CRCMG
CONSELHO REGIONAL DE CONTABILIDADE DE MINAS GERAIS

Aplicando a LGPD

CRCMG
CONSELHO REGIONAL DE CONTABILIDADE DE MINAS GERAIS

ALEXANDRE NEVES
alliance@alterdata.com.br

A palestra é o "start" do processo de informação para as empresas.

Foco didático Não haverá foco jurídico.

O QUE É A LGPD ?

(Lei Geral de Proteção de Dados)

É a regulamentação para os negócios usarem os dados de pessoas físicas, de acordo com o que foi combinado com os titulares.

15/08/2018 LEI No 13.709, DE 14 DE AGOSTO DE 2018 - Diário Oficial da União - Imprensa Nacional

DIÁRIO OFICIAL DA UNIÃO

Publicado em: 15/08/2018 | Edição: 157 | Seção: 1 | Página: 59
Órgão: Atos do Poder Legislativo

LEI NO 13.709, DE 14 DE AGOSTO DE 2018

Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).

O PRESIDENTE DA REPÚBLICA

Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:

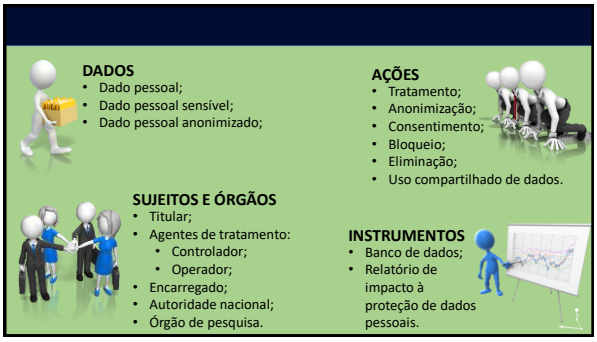
I - o respeito à privacidade;

Como saber se eu me enquadro nessa obrigação ?

Se você responder SIM a pelo menos um item a seguir, sua empresa já está dentro da nova regulamentação e precisa se preparar para as exigências de forma eficiente e sustentável:

1. Coletam dados de clientes para negócios ou envio de ações promocionais ?
2. Coletam dados através de site e aplicativos para vender produtos ou serviços?
3. Analisam comportamento dos clientes para sugerir conteúdo específico?
4. Mantém dados de colaboradores e utiliza para pagamentos de salários?
5. Terceiriza a coleta, armazenamento e/ou tratamento de dados pessoais?

A LGPD vale pra todo mundo: empresas grandes ou pequenas, digitais ou não.



Dado pessoal

qualquer informação relacionada a pessoa natural identificada ou identificável

Dado pessoal sensível

"dado pessoal sobre a intimidade do titular:

. origem racial ou étnica
. convicção religiosa
. opinião política
. filiação a sindicato ou
. organização religiosa
. filosófica ou política
. dado referente à saúde ou
. vida sexual
. dado genético ou biométrico
quando vinculado a uma pessoa natural"

Dado anonimizado

dado relativo a titular que **não possa ser identificado**, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento

> CPF : 918*318*424*00_

Outra forma de **supressão de valores identificáveis** é a utilização de técnicas de **generalização**.

> Idade: etários 18-24 anos

não sofrem a aplicação da LGPD

A lei detalha os papéis de quatro diferentes agentes:

Como fica a Relação contratual de sistemas Web/Nuvem ?

CLIENTE CONTROLADOR NO INPUT DAS INFORMAÇÕES

FORNECEDOR SERÁ O CONTROLADOR NO FORNECIMENTO DE SERVIÇOS DE WEB/NUVEM, POIS ELE DEFINE OS MEIOS DE PROCESSAMENTO E É RESPONSÁVEL PELAS IMPLEMENTAÇÕES DAS MEDIDAS DE SEGURANÇA

Passo 1:

COMITÊ INTERNO

A **ANPD** poderá receber denuncias de concorrentes e acionar fiscalização.

Por isso crie um **Comitê interno** para analisar impacto da LGPD na empresa, categorizando os dados (normal, sensível, critico).

