LEI GERAL DE PROTEÇÃO DE DADOS

Cartilha da CCS – Tecnologia e Serviços S.A.

A CCS se preocupa muito com as Legislações e normas definidas pelos órgãos governamentais, sendo assim criou esse material para que você possa tomar conhecimento geral do tema, e com isso nos ajudar sempre em busca da perfeição.

A Lei Geral de Proteção de Dados —LGPD —Foi criada no Brasil para Consolidar Direitos e Deveres em relação à Proteção de Dados. Iniciativas que garantam a privacidade e a segurança dos dados pessoais são cada vez mais frequentes em um cenário global.

Devemos cuidar dos dados que estão sob nossa responsabilidade da mesma forma que gostaríamos que os nossos dados fossem tratados.

Então, faça sua parte: tenha atenção e cuidado no uso dos dados!

Qualquer dúvida ou necessidade, entre em contato com o encarregado de dados através do e-mail:

encarregado_dados@ccstec.com.br

1. Introdução

1.1. Contexto.

A Lei Geral de Proteção de Dados ("LGPD" -Lei nº 13.709/2018), publicada em 15 de agosto de 2018, com início de vigência em vigor em 18 de setembro de 2020, é um importante marco legislativo nacional no tratamento de Dados Pessoais, fazendo parte de um movimento mundial de preocupação com Dados Pessoais e o papel que os particulares e o Estado devem desempenhar no tratamento de dados.

Muito da nova lei é inspirado na General Data Protection Regulation (GDPR) da União Europeia, a qual entrou em vigência em maio de 2018, que tem como principal foco criar regras de tratamento de dados buscando empoderar o usuário com o controle sobre as suas informações. Dessa forma, há um foco grande na liberalidade do usuário em controlar, retificar e excluir seus dados dos bancos de dados públicos e privados.

A CCS apresenta esta cartilha com o objetivo de conscientizar os colaboradores no tratamento de Dados Pessoais, sabendo que o novo cenário tem sua complexidade, o que traz desafios e incertezas para todos. Os desafios chegam em ritmo de contagem regressiva, com foco na adequação de operações e processos aos requisitos trazidos por essa regulamentação, que já está em vigor.

1.2. Objetivo da Lei.

A LGPD estabelece os princípios, direitos e deveres que deverão ser observados, no tratamento de Dados Pessoais, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (pessoa física).

1.3. Abrangência.

A LGPD se aplica a qualquer operação de tratamento de Dados Pessoais (vide definição no item 2), seja por pessoa física ou jurídica, de direito público ou privado, independente do meio, país de sua sede ou país onde estejam localizados os dados, desde que:

i. a operação de tratamento seja realizada no Brasil;
ii. a operação de tratamento tenha como objetivo a oferta ou fornecimento de bens, serviços ou tratamento de dados de pessoas físicas localizadas no Brasil;
iii. os Dados Pessoais tenham sido coletados no Brasil.

Ainda, podem ser considerados Dados Pessoais, nos termos do §2° do Art. 12 da LGPD, os utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada. Por exemplo: cruzamento de bases anonimizadas que levam à identificação do indivíduo.

A LGPD também dá tutela diferenciada e limita as hipóteses de tratamento de Dados Pessoais sensíveis (Artigo 11) e de crianças e adolescentes (Artigo 14).

1.4. Exceções.

De acordo com o artigo 4°, a LGPD não abrange o tratamento de dados:

i. por pessoa física, com fins particulares, não econômicos (exemplo: agenda pessoal de contatos; lista de convidados de uma festa particular);
ii. para fins exclusivamente jornalísticos, artísticos e acadêmicos; e
iii. para fins exclusivos de segurança pública; defesa nacional; segurança do Estado; atividades de repressão de infrações penais;

iv. Dados provenientes de fora do Brasil e que não sejam objeto de tratamento por agentes de tratamento brasileiros (vide o conceito de "agentes de tratamento" no Capítulo 2).

