve conter regras e diretrizes que orientem os colaboradores, clientes e fornecedores, com relação aos padrões de comportamento ligados à segurança da informação, condições de instalações de equipamentos, restrições de acesso, mecanismos de proteção, monitoramento e controle, entre outros cuidados imprescindíveis aos processos de negócio. O objetivo é preservar as informações quanto à integridade, confidencialidade e disponibilidade. Deve ser solidificada com base nas recomendações propostas pela norma ABNT NBR ISO/IEC 27001:2005, bem como estar em sintonia com a legislação do país.

Principais entregas em relação ao documento:

- Responsabilidade dos colaboradores? Responsabilidade da área de TI?
- Informações ligadas à logística da implementação da TI na organização;
- Há níveis de acesso e permissões? Regras de senha e credenciais de acesso para criar um login forte? Há algum comitê de segurança/riscos ou encarregado? Quais normas de mercado são utilizadas? Há uso/rastreio de logs? Há criptografia? Há sistema de recuperação e backup? Há um monitoramento periódico dos seus hardwares, softwares e rede?
- Todos os colaboradores participam da elaboração dessa política? Essa política é comunicada e disponível para todos?
- Tecnologias de defesa contra ciber-ataques; como ocorre a política de atualização de softwares? Existem planos de contingência e de gerenciamento de riscos? Existem modelos de classificação de ameaças?
- Há alguma política de treinamento aos colaboradores? Reuniões são realizadas periodicamente para revisar os planos e atividades de segurança? O setor de TI fica atento para novas tecnologias?
- Existem penalidades caso ocorra a violação dessa política?

Eventuais modelos (Ctrl+clique para ir até a página):

- Intelipost
- Iphan – Instituto do Patrimônio Histórico e Artístico (bem completo)
- Dnocs -Departamento Nacional de Obras Contra a Seca

ceon

PROCEDIMENTO DE ATENDIMENTO À REQUISIÇÕES DE TITULARES

Conceito: É essencial saber reconhecer se a solicitação feita pelo titular de dados se aplica com base na Lei vigente e quando ela pode ser recusada, bem como ter um plano estruturado para responder às solicitações, reclamações e retificações. A empresa deverá decidir como operacionalizar o cumprimento das solicitações de direitos dos titulares.

Principais entregas em relação ao documento:

- Quem são os titulares dos dados? Quais são os seus direitos? (Política de Direito dos Titulares);
- Existe um canal para registro das solicitações dos titulares? Esse canal é amplamente divulgado e de fácil acesso?
- Há situações em que se possa recusar a solicitação? Qual situação? Onde está o documento?
- É preciso revelar a identidade do solicitante, para que não dê respostas de outro titular.
- Há um gerenciamento do tempo de pergunta e resposta? Há registro de quem respondeu à pergunta? Há alguém responsável pelo setor? Há treinamento desse(s) responsável(eis)? Há um modo de comprovar as respostas já respondidas?
    - Pela LGPD, você tem até 15 dias para retornar a DSAR (requisição de acesso aos dados do titular) – qualquer cliente, ou até funcionário, pode pedir uma DSAR.
- Há ferramentas que ajudem na segurança dessas informações e que facilitem a operação de resposta? Há um fluxo organizado, com padrão de respostas e que permita o exercício de direitos?
- Há muita demanda de pedido/pergunta? A equipe consegue dar conta? Há alguma solução para isso?
- É preciso registrar todo esse processo, para evitar problemas futuros.
- Em resumo, para garantir a resposta aos direitos dos titulares, três grandes pilares devem ser observados: jurídico (é valida a solicitação?); operacional (local e gerenciamento de solicitações); e tecnológico (Solução da solicitação).

Eventuais modelos (Ctrl+clique para ir até a página):

- Braspag (parcialmente completo)
- Opice Blum Academy (educativo/o que é)

REGISTRO DAS OPERAÇÕES DE TRATAMENTO DE DADOS (ROPA)

Conceito: O ROPA, nada mais é do que o registro de todas as operações que envolvam dados pessoais, devendo ser realizado por controladores e operadores (art. 37 LGPD), especialmente quando a base legal do tratamento for o legítimo interesse. O ROPA (Record of Processing Activities) é mencionado no artigo 30 do GDPR (General Data Protection Regulation), sendo fundamental a sua elaboração e é o primeiro passo para adequação à LGPD.

O documento pode estar incluso na Política de Privacidade e Proteção de dados.

