As Ouvidorias e a Lei Geral de Proteção de Dados Pessoais (LGPD ou LGPDP) - Lei 13.709/18

Abril 2019

Contexto

- Pizzaria Google, boa noite! ?
– De onde falam?
– Pizzaria Google, senhor. Qual é o seu pedido?
– Mas este telefone não era da Pizzaria do…
– Sim senhor, mas a Google comprou a Pizzaria e agora sua pizza é mais completa.
– OK. Você pode anotar o meu pedido, por favor?
– Pois não. O Senhor vai querer a de sempre?
– A de sempre? Você me conhece?
– Temos um identificador de chamadas em nosso banco de dados, senhor. Pelo que temos registrado aqui, nas últimas 53 vezes que ligou, o senhor pediu meia quatro queijos e meia calabresa.
– Puxa, eu nem tinha notado! Vou querer esta mesmo…
– Senhor posso dar uma sugestão?
– Claro que sim. Tem alguma pizza nova no cardápio?
– Não senhor. Nosso cardápio é bem completo, mas eu gostaria de sugerir-lhe meia ricota, meia rúcula.
– Ricota??? Rúcula??? Você ficou louco? Eu odeio estas coisas.
– Mas, senhor, faz bem para a sua saúde. Além disso, seu colesterol não anda bom…
– Como você sabe?
– Nossa Pizzaria tem o banco de dados mais completo do planeta. Nós temos o banco de dados do laboratório em que o senhor faz exames também. Cruzamos seu número de telefone com seu nome e temos o resultado dos seus exames de colesterol. Achamos que uma pizza de rúcula e ricota seria melhor para sua saúde.
– Eu não quero pizza de queijo sem gosto e nem pizza de salada. Por isso tomo meu remédio para colesterol e como o que eu quiser…
– Senhor me desculpe, mas acho que o senhor não tem tomado seu remédio ultimamente.
– Como sabe? Vocês estão me vigiando o tempo todo?
– Temos o banco de dados das farmácias da cidade. A última vez que o senhor comprou seu remédio para Colesterol faz 3 meses. A caixa tem 30 comprimidos.
– Poxa! É verdade. Como vocês sabem disto?
– Pelo seu cartão de crédito…
– Como?!?!?
– O senhor tem o hábito de comprar remédios em uma farmácia que lhe dá desconto se pagar com cartão de crédito da loja. E ainda parcela em 3 vezes sem acréscimo… Nós temos o banco de dados de gastos com cartão na farmácia. Há dois meses o senhor não compra nada lá, mas continua usando seu cartão de crédito em outras lojas, o que significa que não o perdeu, apenas deixou de comprar remédios.

– E eu não posso ter pagado em Dinheiro? Agora te peguei…
– O senhor não deve ter pagado em dinheiro, pois faz saques semanais de R$ 250,00 para sua empregada doméstica.
Não sobra dinheiro para comprar remédios. O restante o senhor paga com cartão de débito.
– Como você sabe que eu tenho empregada e quanto ela ganha?
– O senhor paga o INSS dela mensalmente com um DARF. Pelo valor do recolhimento dá para concluir que ela ganha R$ 1.000,00 por mês. Nós temos o banco de dados dos Bancos também. E pelo seu CPF…
– ORA VÁ SE DANAR!
– Sim senhor, me desculpe, mas está tudo em minha tela. Tenho o dever de ajudá-lo. Acho, inclusive, que o senhor deveria remarcar a consulta que o senhor faltou com seu médico, levar os exames que fez no mês passado e pedir uma nova receita do remédio.
– Por que você não vai à m….???
– Desculpe-me novamente, senhor.
– ESTOU FARTO DESTAS DESCULPAS. ESTOU FARTO DA INTERNET, DE COMPUTADORES, DO SÉCULO XXI, DOS BANCOS DE DADOS, DA FALTA DE PRIVACIDADE E DESTE PAÍS…
– Mas senhor…
– CALE-SE! VOU ME MUDAR DESTE PAÍS PARA BEM LONGE. VOU PARA AS LHAS FIJI OU ALGUM LUGAR QUE NÃO TENHA INTERNET, TELEFONE, COMPUTADORES E GENTE ME VIGIANDO O TEMPO TODO…
– Sim, senhor…entendo perfeitamente.
– É ISTO MESMO! VOU ARRUMAR MINHAS MALAS AGORA E AMANHÃ MESMO VOU SUMIR DESTA CIDADE.
– Entendo…
– VOU USAR MEU CARTÃO DE CRÉDITO PELA ÚLTIMA VEZ E COMPRAR MA PASSAGEM SÓ DE IDA PARA ALGUM LUGAR BEM LONGE DE VOCÊ !!!
– Perfeitamente…
– E QUERO QUE VOCÊ ME ESQUEÇA!
– Farei isto senhor… …(breve silêncio)
– O senhor está aí ainda?
– SIM, POR QUÊ? ESTOU PLANEJANDO MINHA VIAGEM… E PODE CANCELAR MINHA PIZZA.
– Perfeitamente. Está cancelada. …(mais um breve silêncio) – Só mais uma coisa, senhor…
– O QUE É AGORA?
– Devo lhe informar uma coisa importante…
– FALE!
– O seu passaporte está vencido.