2. Conceitos.

O Artigo 5°, da LGPD, traz em seus incisos, conceitos importantes para compreender as responsabilidades e o processo de tratamento dos dados. Para fins didáticos e facilidade de consulta, foram organizados em ordem alfabética e indicados, entre parêntesis, a referência legal.

Agentes de Tratamento:
o controlador e o operador (Art. 5°, IX);

Anonimização:
meios técnicos por meio dos quais um dado perde a capacidade de identificar uma pessoa física (Art. 5°, XI);

Autoridade Nacional ("ANPD"):
órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD (Art. 5°, XIX);

Banco de Dados:
conjunto estruturado de Dados Pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico (Art. 5°, IV);

Bloqueio:
suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados (Art. 5°, XIII);

Consentimento:

manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus Dados Pessoais para uma finalidade determinada (Art. 5°, XII);

Controlador:

pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de Dados Pessoais (Art. 5°, VI);

Dado Pessoal:

informação relacionada a pessoa natural identificada ou identificável (Art. 5°, I);

Dado Pessoal Sensível:

dado pessoal sobre 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, quando vinculado a uma pessoa natural (Art. 5°, II);

Dado Anonimizado:

dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento (Art. 5°, III);

Eliminação:

exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado (Art. 5°, XIV);

Encarregado:

pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (Art. 5°, VIII);

Operador:

Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de Dados Pessoais em nome do controlador (Art. 5°, VII);

Órgão de Pesquisa: órgão, público ou privado, sem fins lucrativos, com sede e foro no Brasil, que tenha como objeto a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e (Art. 5°, XVIII);

Relatório de Impacto à Proteção de Dados Pessoais:

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, bem como medidas, salvaguardas e mecanismos de mitigação de risco (Art. 5°, VII).

Titular:

pessoa física a quem se referem os Dados Pessoais que são objeto de tratamento (Art. 5°, V);

Transferência Internacional de Dados:

transferência de Dados Pessoais para país estrangeiro ou organismo internacional do qual o país seja membro (Art. 5°, XV);

Tratamento:

toda operação realizada com Dados Pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (Art. 5°, X);

Uso Compartilhado de Dados:

comunicação, difusão, transferência internacional, interconexão de Dados Pessoais ou tratamento compartilhado de

bancos de Dados Pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente,
com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados (Art. 5°, XVI).

3. Princípios aplicáveis ao Tratamento de Dados e Direitos dos Titulares.

3.1. Princípios:

Os Agentes de Tratamento devem adotar medidas efetivas para que as operações de Tratamento estejam aderentes aos princípios previstos no Artigo 6° da LGPD:

Princípio da Boa-Fé: princípio geral que permeia todas as relações jurídicas. A boa-fé se presume e a quebra da Boa-fé acarreta consequências jurídicas.
Exemplo: Criar um termo de uso de dados intencionalmente ambíguo para o Tratamento de Dados Pessoais, com o intuito de induzir o Titular a dar consentimento excessivo para que os dados sejam utilizados em mais hipóteses do que gostaria viola a Boa-Fé.

Princípio da Finalidade: Os Dados Pessoais devem ser tratados para propósitos específicos, os quais devem ser informados ao Titular dos dados previamente, de modo explícito e sem que seja possível a utilização dos dados posteriormente para outra aplicação.
Exemplo: Dados Pessoais coletados em cadastros de fornecedores/clientes não podem ser utilizados para envio de e-mails marketing sem que o titular tenha fornecido o consentimento expresso para tal tratamento. A coleta do dado em questão pressupõe a finalidade de cumprimento de contrato, e o envio de promoções sem o "ok" do titular seria uma utilização excessiva.

Princípio da Adequação: Os Dados Pessoais devem ser usados de modo compatível com a finalidade declarada ao Titular.
Exemplo: O Titular fornece o consentimento para receber promoções de marketing por parte da CCS. Como esse consentimento é especifico para esse tratamento de promoções, caso a CCS precise compartilhar as informações do titular de dados com terceiro, é necessário recolher um novo consentimento para esse compartilhamento específico.