Principais entregas em relação ao documento:

- Prova de que mantêm registros das operações de tratamentos dos dados pessoais que realizam, desde a coleta até a exclusão, onde deverão estar indicados: A descrição das categorias dos dados e dos titulares; O fluxo dos dados para fora da organização; a finalidade; o tempo em que os dados são retidos pela empresa, os dados do controlador e os recursos e mecanismos de segurança empregados.
- Existem penalidades caso ocorra a violação dessa política?
- Há um registro das operações desde a coleta de dados até a exclusão desses? Como é feita?
- Há esse registro em TODAS as áreas da empresa?
- Geralmente, vem acompanhado do RIPD – Relatório de Impacto à Proteção de Dados Pessoais, que abrange o levantamento dos riscos presentes no tratamento dos dados e dos meios empregados para minimizá-los. O relatório deve incluir, ainda, justificativa para a coleta de dados sensíveis.

Eventuais modelos (Ctrl+clique para ir até a página):

- COVAC

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS (RIPD OU DPIA)

Conceito: Geralmente, acompanha o ROPA. Segundo o artigo 5º e 38 da LGPD, é a documentação do controlador, que é o responsável, que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco. Uma vez que tem como intuito a mitigação de riscos, o RIPD deve ser feito antes de serem iniciadas as atividades de tratamento.

Principais entregas em relação ao documento:

- Há a descrição dos tipos de dados coletados e a metodologia utilizada? Há métodos para garantir a segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados? Há planos de prevenção de eventuais danos em função do procedimento feito?
- Quando é necessário o RIPD?
    - Quando o tratamento de dados pessoais tiver como fundamento o interesse legítimo do Controlador (Art 10 LGPD);
    - Quando o tratamento de dados pessoais gerar riscos às liberdades civis e aos direitos fundamentais dos titulares dos dados (Art 5 LGPD);
    - Quando ocorrer o tratamento de dados pessoais sensíveis, especialmente em grandes volumes (art 38 LGPD);
    - Quando o tratamento for relativo a dados pessoais provenientes de território internacional e que não sejam objeto de comunicação, no uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência (art 4 LGPD);
- Nós temos uma abordagem parecida de compreender e reduzir os riscos envolvidos no tratamento a um nível aceitável, que é a matriz de riscos.



Eventuais modelos (Ctrl+clique para ir até a página):

- BACEN
- Dep. Seg. Pública
- JovensGênios

IMPLANTAÇÃO DE PRIVACY BY DESIGNER

Conceito: É a metodologia de privacidade e proteção de dados desde o design (ou desde o desenvolvimento do software), para que seja poupado trabalho futuro. A técnica prevê que todas as etapas do desenvolvimento de sistemas, produtos ou serviços coloquem a privacidade do usuário e a proteção de dados pessoais em primeiro lugar. A ideia é que a segurança dos dados seja um eixo central, e não apenas um complemento. (art 46 e 47 LGPD)

Principais entregas em relação ao documento:

- Há treinamento da equipe em relação a esse documento? Os requisitos/exigências para o tratamento de dados estão documentados (finalidade, encarregado...)? São realizados testes para prevenir problemas? Há manutenção dos sistemas/software periodicamente? Há funcionalidade total (soma-positiva e não soma-zero)?
- Alta gerência, TI e cybersecurity são as áreas da empresa responsáveis por isso;
- Como a privacidade é importante e gera confiança, toda a marca deve apresentar sinais que está levando a boas práticas de privacidade e segurança.
- Sempre deixar o usuário confortável que a sua empresa está cuidando o máximo possível dos dados, mostrando a ele como o software funciona, sistemas de segurança, etc.
- Ser proativo, e não reativo (sempre tentar prever o que pode acontecer e estar a frente de eventuais problemas); lema de segurança de ponta a ponta; sempre transparente com dados;
- Uma possibilidade é apresentar artes no início da estruturação que demonstrem o armazenamento de dados pessoais no próprio dispositivo do usuário, com compartilhamento apenas de dados estatísticos que irão compor um banco de dados anonimizados, bem como outros documentos técnicos e de design da solução que destaquem quaisquer outras medidas de minimização do tratamento de dados pessoais ou dos riscos à privacidade. Também pode ser feito mediante a apresentação dos registros da persona e do mapa da empatia com aspectos de privacidade

Eventuais modelos (Ctrl+clique para ir até a página):

- Modelo