CONVENÇÃO SECOVI 2019

PROTEÇÃO DE DADOS: SOMOS TODOS RESPONSÁVEIS

Márcio Chaves

26.08.2019

Márcio Chaves

- Advogado especialista em Direito Digital, Sócio do Peck Advogados (agora PG Advogados) e da Peck Sleiman Treinamentos
- Professor dos cursos de MBA em Segurança da Informação do Centro Universitário UNA (MG) e em Gestão da Inovação e Direito Digital da FIA Business School (SP)
- Mestre em Propriedade Intelectual pela Organização Mundial de Propriedade Intelectual OMPI, Genebra/Suíça e Università Degli Studi di Torino, Turim/Itália
- Certificado em Data Protection pela EXIN
- Formado Direito com foco em Direito Empresarial pela Faculdade de Direito Milton Campos, Belo Horizonte/Brasil
- Extensão em Direitos Autorais Avançados na Organização Mundial de Propriedade Intelectual WIPO Academy (Genebra/Suíça), em Direito da Mídia na Faculdade de Direito da Fundação Getúlio Vargas, FGV-RIO (Rio de Janeiro, Brasil), e em Direito de Informática na Faculdade de Direito da PUC Minas (Belo Horizonte)
- Membro do Capítulo Brasileiro da Internet Society - ISOC-Brasil, do Instituto Brasileiro de Direito Digital (IBDDIG) e da Association for the Advancement of Artificial Intelligence (AAAI)
- Coautor dos Livros “WIPO IP Research Papers” pela World Intellectual Property Organization (WIPO) Academy, 2010, “Direito Digital Aplicado 2.0” (RT, 2016) e “Direito Digital Aplicado 3.0 (RT, 2018)