Em março de 2018, os jornais *The New York Times* e *The Observer* noticiaram que a Cambridge Analytica usou informações pessoais de 50 milhões de perfis do Facebook, que foram obtidas por um pesquisador externo. O jornal *The Guardian* informou que o Facebook tinha conhecimento que essa violação de segurança aconteceu por dois anos, mas não fez nada para proteger seus usuários.

Em abril do mesmo ano o Facebook anunciou que as contas de pelo menos 87 milhões de pessoas foram atingidas em 10 países, e, segundo suas estimativas, os dados pessoais de 43 117 brasileiros foram usados sem consentimento prévio. Nos Estados Unidos foram atingidas mais de 70 milhões de pessoas.

Em 18 de maio de 2018, a empresa registrou seu pedido de falência na Corte de Falências do Distrito Sul de Nova York (Fonte: wikipedia).

PETROBRAS

Dados de milhões de usuários do Facebook foram encontrados expostos publicamente em servidores de computação de nuvem da Amazon, alertaram nesta quarta-feira pesquisadores da empresa de cibersegurança UpGuard. A descoberta mostra que, um ano após o escândalo de uso de dados de membros da rede social pela consultoria Cambridge Analytica, as informações pessoais continuam desprotegidas e disseminadas pela internet. (Fonte: O Globo, por Carla Arede)

NP-1

Estrutura

A Lei, promulgada em 14 de agosto de 2018, possui 10 capítulos e 65 artigos. O texto foi inspirado na regulação europeia (GDPR - General Data Protection Regulation).

Começa a vigorar, nos termos da MP nº869/2018, em agosto de **2020**.

Qualificação dos Tipos de Dados

DADOS PESSOAIS

- Nome
- Endereço de residência
- E-mail
- Dados de Conexão (Cookies, IP, Histórico, etc.)

DADOS SENSÍVEIS

- Origem Racial
- Religião
- Posicionamento Político
- Filiação a sindicato
- Dado referente à saúde ou à vida sexual
- Dado genético ou biométrico

DADOS NÃO PESSOAIS

- Número de registo de empresa
- Endereço eletrônico de empresa
- Dados anônimos

Na LGPD o consentimento é a regra.

E sua dispensa, a exceção.