Princípio da Necessidade: O Tratamento deve ser limitado ao mínimo necessário para o alcance da finalidade.
Exemplo: Conjugado com o exemplo do Princípio da Finalidade: O dado é recolhido para uma finalidade específica e apenas porque é necessário para a realização da operação. Por exemplo, em caso de venda para pessoa física, é necessário que o titular forneça o CPF, porque caso não seja fornecido, a venda não será concluída.

Princípio do Livre Acesso: Garantia aos Titulares à consulta facilitada e gratuita sobre a forma e a duração do Tratamento, bem como o acesso à integralidade dos seus Dados Pessoais. Ênfase nos termos "facilitada", "gratuita" "acesso à integralidade".

Princípio da Qualidade: Deve ser garantido ao Titular exatidão, clareza, relevância e atualização dos dados.

Princípio da Transparência: Deve ser garantida a prestação de informações claras e facilmente acessíveis pelos Titulares. O Titular deverá ser capaz de solicitar seus dados, de corrigi-los ou de solicitar sua exclusão de forma rápida, fácil e descomplicada.

Princípio da Segurança: Deverão ser adotadas medidas técnicas e administrativas aptas a proteger os dados de acessos não autorizados. O Artigo 46, § 1° e 2° estipulam que, além da responsabilidade pela adoção das medidas de proteção, a ANPD poderá dispor sobre os padrões técnicos mínimos aceitáveis.

Princípio da Prevenção: Deverão ser adotadas medidas para prevenir a ocorrência de danos em virtude do Tratamento de Dados Pessoais. Notem que o princípio é de prevenção. Não bastará mais agir de modo reativo, ou seja, após o acidente. Se uma prevenção não for adequadamente implementada, os pressupostos jurídicos para uma ação de responsabilidade civil estarão postos: houve negligência, ou seja, descumprimento do dever geral de diligência (cuidado) a que todos estão subordinados. Além do Artigo 46, a lei ainda traz outros elementos no artigo 50 e seguintes, propondo ações de governança e treinamentos.

Princípio da Não Discriminação: Impossibilidade de tratamento para fins discriminatórios. Utilizar dados para fins que gerem discriminação são proibidos.
Exemplo: Nos procedimentos do RH, a indicação da filiação partidária, orientação religiosa e sexual não pode ser utilizada para cunho discriminatório. O assunto somente deve ser tratado caso haja necessidade e deve ser restrito apenas àquelas pessoas que tenham finalidade e necessidade de tratamento do dado.

Princípio da Responsabilização e Prestação de Contas: A CCS deve apontar um Encarregado e atribuir responsabilidades aos seus colaboradores com a segurança da informação e proteção de dados. A LGPD impõe a elaboração de um Relatório de Impacto à Proteção de Dados Pessoais, que consiste no documento que contém todos os pontos de interesse relativos à proteção de Dados Pessoais, incluindo medidas de segurança e contenção de riscos documentadas, funcionando perfeitamente ao atendimento deste princípio. Sobre o Relatório de Impacto, a ANPD irá regulamentar em quais situações e quais os requisitos devem constar do documento.

3.2. Direitos dos titulares:

O artigo 18 da LGPD preceitua que o titular de dados possui o direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
I - confirmação da existência de tratamento;
II - acesso aos dados;
III - correção de dados incompletos, inexatos ou desatualizados;
IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD;
V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;

VI - eliminação dos Dados Pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da LGPD;
VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
IX - revogação do consentimento, nos termos do § 5° do art. 8° da LDPD.

