

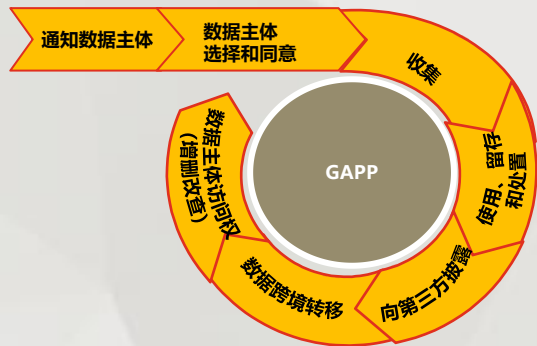
GDPR 与 隐私技术

李雨航 Yale Li

个人隐私数据保护的框架

GAPP Generally Accepted Privacy Principles (GAPP)

A framework intended to assist Chartered Accountants and Certified Public Accountants in creating an effective privacy program for managing and preventing privacy risks. The framework was developed through joint consultation between the Canadian Institute of Chartered Accountants (CICA) and the American Institute of Certified Public Accountants (AICPA) through the AICPA/CICA Privacy Task Force. The GAPP framework was previously known as the














GAPP(Generally Accepted Privacy Principles)

-美国模式，处理个人数据时，数据主体同意是首选

General Data Protection Regulation (GDPR)

After four years of preparation and debate the GDPR was **finally approved** by the EU Parliament on **14 April 2016**. Enforcement date: **25 May 2018** - at which time those organizations in non-compliance may face heavy fines.

The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy.

											
	EU	USA	JPN	KOR	IND	AUS	CAN	BRA	ARG	MEX	CHN
合法、正当、透明	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
目的限制	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓
数据最小化	✓			✓	✓	✓	✓		✓	✓	✓
准确性	✓		✓	✓		✓	✓		✓	✓	✓
存储最小化	✓			✓			✓		✓	✓	
完整性与保密性	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
可归责	✓	✓	✓	✓			✓		✓	✓	

GDPR (General Data Protection Regulation)-欧盟模式，数据处理要满足法律依据，数据主体的同意不是首选

关于欧洲数据保护协议（GDPR）

加强之前的欧盟数据保护法（第95/46/EC号指令）

- 个人对于本人数据如何被使用，具有更多控制权。
- 对高风险活动有更高要求
- 要求开展更多与安全相关的活动



自**2018年5月25日**起强制执行，辐射所有从欧洲经济区（欧盟+冰岛+挪威）获取数据和互联网服务的主体

- 不仅仅是欧盟内部，包括与欧盟做生意的人，在欧盟的企业，或者在欧盟有分部的企业
- 还处理欧盟公民数据的非欧盟企业也需遵守

严厉制裁

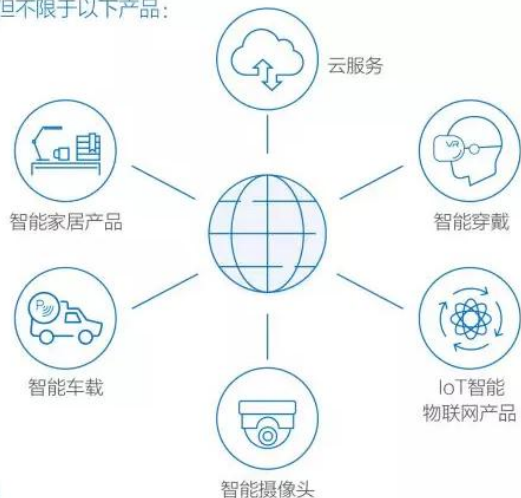
- 对不合格的企业处以2000万欧元或4%年营业额的罚款；
- 下架禁售产品，以及关停服务。

GDPR 一应对措施



GDPR的限制对象

包括但不限于以下产品:



违反GDPR的严重后果!



下架
禁售产品!



关停服务!

不合规的企业, 可能面临高达2000万欧元
(约合1.5亿人民币)或4%年营业额的罚款

如果你是企业主(厂商)!



企业内部学习研究GDPR法案, 并整改个人数据的使用和管理方法



通过第三方认证公司进行详尽的测试和评估, 找到违规项目并及时整改降低风险



进行详细的法律咨询服务, 将风险控制在安全线以内



通过咨询审计公司, 对公司同用户数据相关的流程进行审计, 帮助企业发现风险内容

如果你是用户!

你只需谨记, 没有经过GDPR认可的设备都谨慎使用!

你该怎么办?



中国云安全与新兴技术安全创新联盟
China Security Alliance of Cloud and Emerging Technology Innovation

CSA CoC -CSA GDPR 合规行为准则

The CSA CoC for GDPR Compliance (CSA GDPR 合规行为准则) 旨在为云服务提供商 (CSP) 和云消费者提供GDPR合规解决方案，并提供涉及云服务提供商应提交的关于数据保护级别的透明性准则。

CSA GDPR 合规行为准则组成部分:

- 隐私水平协议实施规范 (PLA CoP) , 一项技术标准, 具体说明了GDPR中包含的要求
- 与之相关的认证计划和遵守机制。



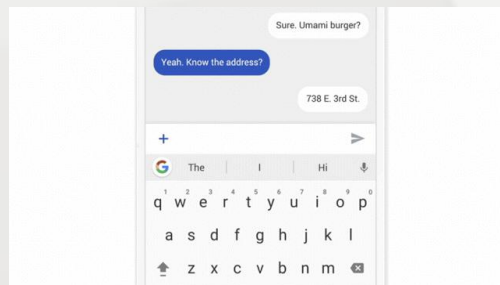
CSA GDPR 合规行为准则旨在提供:

- 为各种规模的云客户提供工具来评估不同云服务提供商提供的个人数据保护水平 (从而支持决策)
- 指导任何规模和地点的云服务提供商, 遵守欧盟 (EU) 个人数据保护法规, 并以结构化的方式披露其提供给客户的个人数据保护级别

AI隐私风险解决方案（场景一）---联合学习 + 安全聚合

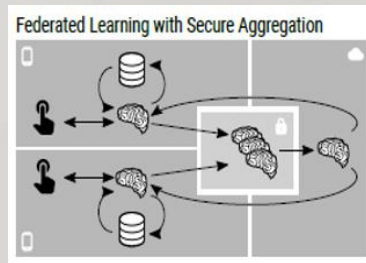
应用场景：

- 输入法搜索推荐
- 根据手机输入习惯改进语言模型
- 根据图片浏览数据改进图片排列



业务价值：

- **保护用户隐私**：在端侧进行学习和运算，训练数据存储在本地；
- **提升机器学习的效率和精度**：利用终端计算能力（AI芯片），提升机器学习效率；通过端云结合的模型更新，提升机器学习的精度



$$\begin{aligned}y_u &= x_u + \sum_{v \in \mathcal{U}: u < v} s_{u,v} - \sum_{v \in \mathcal{U}: u > v} s_{v,u} \pmod{R} \\z &= \sum_{u \in \mathcal{U}} y_u \\&= \sum_{u \in \mathcal{U}} \left(x_u + \sum_{v \in \mathcal{U}: u < v} s_{u,v} - \sum_{v \in \mathcal{U}: u > v} s_{v,u} \right) \\&= \sum_{u \in \mathcal{U}} x_u \pmod{R}\end{aligned}$$

差分隐私 Differential Privacy DP

□ 弥补匿名化的问题

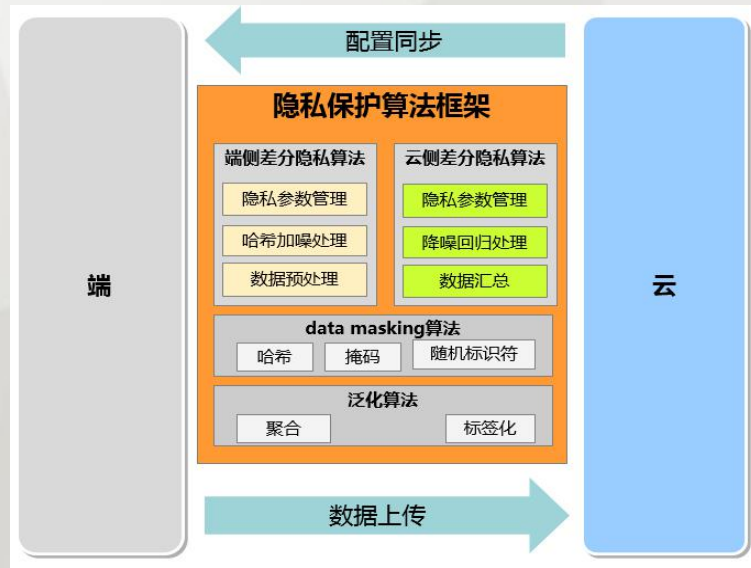
□ 将隐私保护从定性分析，变成定量分析，实现不同方法的量化对比

□ 差分隐私的数学原理

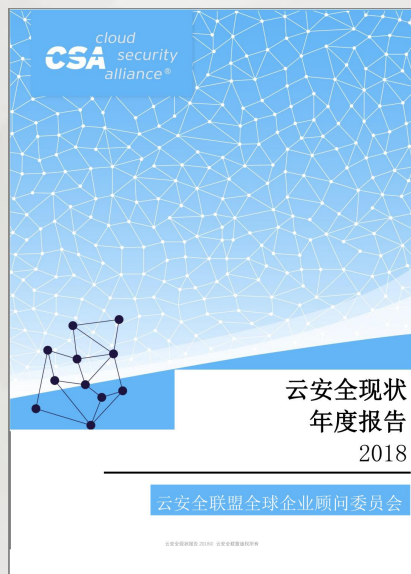
□ 设有随机算法 M ， R 为 M 所有可能输出构成的集合，对于任意两个相邻的数据集 d 和 d' （仅有一行记录的差别）以及 R 的任何子集 S ，若算法 M 满足：对于任何一种可能的查询结果，由两个相邻数据集得出它的概率非常接近

$$\Pr[M(d) \in S] \leq e^\epsilon \Pr[M(d') \in S] + \delta.$$

□ 则称算法 M 提供 (ϵ, δ) -差分隐私保护（DP），其中参数 ϵ 称为隐私保护预算。 ϵ 通常为0-10左右， δ 则通常为 $1e^{-3}$ - $1e^{-8}$ 左右。



《云安全现状年度报告》2018



鸣谢

陈本峰（组长）

李岩、陈皓、罗义兵

刘洁、沈传宝、马韶华

赵锐、杨喜龙、高轶峰

周钰、张全伟、郭迁弟

姚凯、张威

《为实现成功的网络威胁情报交换，构建坚实基础》



鸣谢

沈勇（组长）

冯春进 方 伟 胡泽柱

李建民 罗义兵 马红杰

马韶华 魏琳琳 张 威

下载：<http://www.c-csa.cn/wenxianxiazai.html>

Thank you 谢谢



info@china-csa.org

<http://www.c-csa.cn>