Destacar uma pessoa que fique responsável por estudar a LGPD e seus desdobramentos. Pode ser um colaborador ou uma empresa terceirizada. Será conhecido como "Encarregado" ou "Data Protection Officer (DPO)".

Pequenas empresas devem contratar Encarregados ?

Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.

§ 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive **hipóteses de dispensa** da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

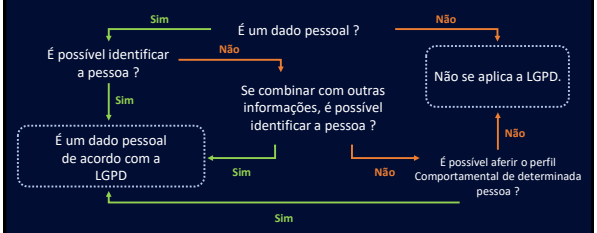
Passo 2:

Sua empresa capta dados de outras pessoas ?

RG, CPF, Endereço, Data de Nascimento, qualquer informação sobre uma pessoa, até mesmo seus gostos, hábitos, localização geográfica

Prova dos "9":
se você usar essa informação, chega ao cliente dono da informação ?

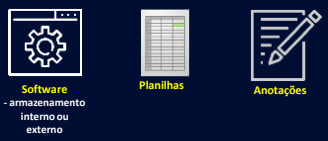
DADO LOCALIZADO



Passo 3:

Localizar o lugar(es) ou maneira(s) como estes dados são armazenados

Onde as informações dos clientes são guardadas ?



Passo 4:

Mapear os dados armazenados
(data mapping – inventário de dados)

ATENÇÃO: O mapeamento de dados devem refletir o caminho percorrido pelo dado pessoal dentro da empresa, incluindo os processos e procedimentos pelos quais o dado transita.

Ou seja, qual a origem (como foi capturado?), a **base legal** que respalda o tratamento deste dado pessoal ?

Quais são os principais objetivos do mapeamento de dados?

Um dos principais objetivos é diagnosticar a forma como a empresa lida com a privacidade e a segurança da informação de seus clientes, colaboradores e parceiros terceirizados.

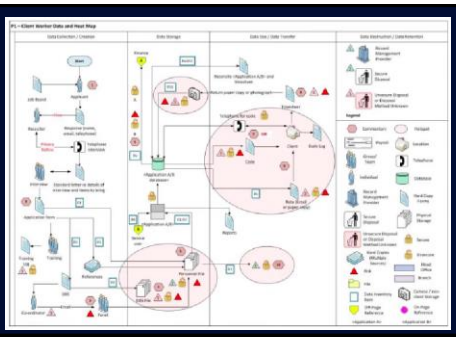
Cumprindo assim, a exigência constante no art. 37 da LGPD onde estipula que o controlador e o operador devem **manter registro** das operações de tratamento de dados pessoais que realizarem.

Apesar de existir no mercado **softwares muito úteis** para o mapeamento, o processo é abrangente e requer uma análise humana mais profunda. Os **dados físicos também precisam ser mapeados,** sendo um dos pontos com dificuldades em algumas ferramentas.

E o resultado do mapeamento de dados?

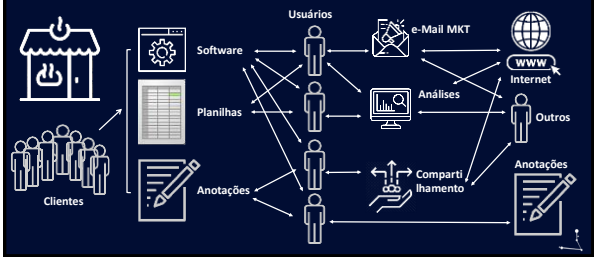
Com as informações coletadas é possível termos a dimensão de todos os dados que a empresa trata, gerando um fluxo dos dados.

