Lauro Gripa Neto

Técnicas e ferramentas para **Governança de Dados**

MAGRATHEA

www.magrathealabs.com

MAGRATHEA

Lauro Gripa Neto
Engenheiro de Software

lauro@magrathealabs.com laurogripa

A ORIGEM DAS LEIS DE PROTEÇÃO DE DADOS

OPINION

Facebook is not free

The economics of much of the Internet is built on two valuable commodities: your time, and your content

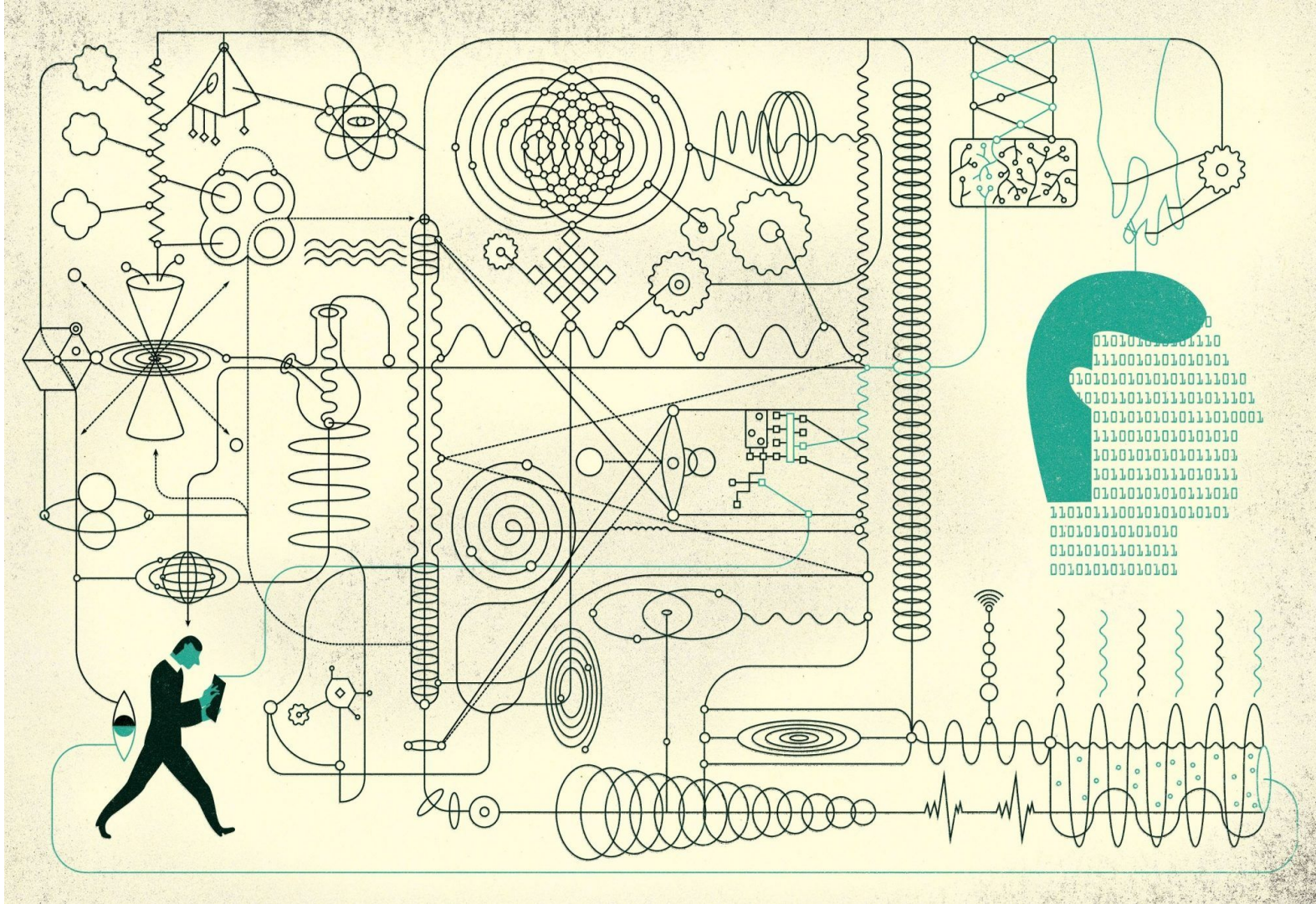
By Ira Winkler

Contributing Columnist, Computerworld