Privacy by Design

Medologia de “privacidade desde a concepção”

Critérios para uso de Dados Pessoais

sem o consentimento do titular

Para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais

Para a realização de estudos por órgão de pesquisa, sem a individualização a pessoa

Para execução de contrato ou procedimentos preliminares relacionados a um contrato

Para a proteção do crédito, nos termos do Código de Defesa do Consumidor

Para a proteção da vida ou da integridade física do titular ou terceiro

Pela administração pública, para o uso compartilhado de dados necessários à execução de políticas públicas

Para o cumprimento de obrigação legal ou regulatória pelo responsável pelo tratamento

Para o exercício regular de direitos em processos judicial, administrativo ou arbitral

Para a tutela da saúde, com procedimento realizado por profissionais da área ou por entidades sanitárias

NP-1

Pontos Importantes

Abrangência
Quaisquer dados pessoais obtidos em qualquer tipo de suporte (papel, eletrônico, informático, som, imagem, etc.)

Vigência
A vacatio legis fixado na promulgação era de 18 meses. Contudo, a MP 869/18 postergou para 24 meses.

Contratos de adesão
Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou serviço, o titular deverá ser claramente informado

Sansões administrativas
Em caso de descumprimento das regras previstas pela LGPD, serão aplicadas sanções a exemplo de advertências ou multas, as quais poderão variar de 2% do faturamento da empresa, grupo ou conglomerado no Brasil, limitada a R$ 50.000.000,00 (cinquenta milhões de reais) por infração.

Dados sensíveis
O texto traz o conceito de dados sensíveis, cujo processamento deve ser realizado quando o consentimento for livre, inequívoco, informado e específico

Responsabilidade civil
O responsável que, em razão do exercício de atividade de tratamento de dados, causar a dano patrimonial, moral, individual ou coletivo, é obrigado a reparar

Pontos Importantes

Direitos do titular dos dados
O titular dos dados pessoais tem direito a obter acesso, correção, eliminação, portabilidade, etc. (art. 18), **nos prazos e nos termos previstos em regulamento**

Direitos do titular dos dados
A confirmação de existência ou o acesso a dados pessoais serão em formato simplificado imediatamente ou
em até 15 (quinze) dias

Dados sensíveis
O controlador deverá indicar encarregado pelo tratamento de dados pessoais. A identidade e as informações de contato do encarregado deverão ser divulgadas
publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador

Conservação dos dados
Os dados pessoais serão eliminados após o término de seu tratamento, autorizada a conservação para cumprimento de obrigação legal ou regulatória pelo controlador

Controlador e operador
O controlador (pessoa diretamente responsável pelos dados pessoais) e o operador (pessoa responsável pelo tratamento dos dados pessoais) devem manter registro das operações de tratamento de dados pessoais que realizarem (operação por terceiro). Deverão comunicar casos de "incidentes de segurança", como vazamentos

Regras
As empresas públicas e as sociedades de economia mista que atuam em regime de concorrência terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares

NP-1

Ponto I

VIII - 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; (Redação dada pela Medida Provisória nº 869, de 2018)

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

§ 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

§ 2º As atividades do encarregado consistem em:

I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II - receber comunicações da autoridade nacional 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 pelo controlador ou estabelecidas em normas complementares.

§ 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.

Juntando outros pontos importantes...

Lei 12.527/11 – art. 40:
III - recomendar as medidas indispensáveis à implementação e ao aperfeiçoamento das normas e procedimentos necessários ao correto cumprimento do disposto nesta Lei; e
IV - orientar as respectivas unidades no que se refere ao cumprimento do disposto nesta Lei e seus regulamentos.

Lei 13460/17 – art. 13:
II - acompanhar a prestação dos serviços, visando a garantir a sua efetividade;
III - propor aperfeiçoamentos na prestação dos serviços;
VI - receber, analisar e encaminhar às autoridades competentes as manifestações, acompanhando o tratamento e a efetiva conclusão das manifestações de usuário perante órgão ou entidade a que se vincula; e

Lei 13709/18 - **art. 41:**

I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
II - receber comunicações da autoridade nacional 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;

Ouvidor como Encarregado, ao menos, preferencialmente.