Essa informação será utilizada para a elaboração de **documentos** como:
. Relatório de impacto de proteção de dados
. Política de gestão de crises
. Manual de procedimentos e controles internos em proteção de dados e outros que forem necessários



Exercício guiado - simplificado

Uma empresa resolve fazer mapeamento dos dados



Exemplo de Mapeamento de Dados

Disponibilizado nos slides

Passo 5:

Sua empresa guarda os dados dos clientes apenas pelo tempo necessário para cumprir o objetivo informado, ou deixa no cadastro sem prazo ?

Esses dados agora só podem ser guardados apenas pelo tempo que for preciso para cumprir as finalidades combinadas com o cliente, na época da coleta.

Passo 6:

A lei exige que a empresa possa **rastrear** como os dados das pessoas são utilizados, quem os utiliza, para qual propósito e por quanto tempo.

O mapeamento de dados ajudará fortemente nesse processo.

Ainda haverá:
. demanda tanto sistemas, quanto de TI
. treinamento de equipe
. criação de métodos de auditoria

Demanda de sistemas:

- Manter seu(s) software(s) atualizado(s);
- Aprender a correta utilização dos novos recursos;
- Estimular diariamente a adaptação da equipe (evitar choque cultural e usar **processo de comunicação adequado**);

Demanda de TI

- Verificar se essa equipe conhece a LGPD. Caso negativo, teremos uma conferência sobre o assunto (https://alterdata.software/conferencia_alliance) ;

- Apurar segurança dos dados nos meios digitais, como sites, e-mails, bancos de dados (criptografia), rede interna e internet;

- Apurar quais as camadas de segurança contra vazamento de dados e o último teste de invasão;

Demanda de TI – dicas para ler depois

Segurança da informação nunca possui uma fórmula pronta, e sempre é importante **entender o contexto da sua empresa e de suas atividades**. Mas algumas dicas podem ser valiosas para toda e qualquer empresa:

- **bloqueie os computadores** quando estiver fora de seu ambiente de trabalho;
- **utilize senhas** em seus computadores e celulares de trabalho, guardando-as em sigilo e alterando-as periodicamente;
- tenha um **controle** de quem acessa as informações nos seus sistemas, quando estas são acessadas, definindo responsabilidades e privilégios de acesso. Ou seja, **quem pode acessar** o que e quando pode acessar;
- quando estiver trabalhando fora da empresa, **fique atento ao seu redor**: certifique-se de que o objeto do seu trabalho não esteja visível a outras pessoas e tome cuidado ao falar nomes de clientes, colaboradores e sobre casos específicos;
- **descarte documentos confidenciais** em papel utilizando um triturador ou rasgando-os em pequenos pedaços; • **tome cuidado ao abrir e-mails e seus anexos**, principalmente de desconhecidos;
- certifique-se de que documentos físicos que contenham dados pessoais estejam armazenados em **locais seguros** (gavetas com chaves e cadeados, por exemplo);
- **registre a identificação dos visitantes** de entrada e saída do seu estabelecimento, acompanhando-os sempre que forem transitar em áreas reservadas aos colaboradores da empresa;
- utilize **criptografia** em todos os computadores, celulares e tablets;
- somente utilize **redes Wi-Fi seguras** e confiáveis;
- **limite o acesso** aos dados pessoais àqueles que realmente precisem tê-lo; e
- diminua o **fluxo de documentos de papel** levados para fora de seu estabelecimento.

Proteste - LGPD para pme

Atenção:

O fato de alguém ser funcionário, não dá direito automático ao acesso e uso dos dados da maneira que desejar.

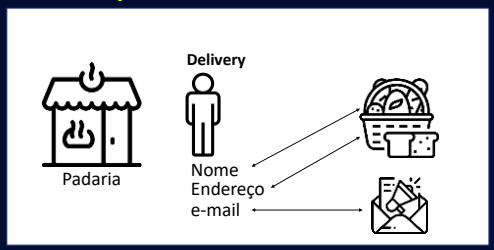
Passo 7:

Sem base legal, você não pode utilizar dados pessoais. Quais as bases legais que a empresa usa para coleta, armazenamento e tratamento de dados ?