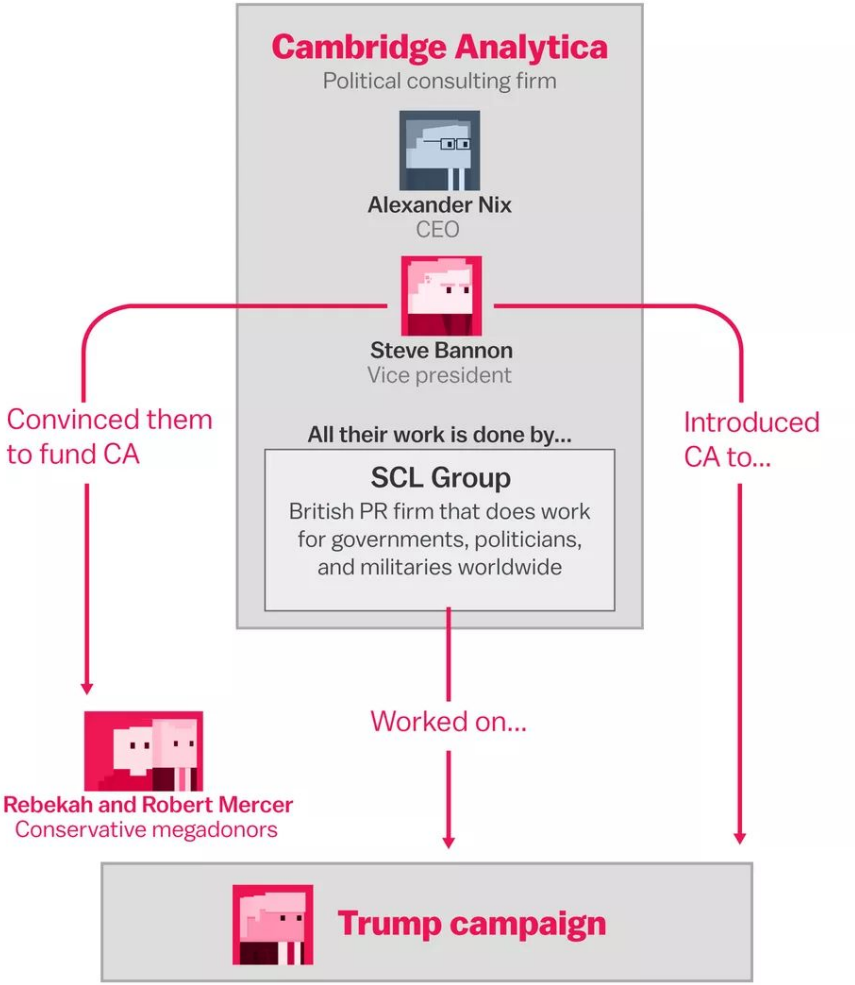
OCT 17, 2011 5:24 PM PST

fonte

se você **não paga**, você é **o produto**.



fontes aqui e aqui


Cambridge Analytica
Political consulting firm
Alexander Nix
CEO
Steve Bannon
Vice president
All their work is done by...
SCL Group
British PR firm that does work for governments, politicians, and militaries worldwide
Convinced them to fund CA
Introduced CA to...
Worked on...
Rebekah and Robert Mercer
Conservative megadonors
Trump campaign

