北京大学数据治理高峰论坛2019
2019年1月15日

香港特区的数据治理:
合规、问责、伦理和道德

黄继儿大律师
香港个人资料私隐专员

2018全球逾十四亿人数据被外泄

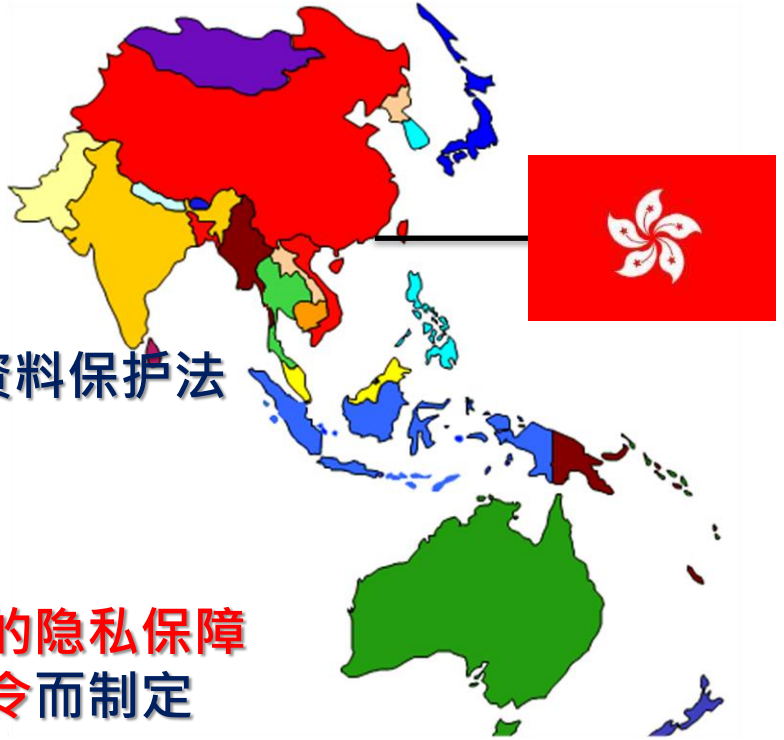
数据外泄事件涉及的公司	涉及数据数量
万豪酒店	3.83亿个用户
Twitter (推特社交网站)	3.3亿个用户
My Fitness Pal (食品及营养应用程序)	1.5亿个用户
Facebook	1.47亿个用户
Quora (问答网站)	1亿个用户
Firebase （ Google旗下的开发平台 ）	1亿个用户
My Heritage (凭借DNA测试寻找祖先及家谱)	9,200万个用户
Uber (出租车公司)	5,700万个账户
Ticket Fly (活动票务网站)	2,700万个账户
Google+	50万个账户
英国航空公司	38万个账户

1

香港《个人资料（私隐）条例》简介

香港法例 第486章《个人资料（私隐）条例》

- 1995年制定
- 独立的个人资料隐私专员
- 亚洲其中一个最早的全面的个人资料保护法
- 涵盖公营（政府）和私营部门
- 参考1980年经济合作与发展组织的隐私保障指引及1995年欧盟的数据保障指令而制定