- Os dados armazenados atendem apenas essas bases legais ou existem dados excessivos ?

- Nos dados excessivos, sua empresa preparará termos de consentimento ou vão excluir as informações ?

Cenário exemplo de dados excessivos



CADASTRO PARA ADMISSÃO DE COLABORADORES

DADOS PESSOAIS – PREENCHER TODAS AS QUESTÕES		
Nome Completo:		Data de hoje: ____/____/____
Nome do Pai:		Nome da Mãe:
CPF:	RG:	Estado onde tirou RG:
Telefone fixo:	Celular:	
Data Nascimento:	Idade:	Local onde nasceu:
Endereço:		Bairro:
Escolaridade:	No momento estuda?	
Cursos realizados:		
Estado Civil:		
Filhos menores de 14 anos?	Idade:	
Religião:	Freqüenta igreja:	
Qual(is) área(s) de interesse? ( )Açougue ( )Padaria ( )Embalador ( )Reposição ( )Caixa ( )Administrativo ( ) Limpeza Outra:		
Possui algum conhecido no [redacted]? _____ ( ) Parentes ( ) Amigos Nome e setor onde trabalha:		
ENTREVISTA		

- no momento da coleta dos dados, é obrigatória a explicação às pessoas, quais as informações são **realmente necessárias** e quais são opcionais;

- agora é preciso **revisar** os dados pessoais que a empresa coleta e armazena, decidir quais realmente devem ser tratados e mantidos e quais não são necessários;

- avaliar para os desnecessários, destruir de maneira segura (informando aos titulares) ou coletar consentimento;

Você precisa ter sua consultoria jurídica próxima de você para analisar a realidade do seu negócio e verificar os procedimentos mais adequados.

Lembre-se do papel do controlador.

A mais conhecida das bases legais é o **consentimento,** que reflete a autorização do indivíduo para que você possa tratar seus dados pessoais.

Portanto será sempre necessário buscar a base legal mais adequada para autorizar o uso dos dados pessoais

QUAIS SÃO AS INFORMAÇÕES OBRIGATÓRIAS DOS TERMOS DE CONSENTIMENTO DO USUÁRIO?

- Qual a finalidade específica do tratamento ?
- Com quem os dados serão compartilhados ?
- Qual o período de duração do tratamento ?
- Possibilidade de não consentimento e quais as consequências da negativa.
- consistir em **manifestação livre** (verdadeira escolha, decisão voluntária), **informada** (informação completa, exata, disponibilizada de forma clara e compreensível) **e inequívoca** (não pode dar margem à dúvida quanto à intenção da pessoa em dar o seu consentimento).

http://consentimentousuario.com.br

TERMOS DE CONSENTIMENTO DO USUÁRIO

O termo a seguir autoriza a empresa Drogaria XYZ a usar os meus dados pessoais, sendo:

Para fins de concessão de desconto de 15% nas compras — Finalidade do tratamento

Dados compartilhados
[ ] Nome completo _____
[ ] CPF _____
[ ] email _____

Duração tratamento
A utilização dos dados será por um prazo de 72 horas, sendo:
[ ] 05s – concessão de desconto de 15%
[ ] 72h – análise cadastral para composição de mala direta promoções digitais

- *Campos não marcados (não preenchidos) serão descartados e desconto não será aplicado no valor total das compras.* — Consequência não aprovação

Confirmo meu desejo de compartilhamento dos dados acima, para concessão de desconto nas compras realizadas dia ***31/02/2020*** às ***14:11*** , o qual abaixo digito CONFIRMO por extenso:

_____ — Manifestação livre, informada e inequívoca

http://consentimentousuario.com.br

TERMOS DE CONSENTIMENTO DO USUÁRIO

Nome: José Jorge Augusto Prado
CPF: 145.245.345-15
Email: jjprado@email.com.br

☑ Autorizo a Drogaria XYZ a me liberar desconto de 15% no total das compras

OK

Fora do padrão

Registre o consentimento

Assim como você guarda recibos e contratos assinados, vai ser preciso também registrar **quando**, **para que** e **como** o titular consentiu (por exemplo, e-mail, telefone, formulário de cadastro etc.), sob o risco de o consentimento não poder ser utilizado como meio de prova.