Up to 87 million Facebook users

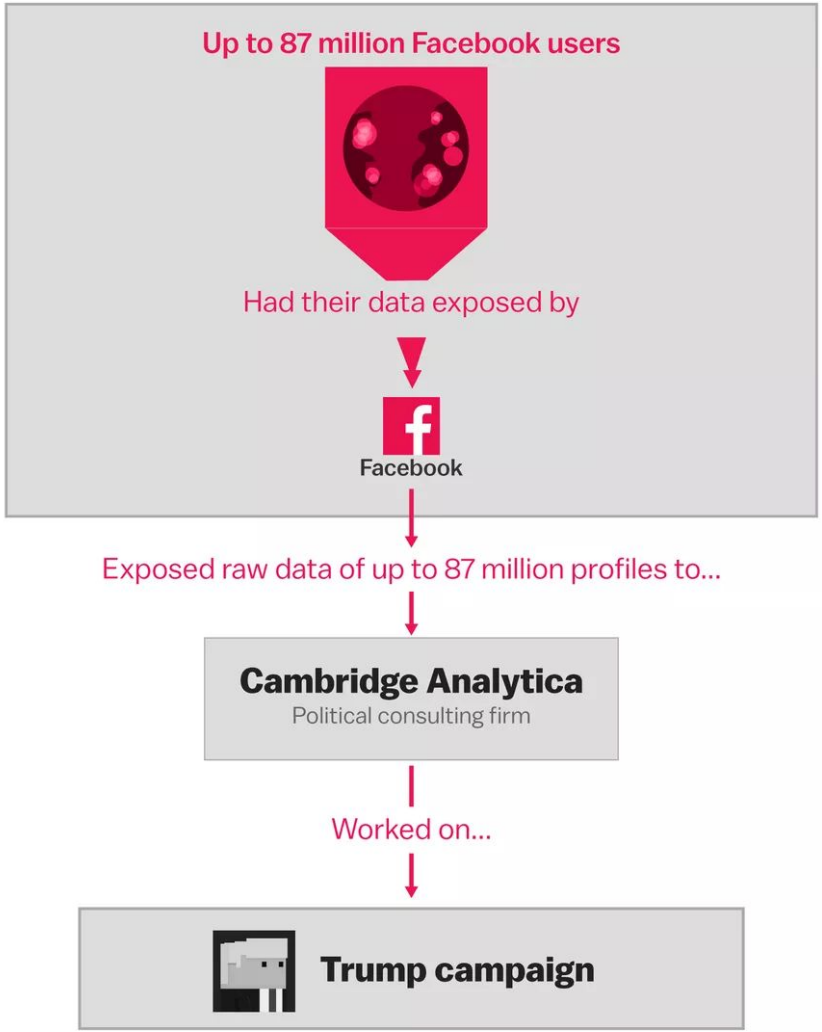
Had their data exposed by

270,000 Facebook users who took the quiz

Who used a quiz app

thisismydigitallife
A quiz app Kogan built on Facebook

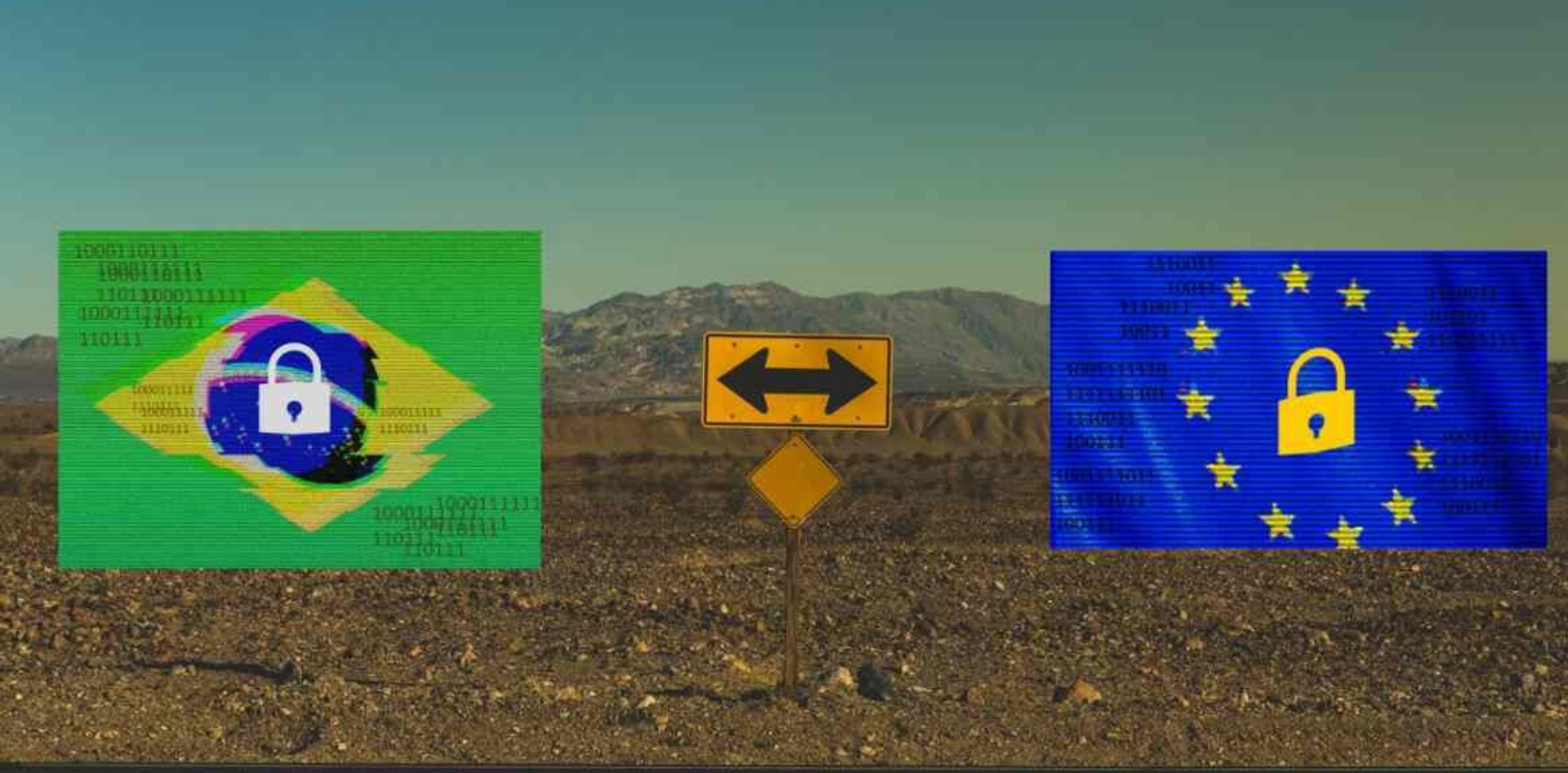
Facebook


Up to 87 million Facebook users
Had their data exposed by
Facebook
Exposed raw data of up to 87 million profiles to...
Cambridge Analytica
Political consulting firm
Worked on...
Trump campaign

fonte


A NETFLIX ORIGINAL DOCUMENTARY
THE GREAT HACK
From the Academy Award nominated filmmakers behind THE SQUARE
Sheffield Doc Fest
AFI DOCS
sundance
NOW STREAMING | NETFLIX

MEDIDAS IMEDIATAS (CURTO PRAZO)



fonte

Utilizando GDPR como base

- LGPD é baseada na lei europeia **G**eneral **D**ata **P**rotection **R**egulation
- Ambas são leis modernas e baseadas em princípios
- Incentivam mudança na cultura (pessoas)
- Existem diversas experiências com GDPR que servem de base para LGPD

Links:

- ➔ https://gdprchecklist.io/
- ➔ https://www.portaldaprivacidade.com.br/home/categories/infogr%C3%A1ficos-e-cartilhas
- ➔ https://github.com/erichard/awesome-gdpr
- ➔ https://github.com/bakke92/awesome-gdpr


GDPR 1
Multas de até €20 milhões ou 4% do faturamento anual
Possibilidade de abrangência a empresas brasileiras
Nomeação de *Data Protection Officer*, quando obrigatório
Realização de **Análise de Impactos de Proteção de Dados**