ESTAMOS
NA ERA DO
SOCIAL
SCORE
芝麻信用
748
信用极好
晒晒一下
信用生活

Rate a Friend

Get Your Rating

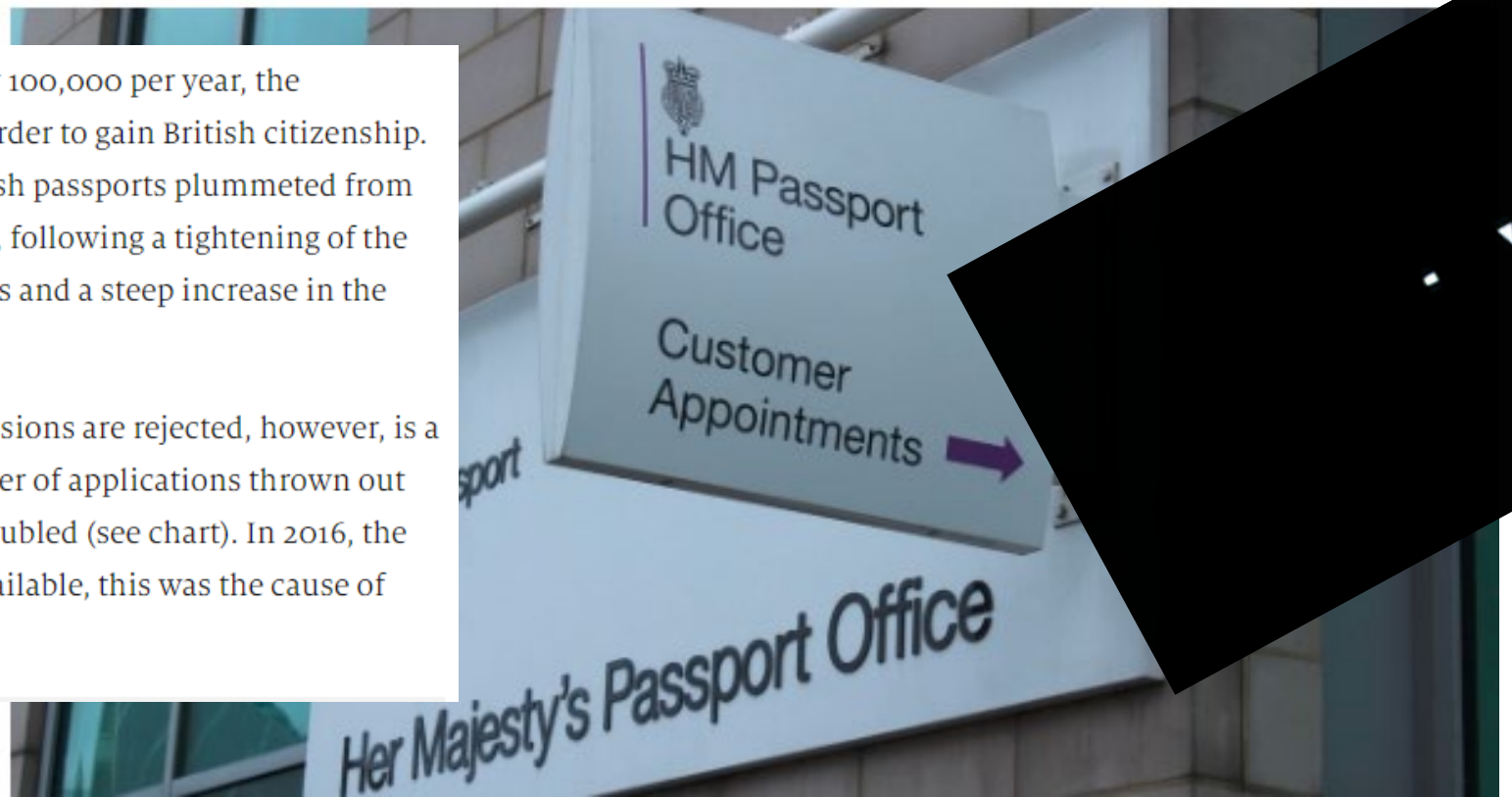
@vickywoollaston rated

@jtemperton 5 stars

Share Share Download

Promiscuous? Divorced? Eccentric-looking? You may be denied a passport

An extraordinarily vague "good character" test accounts for a rocketing number of citizenship refusals