Cumprimento de obrigações legais

Se uma lei ou uma regulamentação exige a utilização dos dados pessoais para algum motivo específico, **não é preciso** solicitar a autorização do titular de dados. É necessário cumprir o disposto na lei, nem que para isso seja necessário tratar dados pessoais do titular.

Se você é um pequeno comerciante, você precisa coletar dados pessoais de seus clientes, como o CPF, para poder emitir a nota fiscal de um produto que será entregue na sua residência. Nesse caso, **não é necessário** pedir a autorização do indivíduo, já que esta é **uma obrigação legal** para cumprimentos de exigências fiscais.

O registro de certas informações de empregados para fazer a folha de pagamento é considerado cumprimento de uma obrigação legal, pois o empregador terá que compartilhá-las com a Receita Federal, por exemplo

Legítimo interesse

Essa é a base legal que permite à empresa tratar dados pessoais, mesmo sem autorização do titular, para finalidades que visem apoiar ou promover as suas atividades ou de terceiros, o que ficou conhecido como interesses legítimos, desde que respeitados os direitos e liberdades do titular.

EXEMPLOS PRÁTICOS

Estabelecimentos comerciais que enviem e-mail em campanhas de marketing digital, para criar e manter o relacionamento com clientes, gerando mais resultados nas vendas e melhorando a retenção de clientes, por exemplo.

Para tanto, normalmente as empresas utilizam-se de dados como informações cadastrais e comportamento do cliente no site.

Nesse caso, considerando que o indivíduo já possui uma relação pré existente com o estabelecimento comercial, não é necessária a autorização do indivíduo para a coleta desses dados e sua utilização, podendo esses estabelecimentos valerem-se do legítimo interesse.

EXEMPLOS PRÁTICOS

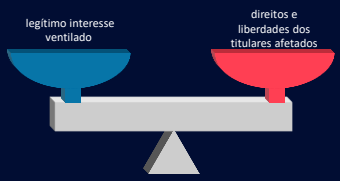
Coleta de dados para fins de prevenção à fraude.

Caso fosse necessário pedir autorização para tratar dados para essa finalidade, **os fraudadores nunca as concederiam**.

Neste caso, é um **interesse legítimo** da empresa tratar os dados, sem autorização prévia do titular, para a **finalidade específica de prevenção à fraude**.

Inciso IX do Artigo 7º da LGPD (“*quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais*”),

Teste de proporcionalidade



Esse teste de proporcionalidade pode ser feito por meio de um *Legitimate Interest Assessment* (“LIA”),

A LIA é uma avaliação interna de legítimo interesse feita pelo próprio controlador previamente ao tratamento de dados, com base em legítimo interesse, impondo ao controlador um ônus de assegurar que essa avaliação tenha sido realizada de forma adequada.

Essa avaliação pode ser a qualquer tempo questionada pela autoridade competente (a Autoridade Nacional da Proteção de Dados “ANPD”), de modo que a diligência e atenção na sua realização deve ser redobrada.

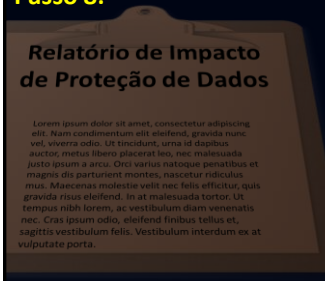
art. 7 § 6º da LGPD:

art. 7 § 6º A eventual ***dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações*** *previstas nesta Lei,* ***especialmente da observância dos princípios gerais e da garantia dos direitos do titular.***

Modelo de teste de proporcionalidade
Legitimate Interest Assessment (LIA)

Disponibilizado nos slides

Passo 8:



é definido como a documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais.