4. Hipóteses de Tratamento de Dados.

4.1. Tratamento de Dados Pessoais

Nos termos da LGPD, o Tratamento de Dados Pessoais somente poderá ser realizado em uma das dez hipóteses previstas nos incisos do Art. 7°. As hipóteses, taxativas, são:

i. mediante o fornecimento de consentimento pelo titular;
ii. para o cumprimento de obrigação legal ou regulatória pelo controlador;
iii. pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
iv. para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos Dados Pessoais;
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;
vi. para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei n° 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
vii. para a proteção da vida ou da incolumidade física do titular ou de terceiros;
viii. para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;
ix. quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos Dados Pessoais; ou
x. para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Nos termos do Artigo 7°, § 4°, é dispensada a exigência do Consentimento para os dados tornados manifestamente públicos pelo Titular, resguardados os direitos do Titular e os princípios previstos na LGPD. Ou seja, os Dados Pessoais podem ser tratados sem o Consentimento, mas balizado pelos princípios e fins legítimos. Não pode ser um Tratamento indiscriminado e abusivo. Não pode apenas atender aos interesses da CCS.

4.2. Tratamento de Dados Pessoais Sensíveis:

A LGPD classifica alguns dados como Dados Pessoais sensíveis, pois identificam informações específicas passiveis de discriminação e, assim, possuem um potencial de gerar danos ao seu titular caso sejam vazados. Por essa razão, os dados sensíveis devem ser tratados com muito mais cautela.

São considerados dados sensíveis, mas não se restringem a eles os:

Dados Pessoais que revelem a origem racial ou étnica, opiniões políticas e convicções religiosas ou filosóficas;

a filiação sindical;

os dados genéticos, dados biométricos tratados simplesmente para identificar um ser humano;

os dados relacionados com a saúde;

os dados relativos à vida sexual ou orientação sexual da pessoa.

Para que as atividades de tratamento de Dados Pessoais Sensíveis sejam consideradas lícitas e legítimas, o artigo 11 da LGPD apresenta as hipóteses de tratamento de Dados Pessoais, quais sejam:

i. quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

ii. sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a. cumprimento de obrigação legal ou regulatória pelo controlador;
b. tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
c. realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos Dados Pessoais sensíveis;
d. exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;
e. proteção da vida ou da incolumidade física do titular ou de terceiros;
f. tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
g. garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9° desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos Dados Pessoais.

5. Sanções e Penalidades.

A LGPD estabelece penalidades bastante rigorosas, em seu art. 52:

i. Advertência;
ii. Obrigação de divulgação do incidente;
iii. Bloqueio ou eliminação de Dados Pessoais;
iv. Suspensão parcial do funcionamento do banco de dados por até 12 meses;
v. Suspensão do tratamento dos dados pelo período máximo de 12 meses;
vi. Proibição parcial ou total do exercício de atividades relacionadas ao tratamento de dados;

vii. Multa simples de até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos e limitada, no total, a R$ 50 milhões por infração.
viii. Multa diária de até R$ 50 milhões, conforme item acima.

No entanto, as penalidades não substituem a aplicação de sanções administrativas, civis ou penais previstas em legislação específica (art. 52, §2°) e existem contingência potenciais, tais como: ações individuais ou coletivas de natureza cível ou trabalhista; rescisão de contratos por quebra de deveres de proteção de dados e sigilo; danos reputacionais; ações promovidas pelo Ministério Público etc.
Os colaboradores que infringirem as normas de privacidade e proteção de dados podem vir a sofrer medidas disciplinares trabalhistas ou penalidades e sanções cíveis, criminais ou administrativas caso não cumpram seu papel de tratamento de Dados Pessoais consciente e de acordo com a LGPD e os materiais internos da CCS, tais como esta cartilha, o Código de Conduta e outros.

6. Questões Relevantes para CCS

6.1. Recebimento de currículos

O currículo é um documento que possui diversos Dados Pessoais, e pode até possuir Dados Pessoais sensíveis. Desta forma, o cuidado com tal documento deve ser redobrado e de competência somente da área de Recursos Humanos, a qual tem efetiva necessidade e finalidade para entrar em contato com tais dados.
Neste sentido:

Boas Práticas
i. o currículo deve somente ser recebido pela área de RH, a qual vai solicitar e registrar o Consentimento do candidato e informá-lo de

maneira clara que seus Dados Pessoais serão utilizados para recrutamento, avaliação e seleção por prazo determinado, findo o qual o currículo será deletado da base de dados;
ii. caso o candidato não seja contratado, eliminar os seus Dados Pessoais, ressalvadas as hipóteses de obrigação legal de conservá-los ou questionar e pedir o Consentimento para armazenar os Dados Pessoais para futuras oportunidades;
iii os colaboradores, não devem receber currículos em seus e-mails ou pessoalmente e, caso isso aconteça, deverão informar ao possível candidato o caminho correto para o envio do currículo, bem como que o currículo eventualmente recebido está sendo deletado/descartado e, efetivamente, deletar/descartar. Em caso de deleção, copiar o RH na resposta para ciência.
iiii. se necessário compartilhar o currículo, fazê-lo apenas com o Consentimento expresso do candidato para o compartilhamento.

Não vá por esse caminho...

i. Fazer uma pasta pessoal de currículos para usar eventualmente.
ii. usar os Dados Pessoais de candidatos para finalidades distintas do processo de recrutamento e seleção;
ii. ser evasivo, ambíguo, pouco claro nos termos de uso e políticas de privacidade para o uso de Dados Pessoais ao longo do processo de recrutamento e seleção;
iii. compartilhar os currículos com outras empresas, ainda que do mesmo grupo econômico, sem o consentimento expresso do candidato.
iv. usar Dados Pessoais com caráter discriminatório e/ou informações pretéritas do candidato (ex.: background checks, existência de ações trabalhistas por ele ajuizadas) como elemento capaz de definir sua contratação ou não, já que, nos termos da LGPD, Dados Pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo (Art. 21).

6.2. Recebimento de atestados.

Os atestados médicos são documentos que possuem Dados Pessoais sensíveis, os quais podem ser utilizados de forma discriminatória e vexatória por colegas imaturos. Para preservar a proteção destas informações pessoais sensíveis, os atestados devem somente ser recebidos pela área do Ambulatório, os quais possuem efetiva necessidade e finalidade para o tratamento das informações, por motivos de compensação de horas ou abono de falta, entre outros.

Boas Práticas

i. os atestados devem ser entregues apenas no ambulatório, não precisando passar pelo gestor para assinar.
ii. zelar pela proteção dos dados constantes no atestado.
iii. armazenar em local seguro e chaveado, o qual somente as pessoas que necessitem e tenham finalidade para o tratamento do dado tenham acesso.

- Meu colega faltou hoje no trabalho e me pediu para entregar o atestado ao gestor, e agora?

Você deve informar ao seu colega que não poderá entregar o atestado dele para o superior, uma vez que o atestado deve ser entregue no ambulatório.

Não vá por esse caminho...

i. vistar o atestado antes de enviar para o ambulatório.
ii. tirar cópia do atestado do colaborador e manter em um banco de dados pessoal do gestor.
iii. deixar em cima da mesa ou em algum lugar de fácil acesso, pois isso pode acarretar fuga de informação.
iv. enviar ou receber o documento por whatsapp.

vi. discriminar o colega por ter entrado em contato com a condição descrita no atestado.
vii. compartilhar as informações que receber.

- Recebi um atestado por WhatsApp, e agora?

Delete o atestado do seu whatsapp e avise o colaborador que esta não é a via oficial de envio.

6.3. Relações de Trabalho e Emprego.

A CCS trata seus Dados Pessoais e, eventualmente, de seus dependentes, para o cumprimento de obrigações legais e concessão de benefícios. Embora a LGPD autorize o Tratamento de Dados Pessoais de colaboradores e prestadores de serviços (Artigo 7°, incisos V e IX) para a legítima execução dos contratos; indispensáveis ao cumprimento de obrigações legais ou regulatórias pelo empregador (ex.: envio de Dados Pessoais dos colaboradores ao Ministério do Trabalho e Emprego, INSS e CEF etc.); e em benefício do próprio empregado, é importante que os colaboradores tenham consciência do tratamento de seus Dados Pessoais.