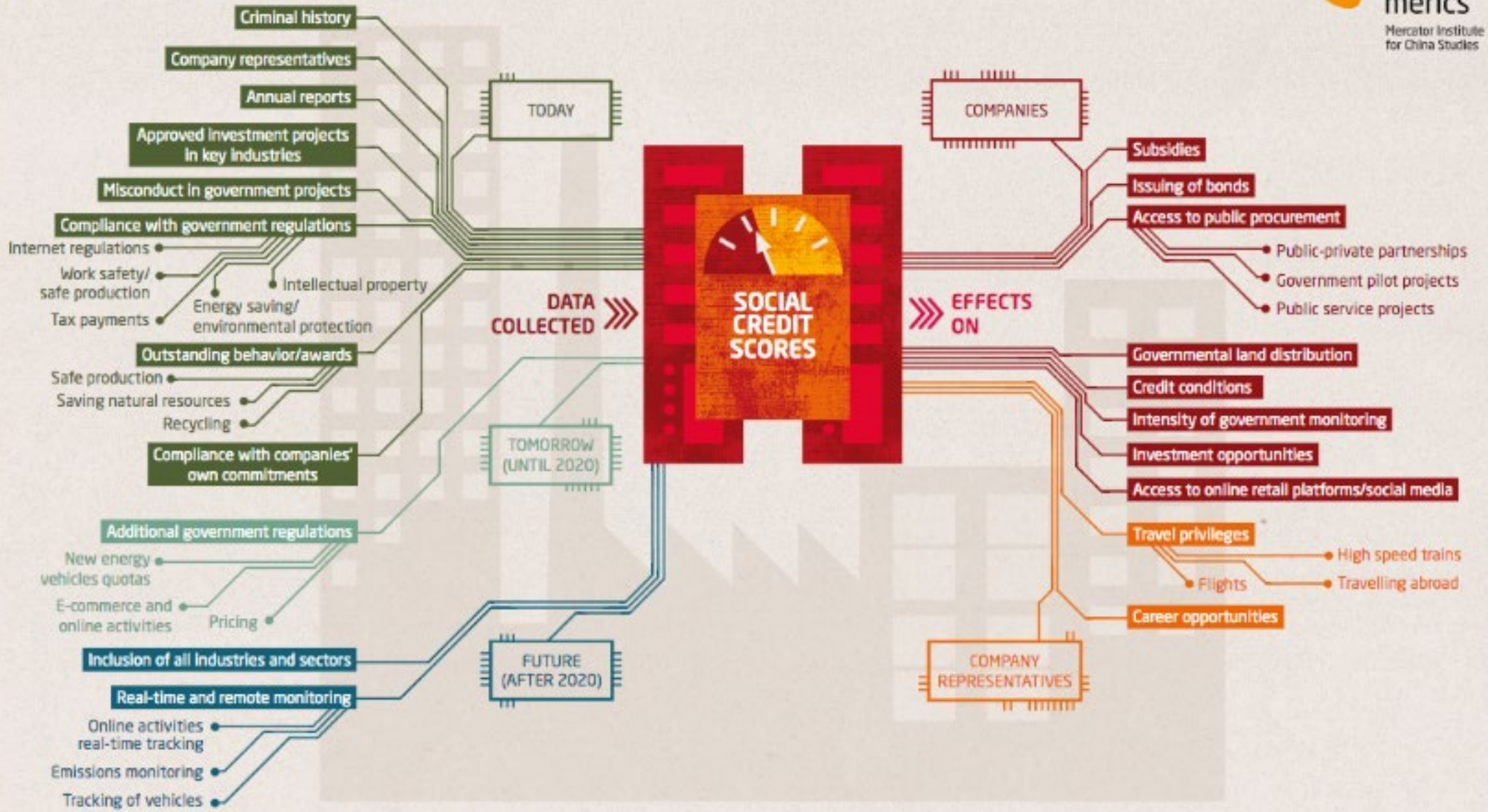


IN ITS drive to get net migration below 100,000 per year, the government has made it drastically harder to gain British citizenship. The number of foreigners getting British passports plummeted from 194,370 in 2012 to just 123,229 last year, following a tightening of the rules for bringing over family members and a steep increase in the cost of applying.

The most common reason that submissions are rejected, however, is a rather vague one. Since 2012 the number of applications thrown out under a "good character" clause has doubled (see chart). In 2016, the most recent year for which data are available, this was the cause of 44% of all refusals.

China's tight grip on enterprises

Influencing business decisions via Social Credit Scores*



*Selection of data collected and exemplary effects of Social Credit Scores.
Source: Policy documents and regulations released by the Chinese central government since 2014.

Como harmonizar as novas tecnologias com o direito à privacidade?

Proteção de dados: UE recebeu 10 mil queixas por mês

Queixas deram origem a 255 investigações a empresas

Cerca de **95 mil queixas** foram feitas na União Europeia, junto das autoridades nacionais de proteção dos dados, após a entrada em vigor do novo regulamento europeu, em maio, relacionadas com **‘telemarketing’ e ‘e-mails’ promocionais**, seguido de **videovigilância**.

Foram feitas **255 investigações a empresas**, **como redes sociais**, por alegado desrespeito ao RGPD (ou GDPR), processos iniciados a partir de **denúncias individuais** ou por **iniciativa das autoridades nacionais competentes**.

Fonte: https://tvi24.iol.pt/internacional/rgpd/protecao-e-dados-ue-recebeu-10-mil-queixas-por-mes

negocios

SAÚDE

Hospital do Barreiro multado em 400 mil euros por não proteger dados clínicos dos doentes

A Comissão Nacional de Protecção de Dados decidiu aplicar uma coima ao Centro Hospitalar Barreiro Montijo por permitir o acesso indiscriminado de dados de saúde dos doentes a pessoas que não deveriam ter essa possibilidade.

Fonte: https://www.jornaldenegocios.pt/economia/saude/detalhe/hospital-do-barreiro-multado-em-400-mil-euros-por-nao-proteger-dados-clinicos-dos-doentes

Clientes da Atlas querem processar empresa por vazamento de dados pessoais

Por **Alexandre Antunes** - 31 AGO, 2018 09:59

A lista dos dados dos investidores de Bitcoin que vazou na última sexta-feira (24) da plataforma de investimentos Atlas Quantum deve resultar em ações judiciais promovidas por alguns dos 264 mil clientes da plataforma que tiveram os dados expostos.