Ele também apresenta as medidas, salvaguardas e mecanismos de mitigação de riscos, conforme o artigo 5º, inciso XVII da Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018).

ANPD Autoridade Nacional de Proteção de Dados

LGPD não traz claramente como e quando fazer o Relatório de Impacto de Proteção de Dados Pessoais

ANPD Autoridade Nacional de Proteção de Dados

O artigo 38 da LGPD estabelece que a **Autoridade Nacional** poderá determinar que o controlador elabore um relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente às suas operações de tratamento de dados, nos termos do regulamento, observados os segredos comercial e industrial.

O Relatório de impacto à proteção de dados pessoais precisa apresentar :

- A descrição sobre os tipos de dados coletados;
- O método utilizado para obtê-los;
- Quais foram as informações fornecidas aos clientes sobre essa garantia de segurança ;
- Análise do controlador sobre todas as ações realizadas para conter os riscos.

Excelente instrumento para a prestação de contas e demonstração de conformidade com a LGPD.

Exemplos de Relatórios de Impacto de proteção de dados

Disponibilizado nos slides

Passo 9:

As pessoas que tiveram os dados captados por você, sabem exatamente como você os utiliza e entendem para que são usados ?

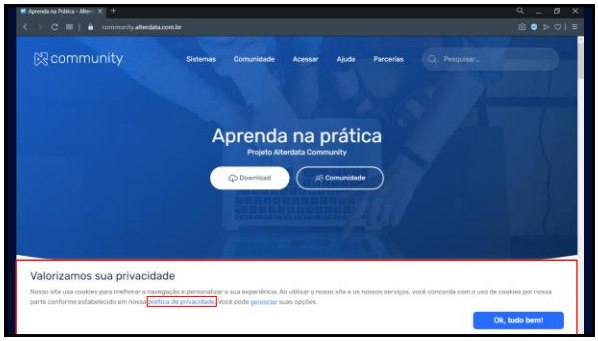
Aplicação do principio da Transparência e Finalidade

Passo 10:

No site da sua empresa, tem divulgada uma política de privacidade ou algum aviso em formulários de cadastro, contratos, propostas, sobre os itens anteriores ?

Política de Privacidade: deverá ser apresentada de forma clara, acessível e ostensiva, devendo conter, entre outros aspectos:

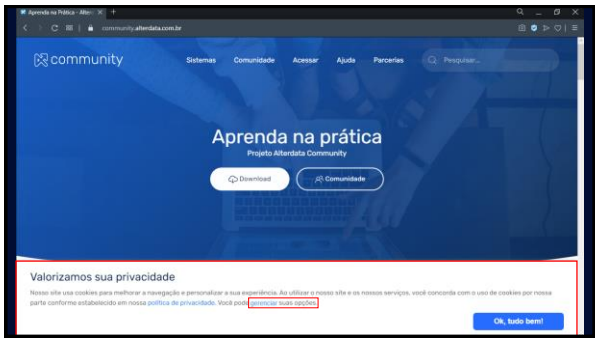
- O que está sendo coletado;
- Qual objetivo com a coleta;
- identificação e informações de contato do controlador;
- informações sobre compartilhamento de dados;
- menção expressa aos direitos dos titulares e como exercê-los;

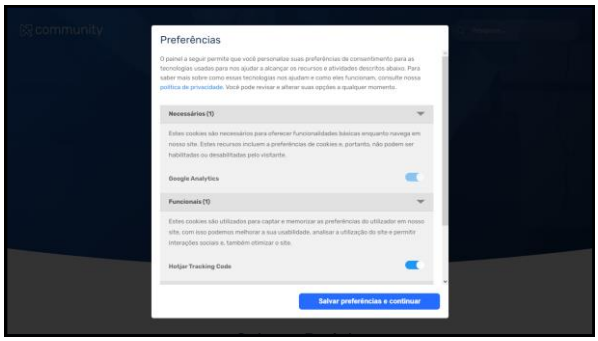


Aviso de Cookies: verifique se o site da sua empresa precisa que você tenha um aviso de que o site utiliza cookies para coletar dados do usuário.

