Guia de Boas Práticas Segurança de Dados - LGPD

Olá, servidor!

Nesta cartilha você encontrará algumas dicas de condutas preventivas que irão tornar o ambiente de trabalho mais seguro, seguindo as diretrizes da Lei Geral de Proteção de Dados - LGPD (Lei 13.709/18).

O que é LGPD?

A Lei Geral de Proteção de Dados Pessoais (LGPD) é a legislação brasileira que regula as atividades de tratamento de dados pessoais para fins comerciais.

O que é dado pessoal?

Informação relacionada a pessoa natural identificada ou identificável.

O que é dado pessoal sensível?

Dados pessoais de crianças, adolescentes e que podem gerar discriminação: origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico.

O que NÃO é dado pessoal?

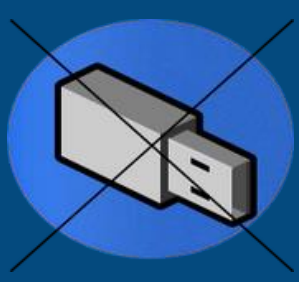
Não é considerado dado pessoal e não incidirá à LGPD:

1. Utilização do dado para fins particulares e não econômicos;
2. Utilização dos dados para fins exclusivamente jornalísticos e artísticos ou acadêmicos;
3. Utilização do dado pessoal para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação repressão de crimes;
4. Dados anonimizados; e
5. Os dados tornados públicos pelos próprios titulares.

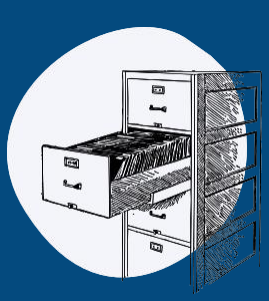
Boas Práticas

1. Colete apenas os dados necessários ao desempenho de sua atividade e do escopo da Prefeitura de Erechim.

2. Tenha conhecimentos das políticas que se refiram a dados pessoais.



3.Evite fazer cópias de arquivos com dados pessoais que são tratados pela Prefeitura de Erechim para dispositivos de armazenamento externo (Ex: *pendrive*, HD) .



4.Não deixe sob a mesa de trabalho suas senhas ou documentos contendo dados de pessoas físicas. Utilize pastas opacas e gavetas com chaves para guardar desses documentos.

5. Evite realizar sua atividade de seu dispositivo móvel particular caso você tenha um dispositivo profissional.

6.Não compartilhe sua senha. Ela é pessoal, intransferível e está sob a sua responsabilidade. Evite senhas fáceis, como nomes, datas de aniversário, placa de automóvel, número de telefone, etc.

- Troque suas senhas a cada 6 meses;
- Evite usar as mesmas senhas para seus acessos;
- Utilize gerenciador de senhas.

7.Bloqueie a tela de seu computador sempre que se ausentar da sua estação de trabalho. Ex: idas ao toalete, cafezinho, conversar com o colega, etc.

8.Ao abrir e-mails, tome cuidado: não abra e-mails de desconhecidos e não baixe arquivos duvidosos. Se estiver em dúvida, apague-os.

- Evite passar dados pessoais seus e de seus colegas por telefone.
- Verifique com seu gestor quais os procedimentos para essa atividade

Direitos dos Titulares de dados

CONFIRMAÇÃO
de que existe um ou mais tratamento de dados sendo realizado.

ACESSO
aos dados pessoais conservados que lhe digam respeito.

CORREÇÃO
de dados pessoais incompletos, inexatos ou desatualizado.

ELIMINAÇÃO
de dados (exceto quando o tratamento é legal, mesmo que sem o consentimento do titular).

PORTABILIDADE
de dados a outro fornecedor de serviço ou produto, observados os segredos comercial e industrial.

OPOSIÇÃO
caso discorde de um tratamento feito sem o seu consentimento.

RECLAMAÇÃO
contra o controlador dos dados junto à autoridade nacional.

REVOGAÇÃO
do consentimento, nos termos da lei.

INFORMAÇÃO SOBRE O NÃO CONSENTIMENTO
de dados (exceto quando o tratamento é legal, mesmo que sem o consentimento do titular).

INFORMAÇÃO SOBRE COMPARTILHAMENTO
de seus dados com entes públicos e privados, caso exista.

ANONIMIZAÇÃO, BLOQUEIO OU ELIMINAÇÃO
de dados desnecessários excessivos ou tratados em desconformidade com a Lei.

Incidente de Segurança Da Informação

Um incidente de segurança da informação é qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação na segurança de informações contendo dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais.

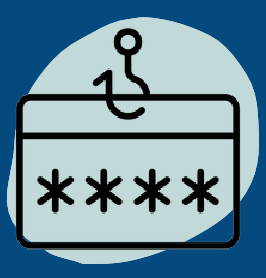
- *São exemplos práticos de incidentes de segurança da informação*

VAZAMENTO DE DADOS PESSOAIS:
quando dados são indevidamente acessados, coletados e divulgados ou repassados a terceiros;

INVASÃO
nos sistemas de segurança;

ENCAMINHAMENTO OU COMPARTILHAMENTO
errôneo/equivocado de mensagens contendo dados pessoais;

OBSERVAÇÕES OU SUSPEITAS
de fragilidade em sistemas ou serviços;



ACESSO INDEVIDO AOS DADOS
contidos em documentos ou sistemas informáticos;

VIOLAÇÕES
de procedimentos de segurança e de acesso.

Não esqueça:

Sua colaboração é essencial.

O que você pode fazer para ajudar a evitar um incidente de dados

- DESCONFIE se o seu computador da Prefeitura de Erechim estiver lento, inacessível ou você notar alguma atividade estranha ao utilizá-lo.
- MANTENHA seus dispositivos com as atualizações de segurança do sistema operacional em dia.
- EVITE usar seus dispositivos pessoais ou de armazenamento em nuvem particular para uso profissional.
- NÃO UTILIZE *softwares* gratuitos ou pagos desconhecidos ou não autorizados.
- PARTICIPE dos treinamentos oferecidos pela administração pública
- ESTEJA ATUALIZADO quanto ao código de ética e regras de segurança da informação da Prefeitura de Erechim.
- ESCLAREÇA SUAS DÚVIDAS sobre proteção de dados com o encarregado de dados nomeado.
- EVITE responder solicitações de titulares de dados caso essa não seja a sua função encaminhando eventual requerimento ao setor competente de acordo com o regramento interno da Prefeitura de Erechim ou ao DPO nomeado.
- CONTATE IMEDIATAMENTE a TI da Prefeitura em qualquer situação de dúvida ou atividade estranha em seus dispositivos institucionais.

Grupo MACIEL