NP-1

Encaminhamentos

Programa de Implementação da LGPD

1. Sensibilização e patrocínio da Alta Direção
2. Definição do Encarregado pelo Tratamento de Dados Pessoais
3. Criação de Comissão (Grupo de Trabalho) de Proteção de Dados Pessoais
3.1. Capacitação dos participantes da Comissão de Proteção de Dados Pessoais
3.2. Levantamento de Processos que tratam Dados Pessoais
3.2.1. Mapeamento dos Dados Pessoais
3.2.2. Mapeamento dos Fluxos de Dados
3.3. Identificação do propósito de coleta de dados
3.3.1. Enquadramento do dado/propósito com base legal de legitimação
3.3.2. Obtenção e Gestão de Consentimentos RH, SMS, TIC, SBS e Outras Un.
3.4. Estruturação de suporte sistêmico (inclui, definição equipe) para atender aos requerimentos do Programa de Proteção de Dados Pessoais
3.5. Realização de Análise de Risco
3.5.1. Identificação e criação de ações mitigadoras de riscos
3.6. Cronograma de implementação/adequação de processos para comunicação / tratamento de incidentes de privacidade
3. 7. Criação de Políticas de Privacidade e de Retenção de Dados Privados
3.8. Criação de processo para Análise Periódica da Necessidade de Coleta e Tratamento de Dados Pessoais
3.9. Criação de Indicadores de Conformidade para Controlador e Operador
3.10.Disponibilização serviços aos Titulares de Dados

Sugestão de consulta: Programa de Protección de Datos - Documento Orientador: http://inicio.inai.org.mx/SitePages/Documentos-de-Interes.aspx?a=m4

7 passos – Recomendações União Europeia

STEP 1 – CHECK THE PERSONAL DATA YOU COLLECT AND PROCESS, THE PURPOSE FOR WHICH YOU DO IT AND ON WHICH LEGAL BASIS

You have **employees**, you are processing their personal data based on the employment contract and based on legal obligations (e.g. reporting to tax authorities / social system).

You can manage a list of **individual customers**, for instance to send them notice about special offers/adverts if you obtained consent from these customers.

You don't always need consent. There are cases when individuals will expect you to process their data. For instance, as a pizza merchant you can process the delivery address to advertise one of your new products. This is called a 'legitimate interest'. You must inform individuals about your intended use and stop processing such data if they tell you to do so.

If you manage a list of **suppliers** or **business clients**, then you do it based on the contracts you have with them. The contracts are not necessarily in a written form.

STEP 2 – INFORM YOUR CUSTOMERS, EMPLOYEES AND OTHER INDIVIDUALS WHEN YOU COLLECT THEIR PERSONAL DATA

Individuals must know that you process their personal data and for which purpose.

But there is no need to inform individuals when they already have information on how you will use the data, for instance, when a customer asks you to do a home delivery.

You also have to inform individuals on request about the personal data you hold on them and give them access to their data. Keep your data in order, so when e.g. your employee asks you about what sort of personal data you have, you can provide it easily with no extra hassle.

STEP 3 – KEEP THE PERSONAL DATA FOR ONLY AS LONG AS NECESSARY

Data on your employees: as long as the employment relationship and related legal obligations.

Data on your customers: as long as the customer relationship lasts and related legal obligations (for instance for tax purposes).

Delete the data where it is no longer necessary for the purposes for which you collected it.

STEP 4 – SECURE THE PERSONAL DATA YOU ARE PROCESSING

If you store this data on an **IT system**, limit the access to the files containing the data, e.g. by a password. Regularly update the security settings of your system.

(Note: the GDPR does not prescribe the use of any specific IT system)

If you store physical documents with personal data, then ensure that they are not accessible by unauthorised persons, lock them in safe or a cupboard.

STEP 5 – KEEP DOCUMENTATION ON YOUR DATA PROCESSING ACTIVITIES

Prepare a short document explaining what personal data you hold and for what reasons. You might be required to make the documentation available to your national data protection authority when it requests it.

Such documents should include the information listed below.