Certas **violações de dados** deverão ser reportadas
Algumas empresas do BR devem **nomear representantes na UE**
Proteção de dados como **padrão** e **desde a concepção** das aplicações
Escopo territorial
Art.3
Sanções
Art.83
Princípios
Art. 5
DPOs
Art.37
Consentimento
Art. 7
DPIA
Art.35
GDPR
Art.16
Direito a retificação
Notificações
Art.33
Art.17
Direito a exclusão
Art.27
Representantes
Art.20
Direito a portabilidade dos dados
Art.25
DP by *design/default*
Transparência, limitação da finalidade e **minimização dos dados ...**
Exigências mais rígidas para o **consentimento** junto ao titular dos dados
Dados incorretos/desatualizados devem ser **retificados**
Os dados não mais necessários deverão ser **excluídos**
Titular pode levar seus dados a outras empresas
fonte
OPICE BLUM

Checklist de conformidade com a LGPD

Entrar em conformidade com a LGPD não precisa ser complicado. Essa é uma checklist básica que você pode utilizar para aumentar sua conformidade com a lei.

Se a sua organização está determinando o próposito de armazemaneto e processamento de informação pessoal, ela é considerada uma **controladora**. Se a sua organização armazena ou processa dados pessoais em nome de outra organização, ela é considerada uma **processadora**. É possível que sua organização tenha os dois papéis. Utilize o filtro abaixo para visualizar somente os itens relevantes a sua organização.

