CARTILHA DE PROTEÇÃO DE DADOS

ABRAREC
Associação Brasileira das Relações Empresa Cliente

LTSA advogados

COMUNICADO[1]

A ABRAREC, associação sem fins lucrativos, preocupada em proporcionar as empresas à possibilidade de aprimorar seu relacionamento com o cliente, identificou na Lei Geral de Proteção de Dados (L. n° 13.709/18) uma grande oportunidade para o setor de relacionamento com o cliente, considerando seu potencial de agregar maior transparência e honestidade nas relações entre clientes e empresas.

Em face disso, a ABRAREC, com a assistência da equipe de Direito Digital do escritório LTSA Advogados, tem se empenhado de forma ativa a fomentar constantes debates em eventos sobre a necessidade da devida aplicação das disposições da LGPD, buscando através disso, a criação de uma cultura entre os associados de garantia da proteção de dados e privacidade de seus clientes.

Diante disso, considerando o encontro entre os interesses da ABRAREC e seus associados e visando contribuir de forma positiva com a implementação da LGPD nos processos do setor de relacionamento entre empresas e clientes, a ABRAREC em conjunto com o LTSA advogados elaborou a presenta cartilha sobre a Lei Geral de Proteção de Dados no Brasil.

Dionísio Moreno
Presidente

Vitor Morais de Andrade
Conselheiro Jurídico

[1]Cartilha elaborada em 10/06/2019, data anterior a sanção e publicação do Projeto de Lei de Conversão n.7/2019, proveniente da Medida Provisória 869/2018.

INTRODUÇÃO

A transformação da sociedade, com a incorporação da tecnologia, deixou em evidência o real valor de nossos dados e, principalmente, a importância do posicionamento das empresas em relação a esses dados.

Frente a isso, após anos de debates, finalmente, depois do início da vigência, em maio de 2018, do Regulamento Geral de Proteção de Dados (General Data Protection Regulation – GDPR), da União Europeia, foi sancionada a Lei Geral de Proteção de Dados, que dispõe sobre a proteção de dados pessoais no Brasil.

Com isso, evidente se tornou a necessidade de as empresas brasileiras priorizarem a forma correta de coleta, tratamento e o armazenamento desses dados, em respeito aos seus titulares.

No setor de relacionamento entre cliente e empresa, não será diferente, a necessidade urgente de adaptação deverá ser prioritária. As empresas e áreas de relacionamento por gerirem diretamente uma grande quantidade de dados de clientes para atendimento de suas solicitações, tendem a formar bancos de dados de larga escala, podendo configurar risco diante das exigências da nova legislação.

E apesar de a LGPD ter sua vigência prevista para agosto de 2020, as mudanças necessárias são implicam em uma mudança cultural, de modo que não há tempo a ser perdido. Assim, o quanto antes as mudanças forem implementadas, melhor será o aproveitamento do seu processo de adaptação.

Com o intuito de orientar seus associados e auxiliá-los nesta mudança significativa, a ABREREC buscou, de forma objetiva, através da presente Cartilha apresentar os principais pontos sobre a Lei Geral de Proteção de Dados, sob o enfoque do relacionamento entre empresas e clientes.

A QUEM SE APLICA A LGPD?

A LGPD se aplica a toda empresa e área que realiza qualquer operação de tratamento de dados (ex. coleta, aquisição, manutenção, compartilhamento, exclusão de dados pessoais) realizada em território nacional ou de indivíduos localizados no território nacional, independentemente de meio utilizado para tanto, do país da sede da empresa ou do país onde estejam localizados os dados.

Ou seja, você empresa que se utiliza de dados, seja para comércio, seja para controle interno, como no caso dos recursos humanos, ou até mesmo para atendimento ao cliente, está sujeita a LGPD, e, portanto deve estar em conformidade até agosto de 2020.

Apesar da complexidade do processo de adequação, este é um cenário de oportunidades, em que as empresas adequadas possuirão o diferencial de ofertar produtos e serviços modelados de forma a atender a privacidade, além de a oferta ser realizada de forma não intrusiva e incômoda ao consumidor. Ademais, a garantia aos direitos dos titulares por meio do relacionamento com os clientes demonstrarão a estes que a privacidade e proteção de dados é um valor da empresa, trazendo segurança e confiabilidade às relações destas.

QUAIS SÃO OS PRINCÍPIOS QUE EMBASAM TODO O TEXTO DA LGPD?