Banco Inter fecha acordo para pagar R$ 1,5 milhão após vazamento de dados de clientes

Compromisso põe fim a processo movido pelo MP-DF desde julho. Segundo acusação, segurança dos dados de 19.961 correntistas foi comprometida.

Netshoes ligará para 2 milhões de clientes afetados por vazamento de dados

Ligações serão feitas a partir de 8 de março. Medida foi adotada após reunião da empresa com Ministério Público do DF.

Netshoes terá de pagar R$ 500 mil por vazamento de dados de 2 milhões de clientes

Valor de indenização foi firmado em acordo com Ministério Público do DF. Incidente comprometeu dados pessoais de servidores da Presidência, da Polícia Federal e do STF.

https://g1.globo.com/df/distrito-federal/noticia/2018/12/19/banco-inter-fecha-acordo-para-pagar-r-15-milhao-de-indenizacao-apos-vazamento-de-dados-de-clientes.ghtml
https://g1.globo.com/df/distrito-federal/noticia/netshoes-ligara-para-2-milhoes-de-clientes-afetados-por-vazamento-de-dados.ghtml
https://g1.globo.com/df/distrito-federal/noticia/2019/02/05/netshoes-tera-de-pagar-r-500-mil-por-vazamento-de-dados-de-2-milhoes-de-clientes.ghtml
https://portaldobitcoin.com/clientes-da-atlas-querem-processar-empresa-por-vazamento-de-dados-pessoais/

A evolução da legislação brasileira quanto aos usos de dados pessoais

PG advogados
pires, gonçalves & associados

Lei nº 8.078
Código de Defesa do Consumidor

1990

Decreto Federal nº 7.962 e nº 7.963
Lei do E-commerce & Plano Nacional de Consumo e Cidadania

2013

Lei nº 12.965
Marco Civil da Internet

2014

Lei nº 13.709/2018 e 13.853/2019
Lei geral de proteção de dados & Autoridade Nacional de Proteção de dados

2018


Pause

Condição daquilo que é privado, **pessoal**, **íntimo**.

O QUE SÃO

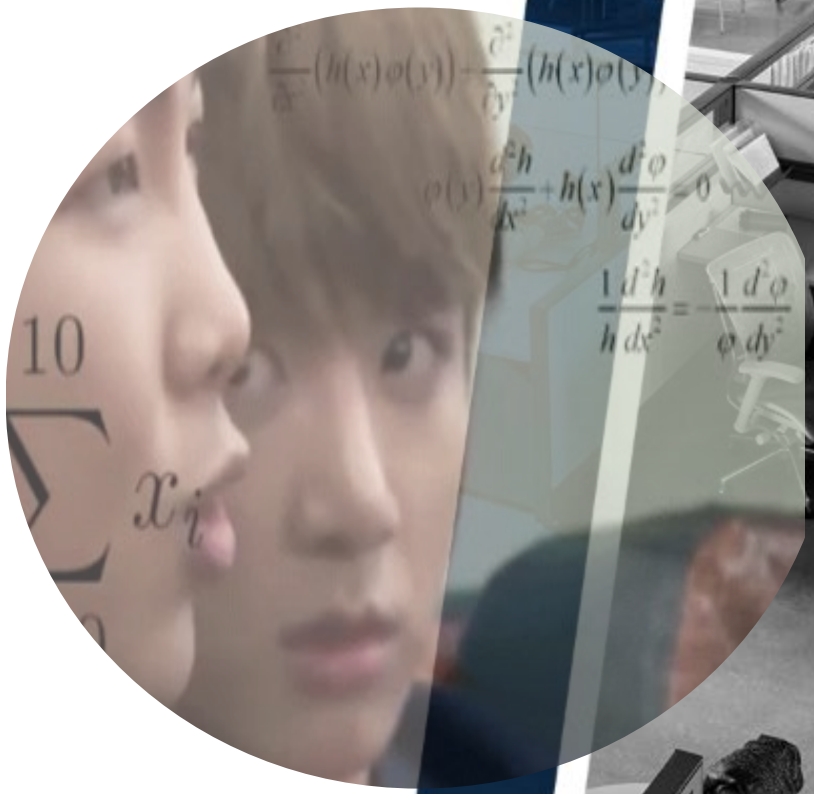
DADOS?

DADO PESSOAL:

Informação relacionada a pessoa natural identificada ou identificável.