Se for o caso, esse aviso deve indicar:

- Qual o objetivo da coleta;
- O que está sendo coletado
- A possibilidade do usuário dar seu "aceite" ou a "recusa" da coleta.
- Possibilidade de gerenciar o Cookie





Contratos – O que diz a LGPD sobre contratos ?

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular:

§ 3º Quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento.

http://www.planalto.gov.br/ccivil_03/_ato2015-2018/lei/l13709.htm

Exemplo de Contrato entre Controlador e Operador

Disponibilizado nos slides

Passo 11:

Sua empresa tem alguma forma dos "donos dos dados" exercerem seus novos direitos ?

Esses direitos incluem, por exemplo:

- solicitar informações à empresa sobre o tratamento de seus dados;
- corrigir ou excluir seus dados;
- ter explicações sobre como e para quais finalidades os dados estão sendo tratados;
- entre outros

Todo o conteúdo da Lei 13.709

incluindo os direitos dos titulares

Disponibilizado nos slides

Término do Tratamento de Dados

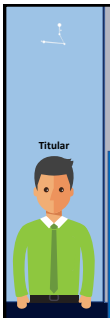
Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

I – verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;

II – fim do período de tratamento;

III – comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou

IV – determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.



Titulares: liberdade para **determinar** a **suspensão da autorização** para o uso dessas informações **a qualquer momento.**
O acesso claro e completo aos dados pessoais do titular, deve ser fornecido em até **15 dias** da data da solicitação.

Em razão da natureza dos dados tratados considerando a existência de legislações ou imposições especificas relativas a estes dados, o controlador (empresa) poderá estar impedido de realizar a exclusão dos dados, pois é de sua responsabilidade cumprir prazo prescricional judicial e administrativo.

Passo 12:

A proteção dos dados agora é responsabilidade de quem guarda.

Por exemplo:

- Sua empresa possui armários com chave para documentos físicos importantes?
- Os computadores possuem antivírus e estão sempre bloqueados por senha?
- Existe um controle de quem acessa o que, nos sistemas e quando as informações são acessadas?

CUIDADO:

LOGS

Muitos sistemas fazem o **registro constante** de **quem** está consultando os dados dos clientes e **o que** foi consultado.

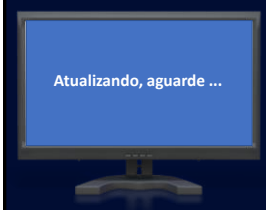
Tenha a certeza de que o sistema do seu escritório possui este recurso.

CUIDADO:

Não passe suas senhas de trabalho para nenhum colega, exceto quando há autorização da sua liderança.

Tenha a certeza de que **bloqueou o seu computador** (logoff) antes de sair do terminal, mesmo que rapidamente.

CUIDADO:



Não interrompa atualizações de sistemas. Elas são voltadas a trazer maior segurança para todos os colaboradores, para a empresa e consequentemente para os clientes.

Em caso de problemas ou dificuldades, notifique a equipe técnica de sua empresa.

CUIDADO:

A mesma orientação vale para **Cópias de Segurança (Backups)**.

Elas também são voltadas a trazer maior segurança para todos os colaboradores, para a empresa e consequentemente para os clientes.

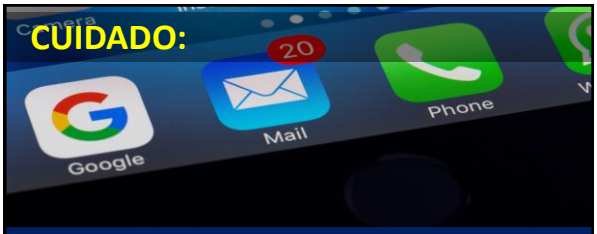
Em caso de problemas ou dificuldades, também notifique a equipe técnica de sua empresa.

CUIDADO:

Cópias de arquivos do trabalho para pendrive ou qualquer outro dispositivo que vá sair da empresa, precisam ser **aprovados**.