Essa lista está longe de ser um documento legal, ela é meramente uma tentativa de facilitar sua vida.

Sinta-se livre para contribuir diretamente no GitHub!

COMPLIANCE TOOLS

GDPR Form
GDPR Tracker

ADAPTADO POR

Magrathea

Selecione o papel da sua organização:

CONTROLADORA: EU DETERMINO PORQUE OS DADOS SÃO PROCESSADOS

PROCESSADORA: EU ARMAZENO OU PROCESSO DADOS PARA TERCEIROS

SEUS DADOS

- [ ] Sua empresa possui uma lista de todos os tipos de informações pessoal exigidas, a origem desses dados, com quem isso é compartilhado, o que é feito com isso e por quanto tempo é armazenado.

repositório

Minha organização precisa de um DPO?

Independente de ser **controlador** ou **processador**, se sua **atividade principal** envolve o processamento de **dados sensíveis** em **larga escala** ou envolve **monitoramento de indivíduos regular e em larga escala**, a presença de um DPO é mandatória.

fonte

O que é um DPO?

Data **P**rotection **O**fficer (pessoa física ou jurídica)

O DPO deve ter conhecimento **multidisciplinar**, conciliando temas das áreas de **tecnologia**, **gestão da informação** e **jurídica**, mas pode contar com o auxílio de comissões especializadas nestas áreas.

O DPO deve **responder às autoridades oficiais** e não deve possuir **conflitos de interesse** com a organização.

fonte

Exemplos de organizações

DPO mandatório

- um hospital processando **grandes conjuntos de dados sensíveis**;
- uma empresa de segurança responsável por **monitoramento** de espaços públicos;
- uma pequena empresa de recrutamento que traça **perfis de indivíduos**.

DPO não mandatório

- um médico local que processa dados de pacientes;
- uma pequena empresa de advocacia que processa dados pessoas dos seus clientes.

fonte

TÉCNICAS E FERRAMENTAS

Governança de dados

fonte

Governança de dados

fonte

- **Autoria:** de quem são os dados?
- **Acessibilidade:** quem pode acessar?
- **Segurança:** quais medidas e sistemas garantem a conformidade dos acessos?
- **Qualidade:** os dados estão estruturados e são rastreáveis?
- **Conhecimento:** agregam valor e tem um motivo para existir?

DPIA - *Data Protection Impact Assessment*

GDPR 5

- Avaliações sobre as conclusões do DPIA
- Implementação das medidas de controle para reduzir os riscos diagnosticados
- Verificação do nível de risco residual
- Observância das recomendações da Autoridade Competente, caso tenha sido consultada
- Auxílio do *Data Protection Officer*, caso exista

- Dados tratados e suas categorias
- Tipos de tratamento (coleta, uso, armazenamento compartilhamento e exclusão)
- Intervenientes e terceiros receptores dos dados
- Identificação dos sistemas utilizados
- Relação dos tipos de sujeitos afetados pelo tratamento

fonte

Anomização

“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.”

Anomização

Strategy	Data Types	When to use
Suppression	All	Useless attributes
Random Substitution	All	Useless attributes with integrity constraints
Variance	Numeric / Dates	Analytics
Encryption	Text	Analytics / UNIQUE attributes
Shuffling	All	Analytics
Faking / Mocking	All	Dev / CI / Functional Testing
Partial Suppression	Text	Direct Identifiers
Generalization	Numeric / Dates	Analytics

fonte

TECNOLOGIAS

GDPR COMPLIANT/COMPLIANCE

Exemplos de aplicações

RAILS

- https://github.com/prey/gdpr_rails
- https://github.com/ankane/ahoy

REDIS

- https://redislabs.com/blog/dont-worry-happy-redis-labs-ready-gdpr/

POSTGRES

- https://www.enterprisedb.com/

AWESOME LISTS

- https://github.com/KevinColemanInc/awesome-privacy
- https://github.com/nikitavoloboev/privacy-respecting
- https://github.com/Kickball/awesome-selfhosted

Hospedagem

- AWS: https://devcenter.heroku.com/articles/gdpr
- Azure: https://azure.microsoft.com/en-us/blog/protecting-privacy-in-microsoft-azure-gdpr-azure-policy-updates/
- Heroku: https://devcenter.heroku.com/articles/gdpr
- DigitalOcean: https://www.digitalocean.com/legal/gdpr/