A LGPD apresenta em seu escopo os princípios norteadores das atividades de tratamento de dados pessoais, totalizando 10 (dez) princípios (art. 6°, LGPD). São eles:

INCISO	PRINCÍPIO	DEFINIÇÃO
I	**Finalidade**	Realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades. Ex.: se a empresa coleta dados para fins de atendimento, caso pretenda se utilizar destes para outros fins, como campanhas de marketing, faz-se necessário, novo consentimento, em caso de esta finalidade não ter sido anteriormente informada.
II	**Adequação**	Compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento. Ex: se a empresa informar que apenas coletará dados para atendimento, deverá se ater ao ajustado, sem desvios de finalidade.
III	**Necessidade**	Limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados. Ex: se a empresa coletar dados para fins de atendimento, mostra-se pertinente, por exemplo, a solicitação de meios de contato, como e-mail e telefone, a fim de que seja dado retorno ao cliente acerca do tratamento da demanda. Dados não pertinentes, devem ser descartados ou não armazenados.

QUAIS SÃO OS PRINCÍPIOS QUE EMBASAM TODO O TEXTO DA LGPD?

INCISO	PRINCÍPIO	DEFINIÇÃO
IV	Livre Acesso	Garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais. O proprietário do dado é o titular, de forma que a este deve ser dado conhecimento acerca dos dados mantidos a respeito de si.
V	Qualidade dos dados	Garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento
VI	Transparência	Garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial. Cuidado: políticas extensas e que demandem diversos clicks do usuário para conhecimento de como seus dados são tratados não são consideradas transparentes!!
VII	Segurança	Utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. Não poderá haver lacunas de segurança ao longo do ciclo de dados (coleta/tratamento/exclusão), considere investir em segurança e conscientização.
VIII	Prevenção	Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais. Paute sua empresa pela prevenção, e não, pela reparação.

QUAIS SÃO OS PRINCÍPIOS QUE EMBASAM TODO O TEXTO DA LGPD?

INCISO	PRINCÍPIO	DEFINIÇÃO
IX	Não discriminação	Impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos. Cuidado com as discriminações realizadas pelos algoritmos.
X	Responsabilização e Prestação de Contas	Demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas. Ex: se a sua empresa coleta dados por meio do opt-in, faz-se necessário comprová-lo, guarde seus registros!

QUAIS AS BASES LEGAIS/HIPÓTESES PARA TRATAMENTO DE DADOS?

A LGPD parte de uma premissa básica, de que os dados pessoais pertencem ao indivíduo, e por isso, sua utilização deve necessariamente se ater a propósitos legítimos, criando assim, a obrigação da empresa somente realizar o tratamento dos dados para finalidade específica informada ao titular dos dados no momento de sua coleta.

Nesse sentido, a LGPD estabelece que a coleta e tratamento de dados somente poderá ser realizado se fundada em alguma das bases legais listada abaixo (artigo 7°, LGPD), do contrário o tratamento será considerado ilícito:

- consentimento (escrito ou por meio que demonstre a vontade do titular);
- cumprimento de obrigação legal (ex: obrigação de manutenção de gravação de atendimento, pelo prazo mínimo de 90 dias, pelas empresas que devem cumprir com o Decreto do SAC – Dec. 6.523/08);
- necessidade para execução contratual;
- exercício regular de direitos em processo judicial, administrativo ou arbitral;
- realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- proteção à vida ou incolumidade física do titular ou de terceiro;
- para a tutela da saúde;
- para atender a legítimo interesse do controlador (quem exerce poder de decisão sobre o tratamento dos dados) ou terceiro (ex. a fraude é considerada como legítimo interesse pelo GDPR);
- para a proteção de crédito; e,
- em razão da publicidade dada aos dados por seu titular ou do acesso público irrestrito a este, desde que observados a finalidade com que o dado fora disponibilizado, a boa-fé e não fira direitos e garantias fundamentais.

E OS DIREITOS DOS TITULARES? HAVERÁ ALGUM IMPACTO EM MEU NEGÓCIO?

Os dados coletados são de propriedade de seus titulares, por isso, visando dar maior transparência a relação e buscando resguardar esses titulares, a LGPD instituiu em seu artigo 18 um rol de direitos, impondo a obrigação ao controlador dos dados de garantir o cumprimento dos pedidos, em caso de solicitação.

Fazem parte dos direitos dos titulares os seguintes:

- Confirmação da existência do tratamento;
- Acesso aos dados;
- Correção de dados;
- Anonimização, bloqueio e eliminação de dados;
- Portabilidade de dados;
- Informação sobre compartilhamento de dados pessoais;
- Informação sobre a possibilidade em não consentir com o tratamento e as consequências da negativa;
- Possibilidade de revogar o consentimento.

