CARTILHA SOBRE

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS - LEI 13.709/2018 (LGPD) E SEGURANÇA DA INFORMAÇÃO

wep compliance

Basso Pancotte

Variedade . Agilidade . Inovação

A **Basso & Pancotte Ltda. / Intersul** está em processo de adequação à Lei Geral de Proteção de Dados - LGPD (Lei 13.709/2018).

Qualquer dúvida sobre tratamento de dados pessoais, o nosso Encarregado de Dados é: Guilherme Salla

Telefone: (54) 9 9691-4645
E-mail: privacidade@baspan.com.br

wep compliance

VOCÊ JÁ OUVIU FALAR NA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS - LGPD?

A Lei entrou em vigor em 18 de setembro de 2020 e representa uma mudança considerável na utilização de **DADOS PESSOAIS** (nome, endereço, CPF, RG, etc.), permitindo que você, Titular, tenha maior controle, proteção e privacidade sobre a forma de utilização de seus dados, além de estabelecer para as organizações, diretrizes importantes e obrigatórias para a coleta, processamento e armazenamento de dados pessoais.

POR QUE A ORGANIZAÇÃO PRECISA SE ADEQUAR?

- Transparência sobre a coleta e utilização de dados
- Exigência legal
- Atenção com funcionários, clientes e fornecedores
- Aumento da credibilidade e confiança na imagem da organização
- Valorização perante a concorrência
- Redução do risco de vazamento, violação e exposição de dados
- Proteção da organização quanto a sanções administrativas

QUAIS SÃO OS DIREITOS DOS TITULARES DE DADOS?

Os Titulares têm direito ao acesso facilitado às informações sobre o tratamento de seus dados pessoais, que deverão ser disponibilizados de forma clara e acessível, mediante solicitação prévia*:

- Confirmação de tratamento e sua finalidade
- Acesso facilitado aos dados
- Correção dos dados
- Anonimização e bloqueio
- Portabilidade
- Retificação, Atualização e Eliminação
- Informações de compartilhamento
- Informações sobre o não consentimento
- Revogação do consentimento
- Reclamação para a Autoridade Nacional de Proteção de Dados - ANPD
- Revisão de decisões automatizadas

* Atendimento à solicitação mediante prévia análise e nos prazos legais.

Observação: Alguns desses direitos ainda precisam ser regulamentados pela Autoridade Nacional de Proteção de Dados – ANPD.

PRINCIPAIS ENVOLVIDOS NA OPERAÇÃO DE TRATAMENTO DE DADOS

Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador;

Encarregado/DPO (Data Protection Officer): pessoa indicada pelo Controlador e Operador para atuar como canal de comunicação entre o Controlador, os Titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

Agentes de Tratamento: O Controlador e o Operador;

Autoridade Nacional de Proteção de Dados (ANPD): órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

BASES LEGAIS PARA TRATAMENTO DE DADOS

São hipóteses que autorizam o tratamento de dados pessoais (permitem que sejam usados dados pessoais):

- CONSENTIMENTO DO TITULAR
- CUMPRIMENTO DE OBRIGAÇÃO LEGAL
- POLÍTICAS PÚBLICAS
- PESQUISA
- EXECUÇÃO DE CONTRATO
- EXERCÍCIO REGULAR DE DIREITOS
- PROTEÇÃO DA VIDA
- TUTELA DA SAÚDE
- LEGÍTIMO INTERESSE
- PROTEÇÃO AO CRÉDITO

GUIA DE SEGURANÇA DA INFORMAÇÃO

Com a vigência da LGPD as organizações terão uma mudança significativa no que diz respeito à segurança dos dados pessoais tratados como, por exemplo, na coleta, armazenamento, utilização e compartilhamento de dados pessoais. Para que o tratamento de dados ocorra de forma adequada é importante que todos fiquem atentos às suas responsabilidades.

Pensando nisso, selecionamos algumas recomendações importantes para você:

1. Evite posts sobre o seu ambiente de trabalho, telas de computadores ou mesmo da mesa de trabalho

Embora isso pareça uma questão de baixa relevância, tais imagens **podem revelar** dados em documentos, telas, gráficos, credenciais de usuários e dados sensíveis da organização.