GDPR TRACKER

GDPR Checklist GDPR Form + Add company

GDPR Tracker

Track the GDPR compliance of **+100** cloud services and subprocessors.

aws

Search powered by Algolia

Track	Name	Status	HQ	Privacy	DPA	Subprocessors	Hosting partners	Data centers	Certifications	
☐	Amazon Web Serv...	●	🇺🇸	Privacy	DPA		AWS	Global	EU-U.S. Privacy Shield, ISO 27001, ...	Edit
☐	Officient	●	🇧🇪	Privacy			AWS	EU		Edit
☐	Netflix	●	🇺🇸	Privacy			AWS	US		Edit
☐	PythonAnywhere		🇬🇧	Privacy	DPA		AWS	US	EU-U.S. Privacy Shield	Edit
☐	Lyft	●	🇺🇸	Privacy			AWS	US		Edit
☐	Knowlex	●	🇧🇪	Privacy			AWS	EU		Edit
☐	Booking.com	●	🇳🇱	Privacy			AWS	EU		Edit
☐	Baremetrics	●	🇺🇸	Privacy			AWS	US	EU-U.S. Privacy Shield, Swiss-U.S. Privacy Shield	Edit
☐	SupportHero		🇺🇸	Privacy		Subprocessors	AWS	EU		Edit
☐	Hubspot	●	🇺🇸	Privacy	DPA		AWS		EU-U.S. Privacy Shield, ISO 27001, ...	Edit
☐	Airtable		🇺🇸	Privacy			AWS	US	SOC 1, SOC 2 Type I, ...	Edit
☐	Grammarly		🇺🇸	Privacy			AWS	US	Swiss-U.S. Privacy Shield, EU-U.S. Privacy Shield	Edit

NOSSAS EXPERIÊNCIAS

Desafios

- **Obtenção de consentimento**
  - Adquirir consentimento para uso de cookies e envio de e-mail marketing
    - Clientes de clientes
- **Acessibilidade**
  - Developers não tem mais acesso a contas de usuários
- **Direito de ser esquecido**
  - Remoção dos dados (em até 7 dias)
  - Construção de interface para edição, deleção ou download dos dados
    - Clientes de clientes

Preocupações

- ➔ **Imagem/marketing**
- ➔ **Relações comerciais**
- ➔ **Produtividade**
- ➔ **Desempenho**
- ➔ **Escalabilidade**

Soluções

- **Obtenção de consentimento**
  - Double Opt-in para conversão de Leads
  - Cookie consent para rastreamento
- **Acessibilidade**
  - Anonimização dos dados
- **Direito de ser esquecido**
  - Foco em qualidade
  - Gerenciar consentimento
  - Nem todos os dados precisam deletados. Alguns podem ser matindos em **legítimo interesse**, porém, sempre busque o **consentimento**.

Dicas

- ➔ **Pensamento sistêmico**
- ➔ **Princípios**
- ➔ **Framework de Governança de Dados**
- ➔ **Foco em qualidade**
- ➔ **Desenvolver pensando em dados (data-driven)**
- ➔ **Processos bem definidos**
- ➔ **Transparência e boa vontade de estar em conformidade**
- ➔ **Disseminação de conhecimento (mudança na cultura)**