A empresas controladoras dos dados, aquelas que decidem efetivamente sobre o tratamento de dados, devem disponibilizar um canal de atendimento para que o titular de dados possa realizar as solicitações já elencadas. A Lei não exige formato específico a este canal e nem que seja este exclusivo para tais solicitações.

Em suma, as empresas deverão informar aos titulares o rol de direitos e serem capazes de atender a todos os pedidos enquadrados dentro dos direitos dos titulares dos dados, principalmente no que cerne ao pedido de exclusão de dados.

E NO CASO DE DESCUMPRIMENTO DA LGPD?

Caso a empresa não consiga se adequar a tempo, ficará a mercê da fiscalização, e consequentemente se sujeitará a LGPD em seu artigo 52, que enumera as seguintes sanções administrativas aplicáveis[2]:

Advertência: com indicação de prazo para adoção de medidas corretivas;

Multa: multa simples ou diária de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, limitada, no total, a R$ 50.000.000,00, por infração.

Publicização: publicização da infração após sua apuração e confirmação de ocorrência, possibilidade de sanção em caso de vazamento de dados pessoais.

Bloqueio dos dados: a que se refere a infração até a sua regularização.

Eliminação dos dados: a que se refere a infração.

Lembrando que a aplicação das sanções será precedida de procedimento administrativo, dando a oportunidade de ampla defesa, de acordo com as peculiaridades do caso concreto (art. 52, §1°, LGPD).

[2]Se o Projeto de Lei de Conversão n.7/2019 for sancionado e publicado como aprovado no Congresso Nacional, poderão serincluídos no rol de sanções da Autoridade Nacional de Proteção de Dados (ANPD) : (i) suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; (ii) suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; e (iii) proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados (art. 52, X, XI, XII)

QUEM PODERÁ APLICAR AS SANÇÕES LEGAIS?

A princípio, a LGPD fora publicada com vetos nos artigos 55 a 59 referentes a criação da Autoridade Nacional de Proteção de Dados (ANPD)[3], sem que, contudo, fossem excluídas as demais disposições que tratavam da ANPD, gerando como resultado, um clima de insegurança jurídica quanto a aplicação da Lei.

Contudo, após quase seis meses da LGPD, em 28 de dezembro de 2018, foi publicada a Medida Provisória 869/2018, que alterou alguns dos dispositivos da LGPD e criou a ANPD. E apesar de tratar de algumas lacunas, e principalmente, por tratar da criação do responsável pelo monitoramento do cumprimento da LGPD, a Medida Provisória ainda se encontra em tramitação.

Se sancionado o Projeto de Lei de Conversão n.7/2019, proveniente da Medida Provisória 869/2018, a Autoridade Nacional de Proteção de Dados será instituída como órgão da administração pública federal, integrante da Presidência da República.

COMO MINHA EMPRESA DEVE ADEQUAR?

Apresentados todos esses requisitos, permanece a dúvida, como posso tornar minha empresa *compliance* com a LGPD? Pois bem, considerando o início da vigência em agosto de 2020, necessário que as empresas priorizem a criação de um cronograma de adequação, abordando todas as obrigações impostas pela LGPD e criando ferramentas capazes de garantir o cumprimento da legislação.

Portanto, quanto mais cedo se iniciar o processo de *compliance*, maiores as chances de conseguir se adequar a LGPD a tempo. Nesse sentido, seguem algumas sugestões de ações para adaptação:

- Identificar e mapear todos os fluxos de dados, em sua integralidade (coleta, tratamento, compartilhamento, exclusão);
- Elaborar Relatório de Impacto de Proteção de Dados;
- Utilização de medidas técnicas aptas a proteger os dados de acessos não autorizados, situações acidentais ou ilícitas (art.6º e 46, LGPD);
- Criar procedimento para casos de vazamento/violação de dados;
- Somente realizar tratamento de dados pessoais frente a uma das hipóteses/bases legais (art.7º, LGPD);
- Restringir-se, a somente realizar o tratamento de dados para finalidade determinada pelo qual o dado fora compartilhado pelo titular (art.6º, LGPD);
- Possuir documentação eficaz e capaz de comprovar a observância e cumprimento das normas de proteção de dados pessoais (art.6º, LGPD);
- Não realização de tratamento para fins discriminatórios ilícitos ou abusivos (art.6º LGP);
- Caso a empresa seja classificada como "controladora", a nomeação de um encarregado pelo tratamento de dados pessoais torna-se obrigatória (art.41, LGPD);

COMO MINHA EMPRESA DEVE ADEQUAR?