DADO ANONIMIZADO (ART. 12): *dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.*

ANONIMIZAÇÃO: *utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado* ***perde a possibilidade de associação****, direta ou indireta, a um indivíduo.*



DADOS PESSOAIS

Informações que tornam possível a **identificação da pessoa (identifica ou é identificável)**; como endereço, CPF, nome, endereço de IP, fotos, placa de carro, etc.

≠

DADOS PESSOAIS SENSÍVEIS

Informações acerca da individualidade da pessoa; como informações genéticas, de saúde, sua visão política, orientação religiosa ou expressão de sexualidade, sindical, biometria, etc.

PG advogados
pires, gonçalves & associados

HD

DVD

CD

Pendrive

Cartão SD

Memory Stick

HD Portátil

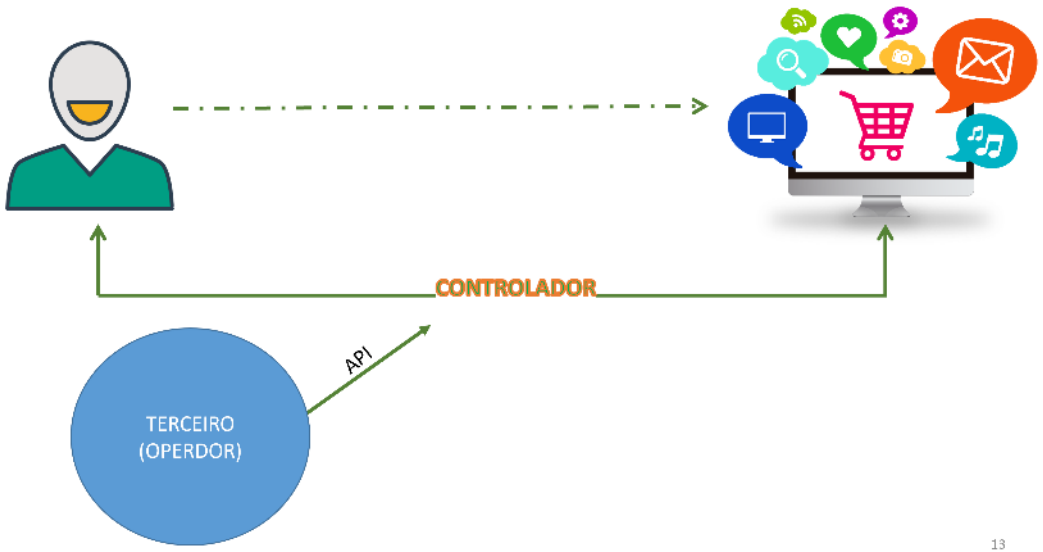
Disquete

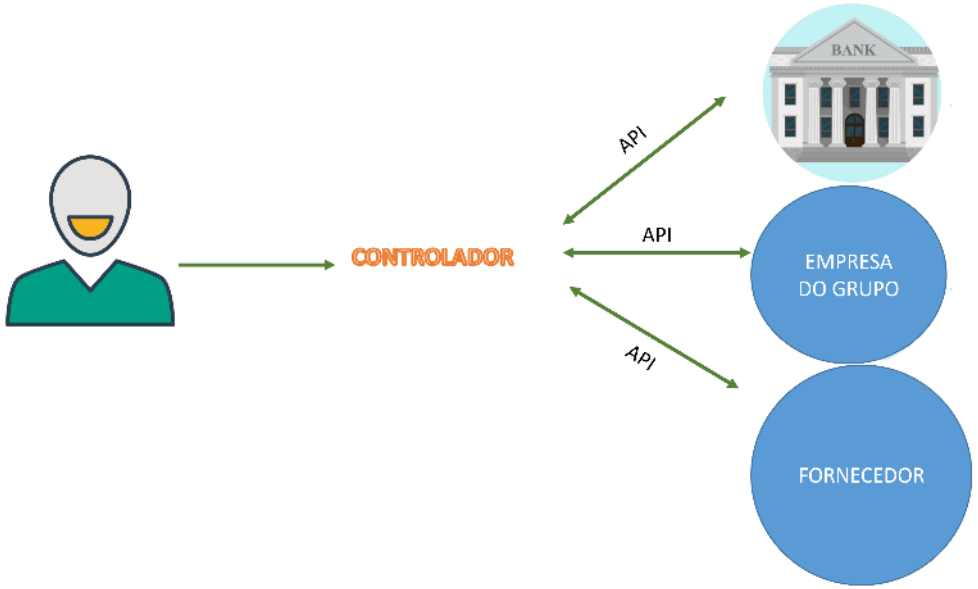
ARMAZENAMENTO DE DADOS

Os dados podem ser armazenados em diversos meios, *ONLINE* E *OFFLINE*, tais como:

Conceitos – artigo 5º. LGPD

CONTROLADOR	OPERADOR
Toma as decisões relativa ao tratamento de dados pessoais	**Realiza** o tratamento de dados pessoais **em nome do controlador**





Direitos do Titular (art. 18)

- ✓ Confirmação da existência de tratamento
- ✓ **Acesso aos dados**
- ✓ Correção de dados incompletos, inexatos ou desatualizados
- ✓ **Anonimização**
- ✓ Bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei
- ✓ **Portabilidade** dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial
- ✓ Eliminação dos dados pessoais tratados com o consentimento do titular
- ✓ **Informação** das entidades públicas e privadas com as quais o controlador realizou uso **compartilhado de dados**
- ✓ informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa
- ✓ **Revogação do consentimento**

DATA PROTECTION OFFICER (DPO)

PG advogados
pires, gonçalves & associados

DATA PROTECTION OFFICER (DPO) – arts. 37 a 39

GDPR

DPO they know the company

They are the translators (between CEO, IT, Legal)

Andrea Jelinek

Chairwoman European Data Protection

DPA - Austrian

DATA PROTECTION OFFICER (DPO)

No Brasil, o DPO ou Encarregado:

- É pessoa indicada pelo Controlador e pelo Operador (art. 5º, VIII) – pode ser natural ou jurídica (termo pessoa genérico)
- A ANPD regulamentará os casos em que o Operador deverá indicar Encarregado art. 41 § 4º, inc I);
- É o **canal de comunicação** entre o Controlador, os Titulares de Dados e a Autoridade Nacional (art. 5º, VIII).

DATA PROTECTION OFFICER (DPO)

De acordo com o 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 são:

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.

PRINCÍPIOS E HIPÓTESES DE TRATAMENTO DE DADOS PESSOAIS

1) *PRIVACY BY DESIGN* E *PRIVACY BY DEFAULT*

2) MINIMIZAÇÃO DO USO

Minimização dos usos dos dados pessoais

Os dados pessoais devem ser:

- Adequados;
- Pertinentes;
- Limitados às finalidades para os quais são tratados.

A LGPD exige a **minimização do uso dos dados pessoais**, isso se impacta com o objetivo das empresas que é a **maximização**.

“...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”

3) TRANSPARÊNCIA:

4) 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;”

Princípios do tratamento

- **Art. 6º. Tratamento:** Deve observar a **boa-fé e os seguintes princípios**:

✓ finalidade do tratamento;
✓ compatibilidade do tratamento com as **finalidades informadas** ao titular;
✓ limitação do tratamento ao **mínimo necessário** para a realização de suas finalidades;
✓ garantia, aos titulares, de consulta facilitada e gratuita sobre a forma do tratamento;
✓ 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;
✓ **transparênci**a aos titulares;
✓ utilização de **medidas técnicas e administrativas aptas** a proteger os dados pessoais;
✓ prestação de contas, pelo agente, da **adoção de medidas capazes de comprovar** a proteção de dados pessoais.

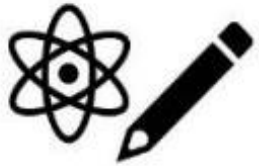
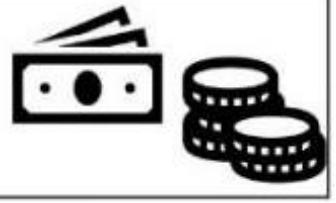
Tratamento de dados pessoais

Qualquer operação feita com dados pessoais, incluindo:

- Coleta
- Produção
- Recepção
- Classificação
- Utilização
- Acesso
- Reprodução
- Transmissão
- Distribuição
- Processamento
- Arquivamento
- Armazenamento
- Eliminação
- Avaliação ou controle da informação
- Modificação
- Comunicação
- Transferência
- Difusão
- Extração

...de dados pessoais.