Encerrada a relação de trabalho, seja por iniciativa do colaborador ou da administração da CCS, os Dados Pessoais do colaborador devem ser eliminados, salvo nas hipóteses de obrigação legal de conservar tais documentos, para atendimento, por exemplo, de fiscalizações e ações trabalhistas.

Boas Práticas
i. dar ciência ao colaborador do uso dos seus Dados Pessoais, autorizando-o para a realização de todas as ações relacionadas ao seu contrato de trabalho.
Ii. incluir aditivo de contrato de trabalho, o qual contenha cláusulas

protetivas em relação à proteção de dados e segurança da informação.
iii. comunicar todas as alterações relacionadas ao Tratamento de Dados Pessoais nos documentos da CCS;
iv. apresentar as hipóteses que o colaborador pode escolher ou não fornecer/compartilhar Dados Pessoais, como, por exemplo, o compartilhamento de aniversários dentro da CCS, que deve ser feita somente com autorização do titular.

Não vá por esse caminho...

i. não incluir cláusula de proteção de dados, como obrigação, no contrato de trabalho;
ii. não requerer ou presumir o Consentimento do empregado, em situações que o mesmo é necessário;
iii. não ser transparente com as informações dos colaboradores;
iv. vender informações de colaboradores;
v. não eliminar informações de ex-colaboradores, após transcorridos prazos prescricionais;
vi. violar direitos de proteção de dados e privacidade de colaboradores;
vii. não considerar fins e hipóteses legítimas de Tratamento de Dados Pessoais;
viii. assediar o colaborador para que este dê seu Consentimento para determinada situação concreta.

6.4. Interação com Dados Pessoais

Os Dados Pessoais de colaboradores, terceiros e clientes permeiam os trabalhos na CCS. Ainda que a empresa seja B2B, sempre há uma pessoa física que representa a pessoa jurídica e, por vezes pode haver a interação com os Dados Pessoais destas pessoas. O tratamento de dados, que inclui seu armazenamento, manutenção, atualização, anonimização e eliminação, deve observar os princípios da finalidade e a necessidade, que constam no artigo 6º da LGPD.

Boas Práticas

i. sempre verificar a necessidade e finalidade de manuseio dos Dados Pessoais.
ii. após o tratamento e caso não precise mais ser utilizado, o dado deve ser deletado/ descartado.
ii. Não receber dados e/ou cópias de documentos pessoais que não sejam necessários para o desempenho da atividade.
iii. Armazenar as informações de forma segura e que somente franquear o acesso aos colaboradores que tenham necessidade e finalidade para acesso ao dado.
iv. no cadastro de clientes e fornecedores, apenas recolher as informações necessárias para concluir o pedido e fechar o contrato de compra ou venda do produto.

- Recebi os dados para cadastramento do cliente/fornecedor por um terceiro, e agora?

O cliente/fornecedor sabe que você tem os dados dele? Esse terceiro te passou o consentimento expresso do titular?

Não vá por esse caminho...

i. manter um banco de dados com informações excessivas e que não possuem mais finalidade e necessidade para o tratamento.
ii. deixar informações pessoais em cima da mesa, à vista de outras pessoas que não tenham necessidade e finalidade de contato.
iii. compartilhar as informações com colegas ou terceiros, sem o consentimento do titular.

- Nunca apaguei meu banco de dados e estou na empresa há 25 anos, e agora?

Analisar se todos os documentos com Dados Pessoais que possui tem finalidade e necessidade para o tratamento. Se não tiver, os

documentos tem que ser deletados/excluídos dos arquivos digitais/físicos.

6.5. Meios de comunicação

Com o advento da tecnologia, diversos meios de comunicação foram criados para facilitar a troca de informações e transforma-las em meios rápidos de comunicação. No entanto, da mesma forma que a troca é rápida, o vazamento e a fuga de informações também são rápidos. Neste sentido, é necessário ter um cuidado maior com a utilização destes veículos.

Boas Práticas

i. Troca de Dados Pessoais necessários devem ser feitos apenas pelos meios corporativos, preferencialmente pelo e-mail corporativo.