Ser capaz de informar e garantir os direitos dos titulares (art. 18, LGPD);

- Escolher somente parceiros com o nível adequado de proteção de dados pessoais;
- Formular regras de boas práticas e governança sobre proteção de dados pessoais (art.50, LGPD).

No mais, pensando no setor de relacionamento com o cliente, reunimos um breve checklist com aspectos relevantes da LGPD que possuirão impacto imediato no setor.

Para cadastro de pedido ou reclamação, muito provavelmente deve o cliente apresentar alguns dados. Dos dados solicitados, são todos eles realmente necessários para o atendimento do pedido?

É cotidiano que as empresas possuam um formulário padrão a ser preenchido em ordem de possibilitar o protocolo da solicitação do cliente. Contudo, é necessário se atentar aos dados coletados, caso não haja real necessidade na coleta, é sempre aconselhável que não se colete o dado. Os bancos de dados devem possuir sua finalidade e base legal bem definidas, o que impossibilita a classificação de dados coletados sem nenhum uso específico, ferindo o disposto na LGPD, e gerando um risco desnecessário.

Nesse caso, recomenda-se a aplicação do modelo de *privacy by default*[1], buscando preservar ao máximo a privacidade do cliente, coletando e tratando somente os dados estritamente necessários, e buscando dessa forma minimizar o processamento de dados pessoais.

[1] GDPR. Art.25, (2) "O responsável pelo tratamento aplica medidas técnicas e organizativas para assegurar que, por padrão, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento. Essa obrigação aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade. Em especial, essas medidas asseguram que, por padrão, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares".

Ainda sobre esses dados coletados, são eles dados pessoais ou sensíveis?

A LGPD faz uma diferenciação em sua definição, e consequentemente, de suas obrigações, sendo dessa forma, de extrema importância ter conhecimento sobre os tipos de dados coletados.

Enquanto o dado pessoal engloba qualquer dado que esteja relacionada a um indivíduo ou que possibilite a identificação de um indivíduo (art. 5, I, LGPD), o dado pessoal sensível, trata de um gênero do dado pessoal, que sejam relativos especificamente a 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, LGPD).

Sua distinção é importante posto que, **em caso da necessidade indispensável de coleta de dados sensíveis para atendimento da solicitação, deve a empresa se atentar a base legal com que o faz, sendo necessário reforçar a recomendação da necessidade de registro do consentimento, específico e destacado, nesses casos (art. 11, LGPD).**

Em atendimento de pedido do cliente, qual a base legal utilizada para a utilização dos dados coletados?

Conforme já enumerado, são 10 (dez) as bases legais para embasamento da coleta e tratamento de dados pessoais. No caso do atendimento ao cliente, considerando ser, pela sua interação ativa, dele o interesse no atendimento, possível o enquadramento do tratamento de dados como cumprimento de obrigação contratual ou legal.

Contudo, caso os dados sejam utilizados futuramente, para contato não diretamente solicitado pelo cliente, deve aloca-lo em outra base, seja legítimo interesse, no caso de abordagem do cliente para, por exemplo, promoção de atividades do controlador.

No caso do tratamento de dados pessoais sensíveis, as bases legais mudam, fique atento para somente fazê-lo, sob pena de descumprimento da Lei, **mediante**: (i) consentimento específico e em destaque; (ii) obrigação legal; (iii) exercício regular de um direito; (iv) proteção à vida ou incolumidade física do titular ou de terceiro; (v) para a tutela da saúde; (vi) garantia de prevenção à fraude e segurança do titular. (art.11, LGPD). Assim, **no caso do atendimento de pedido de cliente**, que necessite do compartilhamento de dados sensíveis, **necessário que seja recolhido o consentimento específico e em destaque do titular do dado, independente, do interesse pelo primeiro contato realizado por ele.**

Você se utiliza de algum sistema de CRM (Customer Relationship Management)? Caso positivo, existe no sistema alguma configuração da interface para coleta de consentimento?

A utilização de sistema de CRM busca facilitar o gerenciamento do relacionamento entre o cliente e a empresa, sendo nesse caso, muito prática e principalmente, repleta de dados pessoais.

Considerando esse contexto, devem as empresas buscar no momento da customização de sua ferramenta, se atentar ao modelo Privacy by Design, para o desenvolvimento de plataformas que cumpram com os requisitos legais impostos pela LGPD para coleta e tratamento dos dados pessoais.