Hipóteses de tratamento

I – Consentimento 	VI – Processo Judicial 
II – Obrigação Legal 	VII - Vida 
III – Políticas Públicas 	VIII – Saúde 
IV – Pesquisa 	IX – Legítimo Interesse 
V – Contrato 	X – Crédito 

IX – Legítimo Interesse

1) Quando os dados pessoais forem utilizados para fins razoavelmente esperados pelo titular
2) Quando o impacto à privacidade for mínimo
3) Quando houver justificativa "irrefutável" para o tratamento

Consentimento – LGPD - Art. 8

- ✓**Deve ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.**
- ✓Deve **constar de cláusula destacada das demais cláusulas contratuais.**
- ✓Cabe ao **controlador o ônus da prova de que o consentimento** foi obtido em conformidade com o disposto nesta Lei.
- ✓É **vedado o tratamento de dados pessoais mediante vício de consentimento.**
- ✓O consentimento **deverá referir-se a finalidades determinadas**, e as **autorizações genéricas para o tratamento de dados pessoais serão nulas.**
- ✓**Pode ser revogado a qualquer momento.**

PASSIVO DE DADOS?

https://www.facebook.com/TheEconomist/videos/the-worlds-most-valuable-resource/10155368078074060/

Lei 13.709/18 - LGPD

O que fazer em caso de incidente?

Dever de Notificação (Report) [art. 48, § 1º/ Lei nº 13.709/18]

Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

§ 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

I - a descrição da natureza dos dados pessoais afetados;

II - as informações sobre os titulares envolvidos;

III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

IV - os riscos relacionados ao incidente;

V - os motivos da demora, no caso de a comunicação não ter sido imediata; e

VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

PG advogados
pires, gonçalves & associados

Penalidades

ART. 52: atualizado pela Lei 13.853/2019

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - **multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;**

III - multa diária, observado o limite total a que se refere o inciso II;

IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;

V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

VI - eliminação dos dados pessoais a que se refere a infração;

VII a XII - vetados.

(...) § 2º O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais definidas na Lei nº 8.078, de 11 de setembro de 1990, e em legislação específica.

Independentemente das sanções administrativas...

- **PERDA REPUTACIONAL**
- **CRISE DE IMAGEM - IMPACTO NO *VALUATION***
- **MEDIDAS JUDICIAIS**

Penalidades

Art. 52 - § 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:

I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;
II - a boa-fé do infrator;
III - a vantagem auferida ou pretendida pelo infrator;
IV - a condição econômica do infrator;
V - a reincidência;
VI - o grau do dano;
VII - a cooperação do infrator;
VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;
IX - a adoção de política de boas práticas e governança;
X - a pronta adoção de medidas corretivas; e
XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

Como agir?

1. **TECNOLÓGICO**: soluções tecnológicas
2. **GOVERNANÇA**: revisão / elaboração de contratos, normas, políticas, processos e procedimentos
3. **EDUCACIONAL**: conscientização e treinamento de equipe

MATRIZ TÉCNICA -JURÍDICA:

- **TIPO DE DADO PESSOAL**
- **TIPO DE TRATAMENTO**
- **FINALIDADE**
- **JUSTIFICATIVA**

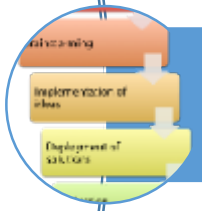
Tipos de dados pessoais coletados → Tipos de tratamentos de dados pessoais Realizados → finalidade de uso → Justificativas jurídicas

PG advogados
pires, gonçalves & associados

CONVIVENDO COM OS DIPLOMAS LEGAIS

Mapear as hipóteses de finalidade com base na(s) legislação(ões) aplicável(eis) conforme as especificidades de cada dado pessoal

Revisar processos de modo a observar os princípios da minimização do uso, garantia de transparência e *privacy by design*



Estabelecer procedimentos de atendimento às solicitações de titulares conforme matriz desenhada

Estabelecer procedimentos e modelos de resposta às notificações e autuações conforme autoridade competente (MP, PROCON, ANPD)

Criar e cultivar a cultura da privacidade e da proteção de dados pessoais

O tempo está VOANDO!