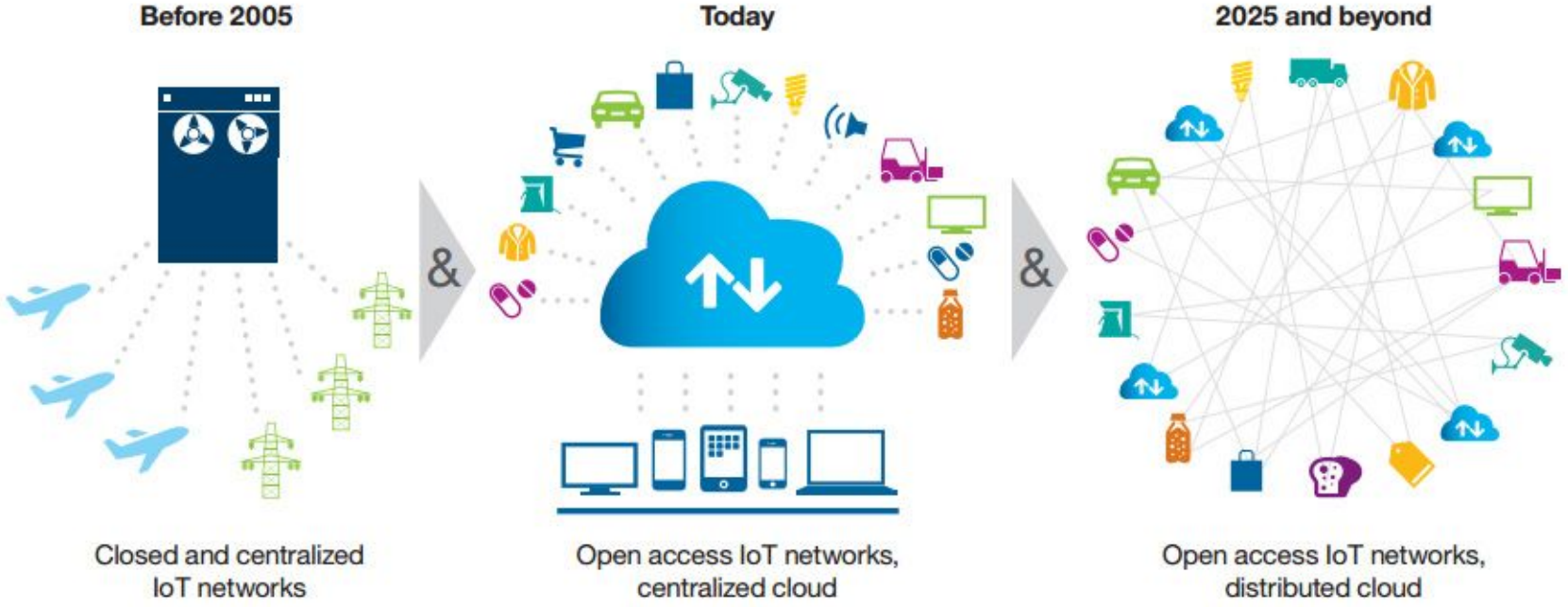
PRIORIZANDO PRIVACIDADE (LONGO PRAZO)

OP-ED

By 2030, You'll Be Living in a World That's Run by Google

And it may be both the best and worst thing to happen to humanity.

fonte


Before 2005
Today
2025 and beyond
&
&
Closed and centralized IoT networks
Open access IoT networks, centralized cloud
Open access IoT networks, distributed cloud

PRIVACY BY DESIGN / PRIVACY BY DEFAULT

★ Recomendado pela GDPR

GDPR

Privacy by Design

"Privacy by Design" and "Privacy by Default" have been frequently-discussed topics related to data protection. The first thoughts of "Privacy by Design" were expressed in the 1970s and were incorporated in the 1990s into the RL 95/46/EC data protection directive. According to recital 46 in this Directive, technical and organisational measures (TOM) must be taken already at the time of planning a processing system to protect data safety.

fonte

PRIVACY BY DESIGN / PRIVACY BY DEFAULT

X Criticado por ser muito vago

Engineering Privacy by Design

Seda Gürses, Carmela Troncoso, and Claudia Diaz

K.U. Leuven/IBBT, ESAT/SCD-COSIC
firstname.lastname@esat.kuleuven.be

fonte

LOCAL-FIRST

Local-First Software: You Own Your Data, in spite of the Cloud

Martin Kleppmann
Department of Computer Science and Technology
University of Cambridge
Cambridge, United Kingdom
martin.kleppmann@cl.cam.ac.uk

Adam Wiggins
Ink & Switch
Berlin, Germany
adam@inkandswitch.com

Peter van Hardenberg
Ink & Switch
San Francisco, CA, USA
pvh@inkandswitch.com

Mark McGranaghan
Ink & Switch
Seattle, WA, USA
mark@inkandswitch.com

fonte

LOCAL-FIRST

- rapidez
- suporte à multi-dispositivos
- suporte offline
- colaboração
- longevidade
- privacidade (aplicativos na nuvem são **fundamentalmente não-privados**)
- controle de usuário

* CRDT: conflict-free replicated data types

Quer ser dono dos seus dados?
Comece pela sua **identidade digital**

fonte


Ownership
Knowledge
Accessibility
TECHNOLOGY
PEOPLE
PROCESS
Data Governance
Quality
Security


2025 and beyond
Open access IoT networks, distributed cloud

Obrigado!

MAGRATHEA

www.magrathealabs.com / github.com/laurogripa/presentations