Implementando formas de coleta e registro de consentimento, por exemplo, no caso da necessidade de coleta de dados sensíveis para atendimento de solicitação de cliente, ou ferramentas de cadastro de opt-out dos clientes que possuam integração com o banco de dados de outras áreas e fornecedores.

Em casos de plataformas online de interação com os clientes, como sites ou plataformas de e-commerce, devo alguma satisfação ao usuário-cliente pela utilização de cookies neste ambiente?

Em face do princípio da transparência, deve a empresa sempre comunicar ao seu usuário no caso de coleta de seus dados, independente do meio utilizado.

Assim, considerando que dado pessoal é toda informação que esteja relacionada a um indivíduo ou que possibilite a sua identificação, é possível concluir, que ao reunir informações sobre meu acesso, o cookie traça um perfil de navegação que possibilita a identificação do usuário.

Portanto, necessário, para cumprimento do disposto na LGPD e demais legislações sobre o tema, que a comunicação da coleta de dados por cookie seja efetiva, simples, e que sempre ofereça a opção de recusa da coleta.

A sua empresa está habilitada para atender todos os direitos dos titulares?

Os direitos dos titulares tratam das obrigações impostas aos controladores de dados, como forma de garantir transparência e demonstrar para os titulares dos dados como seus dados estão sendo utilizados.

Nesse aspecto, de todos os pontos de mudança que a LGPD impõe para as áreas de relacionamento com o cliente, a garantia dos direitos dos titulares é fundamentalmente a mais relevante. Posto que será necessariamente através desse canal de comunicação que os titulares, após adquirirem o conhecimento sobre seus direitos, irão naturalmente realizar suas solicitações.

Desta foram, devem estar as empresas atentas a necessidade de integração de todas as áreas na cadeia, posto que, se por exemplo um cliente solicitar a exclusão de todos os seus dados da base de dados da empresa, deve ser o atendimento, capaz de realiza-lo ou pelo menos ser capaz de transferir o pedido para as áreas responsáveis, garantindo que o pedido seja cumprido.

E no caso de incidente de segurança da informação? Existe um procedimento de emergência?

No caso de incidente de segurança da informação que possa acarretar risco ou dano relevante aos titulares, deve o controlador comunicar à Autoridade Nacional e ao titular da ocorrência em prazo razoável, e deverá mencionar, no mínimo: (i) a descrição da natureza dos dados pessoais afetados, com informações sobre os titulares envolvidos; (ii) a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados; (iii) os riscos relacionados ao incidente; e (iv) as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo (art. 48, §1°, LGPD).

A LGPD não traz explicitamente o significado de tempo razoável para notificação, contudo, a GDPR estabelece em seu escopo a obrigação de comunicação em até 72 horas, o que poderia ser utilizado como parâmetro diante de tal lacuna de regulamentação.

Caso a empresa atue como operadora, e identifique eventual incidente de segurança, deverá notificar o controlador a respeito do incidente, devendo este possuir documentação referente notificação para eventual prestação de contas à ANPD.

A Autoridade Nacional verificará a gravidade do incidente, e poderá determinar ao controlador a adoção de providências, como: (i) ampla divulgação do fato em meios de comunicação; e (ii) medidas para reverter ou mitigar os efeitos do incidente (art. 48, §2°, LGPD).

Buscando facilitar a leitura da lei, imprescindível repassar alguns conceitos básicos, dos quais se encontram listados no artigo 5º da LGPD.

Dados pessoais: Nos termos da LGPD, dado pessoal é toda informação que esteja relacionada a um indivíduo ou que possibilite a sua identificação, definição que seguiu os padrões da GDPR. São exemplos de dados pessoais RG, CPF, profissão, entre outros dados que permitam a identificação de uma pessoa.

Dados pessoais sensíveis: Já o dado pessoal sensível, é uma categoria especial de dado pessoal instituída pela LGPD, que tratam 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.

Tratamento de dados: Conforme determina a LGPD, o tratamento de dados se resume a todo tipo de atividade relacionada a dados, ou seja, 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, LGPD).

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (art. 5, VII, LGPD).

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (art. 5, VI, LGPD).

Privacy by design: trata do modelo de incorporação de mecanismos de privacidade durante todo o ciclo do dado utilizado. É incorporar a privacidade ao desenho do produto ou serviço, protegendo todo o ciclo do dado e concedendo-lhe proteção de ponta a ponta.