立法背景

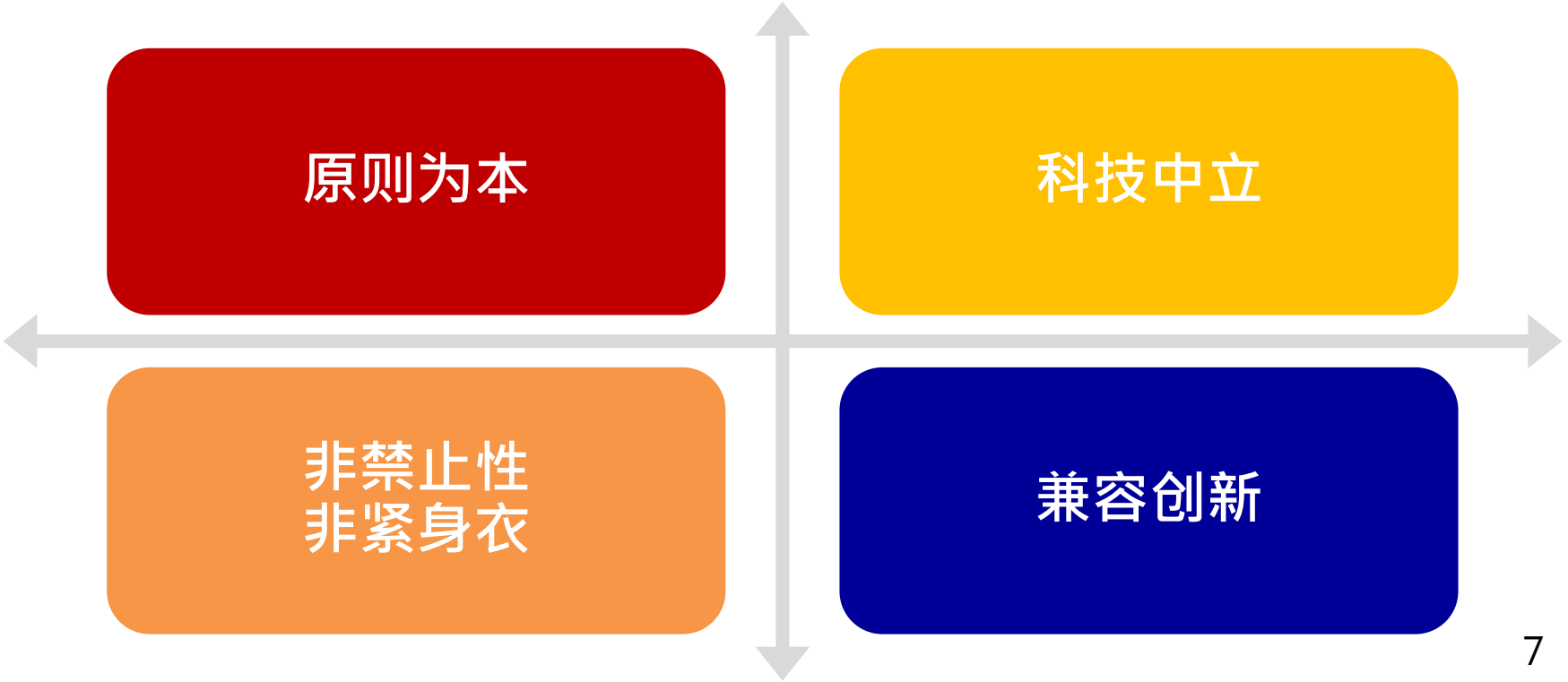
商业

- 便利营商环境
- 维持香港作为金融和贸易中心

人权

- 保护个人的资料隐私

条例的特点



香港个人资料私隐专员公署的角色

独立的监管机构

由私隐专员带领（由香港特别行政区行政长官委任）

执行法定职能并行使条例赋予的权力，例如：

- 教育
- 执法
- 研究
- 立法建议
- 国际联络

条例的主要条文

什么是「个人资料」？

「个人资料」须符合三项条件：

1) 直接或间接与一名在世人士有关

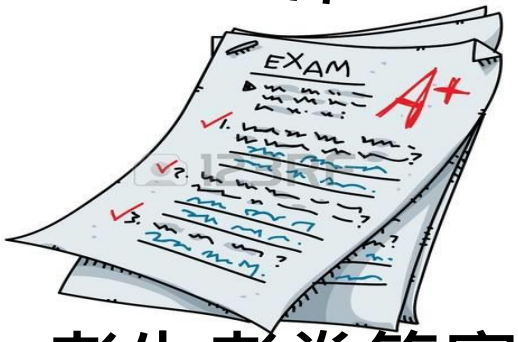
2) 从该等资料直接或间接地确定有关的个人的身分是切实可行的；以及

3) 该等资料的存在形式令予以「查阅」及「处理」均是切实可行的

这些是
个人资料吗？

流言蜚语

指纹资料



考生考卷答案

条例的六项保障资料原则

第1原则 – 收集资料的目的及方式

第2原则 – 准确性及保留期间

第3原则 – 使用

第4原则 – 资料保安

第5原则 – 公开政策

第6原则 – 查阅及更正

第1原则 – 收集料的目的及方式

- 收集目的必须直接与资料使用者的职能或活动有关
- 收集的资料是有实际需要的，而不超乎适度
- 收集的方式必须合法及公平
- 从资料当事人收集数据之时或之前，提供「收集个人资料声明」

第2原则 – 个人资料的准确性及保留期间

- 资料使用者须采取切实可行的步骤，确保所持个人资料的准确性