Também pode expor seus colegas de trabalho.

2. Manuseie os documentos físicos com atenção

O bom funcionamento de qualquer negócio tem por base o correto manuseio de informações. É essencial ter cautela no manuseio dos documentos físicos pois a desorganização pode acarretar riscos.

A **LGPD não trata apenas os dados virtuais.** O cuidado se estende àquele papel deixado na impressora, sobre a sua mesa, nas notas adesivas e até sobre o papel que você utiliza como rascunho. A segurança da informação deve acontecer nos meios online e offline (virtual e físico).

3. Utilize o bloqueio de acesso aos dispositivos móveis

É importante lembrar que a senha é algo pessoal e que não deve ser compartilhada, exposta ou salva automaticamente em seus dispositivos móveis. Atente-se para as alterações periódicas, conforme Política da organização.

Deixe **o seu dispositivo** sempre **bloqueado** enquanto não estiver em uso e, para liberá-lo, utilize senhas fortes, padrões não triviais ou biometria. Lembre-se de fazer *logoff* toda vez que deixar de usar um aplicativo ou site.

Por estar sempre ao nosso alcance, temos a sensação de que nada irá acontecer com os nossos dispositivos móveis e que estamos seguros. Temos que considerar, contudo, que eles estão sujeitos a extravio, roubo, ou ainda, **acessos não autorizados.**

4. Mantenha a confidencialidade, integridade, disponibilidade, autenticidade e legalidade das informações

- Jamais forneça quaisquer dados para desconhecidos, pois há chance de ser golpe.
- Proteja as informações para que se mantenham em seu estado original, ou seja, contra alterações indevidas ou mesmo acidentais.
- Evite armazenar os dados da organização em um *pendrive*.
- Mantenha a atenção com os registros de conversas, pois podem ficar armazenados.

Zele pela sua imagem e reputação pessoal e da sua organização.

GUIA DE SEGURANÇA DA INFORMAÇÃO

Computadores e celulares pessoais não devem armazenar dados corporativos;

É importante que você possua um histórico dos serviços realizados em seus dispositivos ou mídias de armazenamento. Isso permite que atos intencionais ou não intencionais possam ser rastreados, mesmo que para identificar a ocorrência legítima de um procedimento.

5. Aplique autenticação em dois-fatores

Os grandes nomes das redes sociais como Google, Facebook, Twitter, LinkedIn, já incentivam a política de autenticação em dois-fatores, **incorporando uma camada adicional de segurança** em suas contas, como por exemplo, uso do cartão bancário seguido de um código PIN.

Use sempre que possível.

6. Evite utilizar redes abertas e desprotegidas

Não se conecte em contas corporativas a partir de redes abertas que não implementam protocolos de segurança pois as suas credenciais (login e senha) e demais dados podem ser interceptados. Isso vale para *home banking* e demais aplicativos.

Está em dúvida sobre o **conteúdo de um site?**

Pode **ser um site malicioso?**

Busque informações sobre o mesmo e, persistindo dúvidas, não acesse nenhum serviço, não faça *download* e saia imediatamente da página.

7. O seu "clique" pode ser o ponto de partida de um incidente

O seu "clique", "toque com o dedo" ou "tecla enter" podem permitir **acessos indevidos** aos seus dispositivos, fazer *download* de arquivos ou *softwares* maliciosos, direcioná-los a sites maliciosos, expor dados pessoais e profissionais sensíveis.

PORTANTO, TENHA CUIDADO!

FICOU COM ALGUMA DÚVIDA?

Entre em contato com seu Superior ou com o Encarregado de Dados Pessoais de sua organização através dos canais disponíveis.

CONTAMOS COM O APOIO DE TODOS!!

contato@wepcompliance.com.br
Rua Emílio Abichequer, 37, Sala 102 . São Cristóvão | Lajeado - RS

WEPcompliance wepcompliance wepcompliance