Estágios Meta	ESTÁGIO 1 JUL/19	ESTÁGIO 2 AGO/19	ESTÁGIO 3 NOV/19	ESTÁGIO 4 JAN/10	ESTÁGIO 5 MAR/19	ESTÁGIO 6 MAI/20	ESTÁGIO 7 JUL/20
Descritivo	Seleção dos fornecedores para iniciar o projeto de conformidade às novas regulamentações de proteção de dados pessoais	Kick off do projeto, realização do workshop de sensbilização e realização do levantamento inicial de informações e entrevistas. Realizar o inventário com os tipos de dados pessoais atuais (legado) e que podem passar a ser capturados devido aos novos projetos (futuro próximo visão até 2021), elaborar o mapa do fluxo dos dados pessoais e a matriz de tratamentos X finalidades X justificativas (para identificar o que já possui Privacy Risk)	Conclusão do Assessment inicial envolvendo: a) coleta das informações; b) realização das entrevistas; c) análise de Data Discovery (se aplicável); Relatório de Diagnóstico com Gap Analysis; Plano de Implementação. Apresentação do PIA e preparo do modelo para gerar PIA por projeto novo futuro.	Implementação dos itens mais urgentes do Plano de Ação (que geram mais exposição de risco e maior impacto em termos de aplicação de multas) e que já permitem disseminar a cultura de *Privacy by Design* na organização. Implementar o check-list de compliance na área de compras, o check-list de novo projeto, atualizar a Política de Privacidade e de Cookies (itens mais "vitrine"), implementar o modelo de gestão de consentimentos. Implementação de solução de anonimização (se necessário)	Implementação dos itens técnicos e jurídicos do Plano de ação. Realização de campanha educativa sobre o tema de proteção de dados pessoais para as equipes e para os terceirizados mais críticos que realizam tratamento de dados pessoais. Implementação da Política de Gestão da Proteção de Dados Pessoais, revisão de procedimentos, atualização de contratos. Realização de simulação de sala de crise para adequação do procedimento de resposta à incidentes.	Adequação do organograma da organização para atender ao requisito de Encarregado de Dados Pessoais (ou DPO), ou contratação deste serviço. Verificação do status das implementações (especialmente o que envolver ajustes com parceiros de negócios ou outras empresas do mesmo conglomerado, devido ao diagnóstico do fluxo de dados pessoais.	Conclusão da capacitação das equipes, publicação de todos os documentos atualizados. Divulgação dos materiais orientativos para usuários. Realização de teste dos novos serviços necessários para atender aos novos direitos dos usuários (como solicitação de apagamento de dados, portabilidade). Finalização dos procedimentos e modelos para report à ANPD, outro Regulador (ex: BACEN). Implementação de seguro de ciber (se aplicável).

VISÃO GERAL DO PROJETO LGPD

1.

Assessment

90/120 dias

2.

Implementação

180 dias +

1ª ETAPA - *ASSESSMENT*

Previsão de 120 a 150 dias

1. **Workshop de sensibilização com gestores**

2. **Entrevistas com as áreas estabelecidas pelo PG Advogados em conjunto com a empresa para coleta de dados**

3. **Análise dos documentos relacionados à proteção de dados da empresa**

4. **Gap analysis com índice de conformidade**

5. **Plano de Ação**

2ª ETAPA - IMPLEMENTAÇÃO

- **Assessoria para implementação do Plano de Ação**
- **As medidas podem ocorrer em paralelo**
- **Previsão de 120 a 180 dias**

Técnico	Legal	Educacional - Capacitação
Recomendações técnicas de utilização e contratação de ferramentas e soluções tecnológicas	**Elaboração e revisão de normas, contratos, processos** **Suporte** para respostas a notificações durante o prazo em que durar a assessoria	Equipes (colaboradores) Terceiros críticos (processadores) **Formação – *DPO*, Comitê de Crise, Canal de *Report***

DÚVIDAS

PG advogados

pires, gonçalves & associados

Márcio Chaves
mchaves@pgadvogados.com.br
+55 11 98229.4486