- Clientes e fornecedores preferem me enviar documentos pelo whatsapp, pois acham que é um meio mais efetivo de troca de documentos; E agora?

Neste caso, o colaborador deve advertir que apenas irá receber os documentos pelo e-mail corporativo, de acordo com as políticas da empresa.

Não vá por esse caminho...

i. envio de Dados Pessoais por whatsapp pessoais.
ii. compartilhamento de contatos pessoais com terceiros sem o devido consentimento do titular de dados.
iii. troca (envio e recebimento) de documentos pessoais por WhatsApp pessoal.

- Meu amigo pediu uma indicação, quero ajudar, posso encaminhar um currículo do banco da CCS pelo WhatsApp. E agora?

Esta prática não deve ser realizada, somente o RH pode ter acesso a currículos, especialmente fora de processo seletivo. Ainda, para o compartilhamento de documentos que contém Dados Pessoais, é necessário recolher o consentimento específico do titular de dados.

6.6. Terceirização.

Na terceirização de serviços, é preciso ter cautela nos contratos com clientes e fornecedores, uma vez que a responsabilidade da LGPD é solidária, ou seja, se um terceiro vazar dados que foram compartilhados pela CCS, ambos responderão no âmbito judicial e administrativo.
Por isso a cautela com o terceiro é tão importante. Não adianta a CCS estar diligente com a LGPD e contratar um serviço de alguém que não esteja de acordo com a lei, pois caso aconteça, a CCS também será responsabilizada. Neste sentido:

Boas Práticas
i. realizar auditorias, due dilligence ou risk assessment dos terceiros antes de fechar o contrato, para verificar a aderência da empresa à LGPD.
ii. aditar todos os contratos pretéritos e inserir nos novos, cláusulas protetivas de segurança da informação e proteção dos Dados Pessoais.
iii. compartilhar as políticas de tratamento de dados e documentos correlatos com os terceiros para aderência.

- Contratei um terceiro sem averiguar se ele está adepto à LGPD. E agora?

Aditivar o contrato para incluir cláusulas de proteção de dados e segurança da informação. Disseminar os materiais que versem sobre a LGPD para seu terceiro, exigir o respeito e cumprimento destas normas e incentivar o parceiro a se adequar.

Não vá por esse caminho...
i. realizar propostas informais.
ii. não avaliar a empresa e sua aderência à LGPD antes de fechar o negócio.
iii. compartilhar informações excessivas com os terceiros, como Dados Pessoais sensíveis ou dados desnecessários para a realização do trabalho acordado.

- Não utilizo contratos formais para realizar os serviços na CCS. E agora?

Todo o serviço deve possuir um contrato, porém nos casos de propostas informais, devem ser realizadas pelos e-mails corporativos. É bom usar este espaço para colocar um exemplo diferente do dito anteriormente.

6.7. Vazamento de Dados

A definição do termo "Vazamento de Dados" se dá pelo acesso de informações privadas, confidenciais ou pessoais por uma pessoa não autorizada e disponibilização para outras. Em geral, isso acontece quando alguém invade um banco de dados, mas também pode acontecer de outras formas como, por exemplo, quando a pessoa tem permissão para acessar certo dado e o compartilha, sem o consentimento do titular, com outras pessoas que não deveriam ter acesso.
Por mais que pareça apenas uma conduta realizada por hackers e que diz respeito apenas ao TI, o ato de "vazar dados" pode ser realizado por engano por colaboradores da CCS, com o envio de

um e-mail com uma lista de clientes para um destinatário errado, por exemplo. A fuga de informações pessoais precisa ser evitada, para que a CCS não incorra nas penalidades estipuladas pela LGPD. Assim, os colaboradores devem zelar pela proteção das informações da CCS principalmente referentes à Dados Pessoais.