INFORMATION	EXAMPLES
The purpose of data processing	Alerting customers about special offers / providing home delivery, paying suppliers; salary and social security cover for employees
The types of personal data	Contact details of customers; contact details of suppliers; employees' data
The categories of data subjects concerned	Employees; customers; suppliers
The categories of recipients	Labour authorities; tax authorities
The storage periods	Employees' personal data until the end of the employment contract (and related legal obligations); customers' personal data until the end of the client/contractual relationship
The technical and organisational security measures to protect the personal data	IT system solutions regularly updated; locked cupboard/safe
Whether personal data is transferred to recipients outside the EU	Use of a processor outside the EU (e.g. for storage in the cloud)

STEP 6 – MAKE SURE YOUR SUB-CONTRACTOR RESPECTS THE RULES

If you sub-contract processing of personal data to another company, use only a service provider who guarantees the processing in compliance with the requirements of the GDPR (for instance security measures). Before you sign a contract, check if they have already changed and adjusted to the GDPR. Put it in the contract.

STEP 7 – CHECK IF YOU ARE CONCERNED BY THE PROVISIONS BELOW

> To better protect personal data, organisations might have to appoint a Data Protection Officer (DPO). **However, you don't need to designate a Data Protection Officer** if processing of personal data isn't a core part of your business, is not a risky processing and your activity isn't at a large scale;

For example, if your business only collects data on your customers for home delivery, you do not need to appoint a DPO.

Even if you need to make use of a DPO, he/she could be an existing employee tasked with this function in addition to his/her other tasks. Or it could be an external consultant; the same way many organisations use external accountants.

> **You normally don't need to carry out a Data Protection Impact Assessment**

Such an impact assessment is reserved for those that pose more risk to personal data, for instance they do a large-scale monitoring of a publicly accessible area (e.g. video-surveillance).

If you are a small business managing employees' wages and a list of clients, you do not need to carry out a Data Protection Impact Assessment for those processing operations.

Fines

The data protection supervisory authorities are empowered to sanction infringements of the data protection rules. They can adopt corrective measures (such as an order or a temporary suspension of the processing) and/or impose a fine.

Their decision to impose a fine must be proportionate and based on an assessment of all the circumstances of the individual case.

If they decide to impose a fine, the amount of the fine will also depend on the circumstances of the case, including the gravity of the infringement or if the infringement was intentional or negligent. They will also take your attitude and intentions into account.

STEP 1 CHECK THE PERSONAL DATA YOU COLLECT AND PROCESS, THE PURPOSE FOR WHICH YOU DO IT AND ON WHICH LEGAL BASIS

STEP 2 INFORM YOUR CUSTOMERS, EMPLOYEES AND OTHER INDIVIDUALS WHEN YOU COLLECT THEIR PERSONAL DATA

STEP 3 KEEP THE PERSONAL DATA FOR ONLY AS LONG AS NECESSARY

STEP 4 SECURE THE PERSONAL DATA YOU ARE PROCESSING

STEP 5 KEEP DOCUMENTATION ON YOUR DATA PROCESSING ACTIVITIES

STEP 6 MAKE SURE YOUR SUB-CONTRACTOR RESPECTS THE RULES

STEP 7 CHECK IF YOU ARE CONCERNED BY THE PROVISIONS BELOW

To better protect personal data, organisations might have to appoint a Data Protection Officer (DPO). **However, you don't need to designate a Data Protection Officer** if processing of personal data isn't a core part of your business, is not a risky processing and your activity isn't at a large scale;

> **You normally don't need to carry out a Data Protection Impact Assessment**

Such an impact assessment is reserved for those that pose more risk to personal data, for instance they do a large-scale monitoring of a publicly accessible area (e.g. video-surveillance).

NP-1

Obrigado.

JOSÉ EDUARDO ELIAS ROMÃO

Ouvidor

PETROBRAS DISTRIBUIDORA S.A.

Ouvidoria

Rua Correia Vasques, 250 - 8º andar

CEP: 20211-140 - Cidade Nova - Rio de Janeiro - RJ

Tel: (21) 2354-4313

E-mail: joseromao@br.com.br