- 资料使用者须采取切实可行的步骤，确保在完成资料的使用目的后，删除资料

- 如聘用资料处理者处理个人资料，须透过合约规范或其他方法，防止转移予资料处理者处理的个人资料被保存超过所需时间

第3原则 – 个人资料的使用

- 如无当事人的订明同意，个人资料不得用于新目的。

- 容许「有关人士」 于特定情况下代资料当事人提供订明同意， 让资料使用者使用当事人的个人资料于新用途上

- 「新目的」在收集资料时拟使用的目的或直接有关的目的以外的目的

第4原则 – 个人资料的保安

- 资料使用者须采取切实可行的步骤确保个人资料不会经授权或意外的查阅、处理、删除、丧失或其他使用。

- 如聘用资料处理者处理个人资料，须透过合约规范或其他方法，防止转移予资料处理者处理的个人资料未经授权或意外地被查阅、处理、删除、丧失或使用

第5原则 – 资讯须在一般情况下可提供

资料使用者须提供：-

(a) 个人资料的政策及实务

(b) 持有的个人资料的类别

(c) 会为何种主要目的而使用

第6原則 – 查阅个人资料

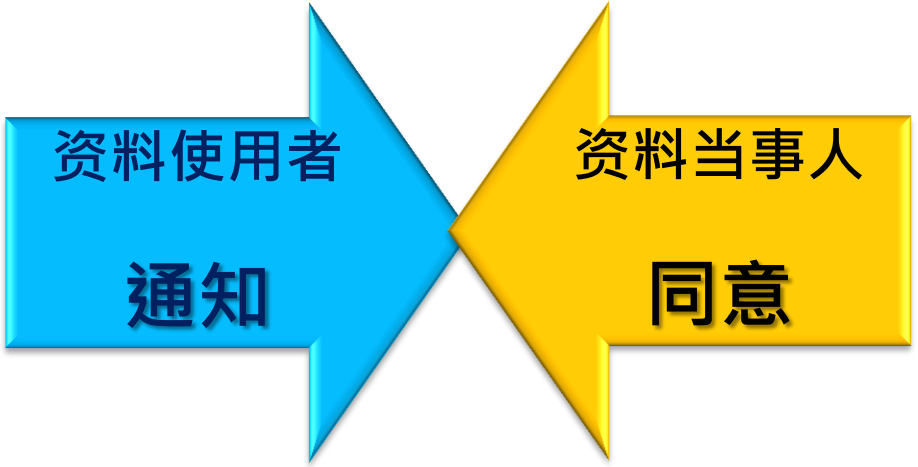
资料当事人有权：-

a) 要求查阅自己的个人资料；资料使用者可收取不超乎适度的费用

b) 要求更改自己的个人资料

直接促销 (条例第6A部)

拟用客户个人资料作直销用途或转交另他人作直销用途



提交个人资料

• 提供「订明信息」及回应途径，让资料当事人选择同意或表示「不反对」个人资料被用作直销 • 通知必须清楚易明	• 必须自愿和清晰作出 • 不反对也属同意

直接促销 (条例第6A部)