Boas Práticas

i. auxiliar no mapeamento de processos que envolvam Dados Pessoais e dos responsáveis pela sua efetividade;
ii. participar de treinamentos sobre o manuseio com Dados Pessoais, prestando atenção nos riscos e noções de segurança da informação e proteção de dados. Isso inclui colaboradores, terceirizados, parceiros de negócios, fornecedores, clientes e todos aqueles que interagem com a CCS e realizam trocas de Dados Pessoais.;
iii. aplicar as boas práticas disseminadas pela área de TI sobre segurança da informação no cotidiano
iv. denunciar violações de dados que ocorrerem dentro da CCS para o Encarregado de Dados.

- Cliquei em um e-mail malicioso, e agora?

Avisar a área de TI para avaliar o e-mail e aplicas as medidas necessárias para conter a contaminação por vírus. Bloquear o e-mail para que seja enviado diretamente para o SPAM novas mensagens como a anterior. Não adiar a instalação do antivírus para que seu computador esteja sempre protegido contra os malwares e phishing.

Não vá por esse caminho...

I. compartilhar dados pessoais sem o devido consentimento;
ii. clicar em e-mails maliciosos ou com cunho de phishing;
iii. não se atentar para as medidas de segurança compartilhadas pela área de TI e o Encarregado de Dados.

iv. não participar de treinamentos periódicos, a todos que lidam com Dados Pessoais, nos riscos e ameaças sob a ótica de TI.
v. enviar e-mails contendo dados pessoais sem checar se o destinatário está correto;

- Reutilizei documentos que encontrei na bandeja da impressora, e agora?

Analisar as folhas utilizadas como rascunho para averiguar se nela continham dados pessoais. Caso possuam, inutilizar o bloquinho imediatamente, triturando-o.

7. Encarregado de Dados - "DPO"

O Encarregado de Dados é o canal responsável pelas demandas sobre Dados Pessoais, bem como é o canal de comunicação entre o Titular de Dados, a CCS e a Autoridade Nacional de Proteção de Dados.
O contato está no site e deve ser utilizado para qualquer questionamento na matéria de proteção aos Dados Pessoais de terceiros, clientes, fornecedores parceiros e colaboradores. Dentre as atribuições deste encarregado, encontram-se:
i. aceitar reclamações e comunicações dos Titulares, prestar esclarecimentos e adotar providências;
ii. receber comunicações da ANPD e adotar providências;
iii. orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de Dados Pessoais; e
iv. executar as demais atribuições determinadas pela LGPD e estabelecidas em normas complementares.

Para mais informações sobre a LGPD, ou em caso de dúvidas sobre o tratamento devido ou indevido de Dados Pessoais, não hesite em contatar o encarregado de dados"
Contato:
encarregado_dados@ccstec.com.br

8. Considerações Finais.

Com a LGPD, o Brasil entrou no rol de países possuem legislação protetiva de Dados Pessoais.
A Lei surgiu como um divisor de águas, exigindo um giro conceitual na forma como as empresas se relacionam com Dados Pessoais. Mais que empoderar as pessoas físicas quanto às informações que lhe dizem respeito, a LGPD se insere em um cenário de transparência e ética no mundo dos negócios, que cada vez mais dependem de meios digitais.
Para que todos levem os seus termos a sério, foram previstas as penalidades severas, que serão evitadas através de boas políticas de dados e termos de uso, que garantam a atuação de todos os Controladores dentro das novas diretrizes, alinhadas com o cenário mundial.
A responsabilidade por essas questões passa a ser de todos que interagem com Dados Pessoais, em nome ou em benefício da CCS, que deverá prestar contas, demonstrar diligência e ressarcir eventuais violações ou inobservância aos termos da LGPD.
Essa cartilha não se destina a esgotar o tema e/ou substituir as políticas, termos, contratos, normativas e orientações emitidas pela CCS.

Protocolo –Assinatura do colaborador

Eu_____
_____, colaborador da CCS com o número de matrícula _____, declaro que li e compreendi as informações constantes na cartilha sobre a Lei Geral de Proteção de Dados.

Data: _____

Assinatura: _____

Via da CCS

LGPD