Poderão haver arquivos que não foram liberados para compartilhamento e gerar um problema sério e desnecessário.

CUIDADO:



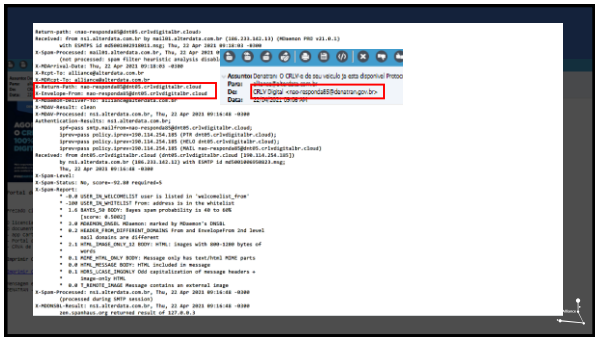
Emails pessoais só devem ser acessados de dispositivo pessoal.

É fundamental que os colaboradores da empresa não misturem a vida corporativa com a pessoal. Ética profissional acima de tudo.

CUIDADO

Não acesse e-mails com **assuntos diferentes** do seu trabalho.

Sempre **desconfie** de cada mensagem recebida.



CUIDADO:

Antivírus precisam estar sempre atualizados.
Avise a equipe técnica se surgir qualquer mensagem de problemas.

Respeite as regras do firewall. Não tente burlar para baixar arquivos bloqueados ou acessar sites não permitidos. A segurança de todos começa com você.

Incidente de Segurança

Um incidente de segurança com dados pessoais é qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação na segurança de 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.

O que fazer em caso de um incidente de segurança com dados pessoais?

- Avaliar internamente o incidente – natureza, categoria e quantidade de titulares de dados afetados, categoria e quantidade dos dados afetados, consequências concretas e prováveis.
- Comunicar ao encarregado (Art. 5º, VIII da LGPD);
- Comunicar ao controlador, se você for o operador, nos termos da LGPD;
- Comunicar à **ANPD** e ao **titular de dados**, em caso de risco ou dano relevante aos titulares (Art. 48 da LGPD);
- Elaborar documentação com a avaliação interna do incidente, medidas tomadas e análise de risco, para fins de cumprimento do princípio de responsabilização e prestação de contas (Art. 6º, X da LGPD).

Qual o prazo para comunicar um incidente de segurança para a Autoridade Nacional de Proteção de Dados?

A LGPD determina que a comunicação do incidente de segurança seja feita em prazo razoável (art. 48, § 1º), conforme será definido pela ANPD.

Embora não tenha havido regulamentação nesse sentido, a realização da comunicação demonstrará transparência e boa-fé e será considerada em eventual fiscalização.

Comunicação de incidentes de segurança

Disponibilizado pela ANPD

Disponibilizado nos slides

Aplicando a LGPD

CRCMG
CONSELHO REGIONAL DE CONTABILIDADE DE MINAS GERAIS

ALEXANDRE NEVES
alliance@alterdata.com.br

- Templates de mapeamento de dados da ICO (*Information Commissioner's Office*) em conformidade com a GDPR:
  https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/
- Exemplo de modelo de teste de proporcionalidade - Legitimate Interest Assessment (Sample LIA Template)
  https://ico.org.uk/media/for-organisations/forms/2258435/gdpr-guidance-legitimate-interests-sample-lia-template.docx
- GDPR em Português
  https://jus.com.br/artigos/81519/lei-gdpr-em-portugues
- Lei 13.709 - LGPDP
  http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm
- Exemplo de Relatório de impacto à proteção de dados pessoais
  https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiatemplateRIPD.pdf
  https://gdpr.eu/data-protection-impact-assessment-template/

- Exemplo de Contrato entre Controlador e Operador – Data Processing Agreement (Template):
  https://gdpr.eu/data-processing-agreement/
- Comunicação de incidentes de segurança
  https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca
- Exemplo de Política de Privacidade
  https://www.alterdata.com.br/politica-de-privacidade