

UBER

UBER

GDPR Compliance & LGPD

Flavia Mitri

Diretora de Privacidade - LATAM



A UBER começou pequena...

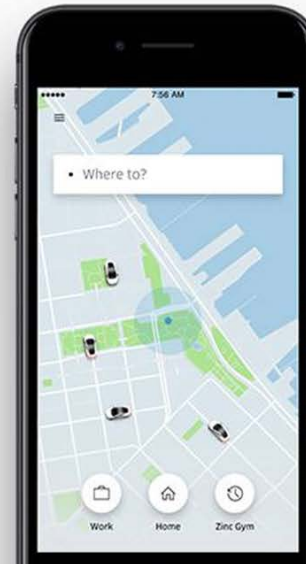
2009



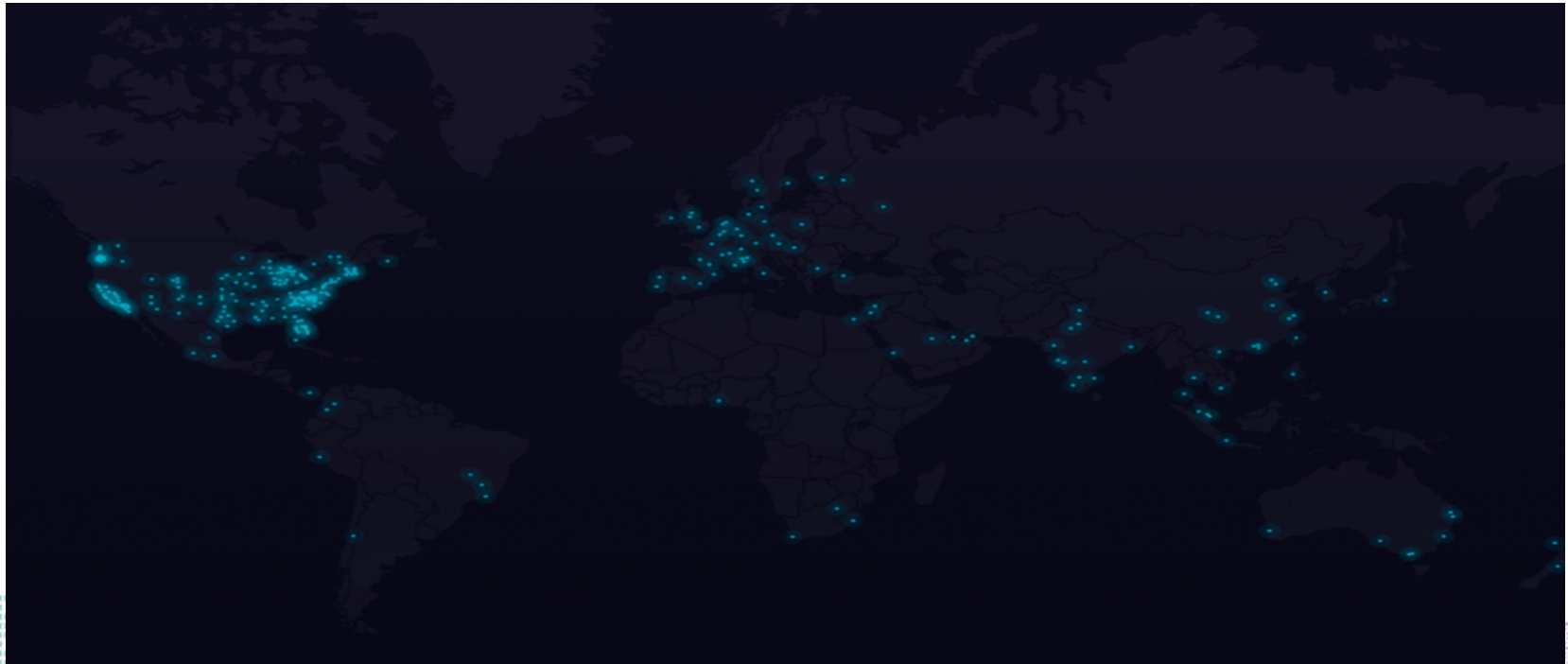
2012



2016



+600 cidades
+65 países
+5bi viagens



27 Estados
+ 100 Cidades
2 mercado mundial



UBER GDPR COMPLIANCE PROGRAM

Programa de compliance criado em 2017: Legal, Segurança, HR, Engenharia & Produto

4 mega-grupos de trabalho:

- 1. Privacy by design: PIAs / Privacy Governance / P&P**
- 2. Customer data management: SARs / controles de acesso / data mapping / deleção**
- 3. Inputs de segurança: planos resposta a incidentes / gerenciamento de fornecedores**
- 4. Transparência: política de privacidade & consentimento**



	Como era	Como está
DATA PROTECTION OFFICER	N/A	DPO on board
PRIVACY REVIEWS	N/A	Processo implementado; 300+ reviews concluídos
CONTROLE DE ACESSO	Empregados com amplo acesso	Agentes de suporte com acesso limitado à ferramentas específicas; bancos de dados sensíveis com duplo fator de autenticação; todo acesso monitorado.
DELEÇÃO / RETENÇÃO	Sem política global	Política global definida, adequada a GDPR
INVENTÁRIO	N/A	inventário manual de +75% das bases; scan automatizado sendo implementado.
DIREITOS DE ACESSO	processo manual / não escalável	Download My Data disponível no app. SARs maiores entregues em até 30 dias.
VENDOR MANAGEMENT	Ad hoc	Processo mandatário para qualquer novo fornecedor. Fornecedores já utilizados foram todos revistos (+ 4.500 empresas. Aprox 700 tiveram seus contratos rescindidos)
POLITICA DE PRIVACIDADE	Linguagem pouco clara	Linguagem revista. GDPR compliant.
RESPOSTA A INCIDENTE	Processo confuso, sem política fixa	Processo estabelecido, com stakeholders por geografia. Política interna publicada

GDPR & LGPD COMPLIANCE - RECOMENDAÇÕES

1. Stakeholders: jurídico, segurança, HR e engenharia

- a. data mapping;
- b. avalie adequação de ferramentas existentes;

2. Plano de ação GDPR/LGPD

- a. Crie protocolos de segurança e privacidade;
- b. Privacy by design;
- c. Realize treinamentos mandatórios.



GDPR & LGPD COMPLIANCE - RECOMENDAÇÕES

3. Adeque sua coleta & processamento de dados

- a. crie (ou reveja) política de privacidade;
- b. implemente processos internos de privacidade;
- c. crie um manual de classificação de dados.

4. Implementação

- a. implemente funções & programas de segurança;
- b. crie um time de resposta a incidentes de segurança;
- c. mapeamento de todas as áreas.



GDPR & LGPD COMPLIANCE - RECOMENDAÇÕES

5. Tenha o staff adequado

- a. DPO - mandatário
- b. Privacy legal & engenharia
- c. Security

6. Constante monitoramento

- a. gerencie adequadamente todos os incidentes de segurança;
- b. verifique sua adequação aos SARs;
- c. revise sua adequação às regras de GDPR / LGPD.



THANK YOU!