- 现行条例规定凡资料使用者在首次使用个人资料于直销活动，须提供一个「拒收直销讯息」的选择予资料当事人
- 如当事人表示拒绝再接收有关的直销资料，资料使用者须在不收费的情况下照办
- 资料使用者如违反关于直接促销的规定，属刑事罪行

与直接促销有关的定罪个案

时期	个案	罚款金额
2015年9月（2012年条例修订后首宗定罪个案）	一间电讯公司没有依从客户的拒收直销讯息要求	被判罚款港币三万元
2015年9月	一间储存服务供货商在直接促销前未有采取指明行动通知当事人及取得其同意	被判罚款港币一万元
2015年11月	一间体检服务公司没有依从客户的拒收直销讯息要求	被判罚款港币一万元
2015年12月	一名人士将在社交场合获取的个人资料提供予第三者作直接促销中使用，但事前未有采取指明行动通知当事人及取得其同意	被判罚款港币五千元

与直接促销有关的定罪个案 (续)

时期	个案	罚款金额
2016年4月	• 一名保险代理人在直接促销前未有采取指明行动通知当事人及取得其同意；及 • 在首次使用个人资料作直接促销时，未有告知资料当事人他有权提出拒收直销讯息要求	被判罚每项控罪各80小时社会服务令
2016年5月	• 一间销售推广公司在直接促销前未有采取指明行动通知客户及取得其同意；及 • 没有依从拒收直销讯息要求	每项控罪分别被判罚款港币八千元
2016年11月	• 四名被告(分别为两间贷款转介服务公司及两名公司的高级人员)被控在使用他人的个人资料作直接促销前,未有采取指明行动通知资料当事人及取得其同意 • 两间公司被裁定罪成 • 两名公司的高级人员则因证据不足获判罪名不成立	两间公司被罚款共16.5万元,并就公司所得的利润的25%,赔偿受害人,共4.78万元
2016年12月	• 一间钟表公司在直接促销前未有采取指明行动通知当事人及取得其同意；及 • 在首次使用个人资料作直接促销时，未有告知资料当事人他有权提出拒收直销讯息要求	每项控罪分别被判罚款港币八千元
2017年1月	• 一间银行没有依从客户的拒收直销讯息要求	被判罚款港币一万元

与直接促销有关的定罪个案 (续)

时期	个案	罚款金额
2017年11月	• 一名理财顾问在使用他人的个人资料作直接促销前未有采取指明行动通知资料当事人及取得其同意，及 • 在首次使用他人的个人资料作直接促销时，未有告知资料当事人他有权要求在不收费的情况下，停止使用他的个人资料。	每项控罪分别被判罚款一万元
2017年12月	• 一间健身公司没有依从客户的拒收直销讯息要求	被判罚款七千元
2018年1月	• 一间超级市场在未获数据当事人同意下，将其个人资料使用于直接促销	被判罚款三千元
2018年1月	• 一间电讯公司没有依从客户的拒收直销讯息要求	被判罚款一万元

条例下的豁免(第8部)

订明在不同情况下，可获豁免而不受保障资料原则所管限，当中包括:

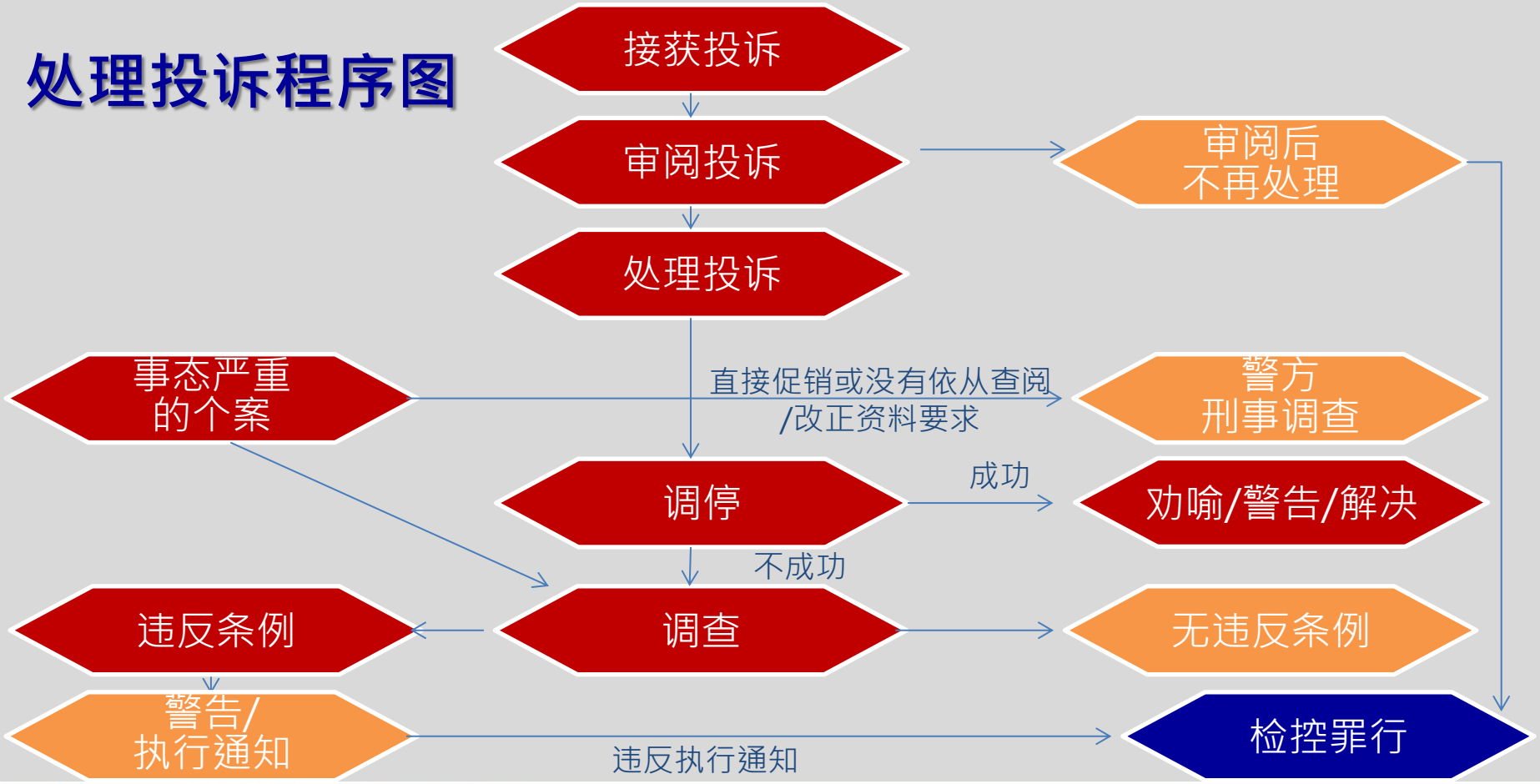
法律条文	豁免情况	适用
第51A条	由法院、裁判官或司法人员在执行司法职能的过程中持有的个人资料	保障资料第1 – 6原则
第52条	由个人持有并只与其私人事务、家庭事务或家居事务有关的个人资料；或只是为休闲目的而如此持有的个人资料	保障资料第1 – 6 原则
第53条 – 第55条	与指定雇佣程序（例如升职）有关的个人资料	保障资料第6 原则
第56条	由资料使用者持有并包含个人评介的个人资料，涉及由一名个人在职业以外的过程中作出，并与另一名个人就职位的合适程度有关	保障资料第6 原则

条例下的豁免(第8部) (续)

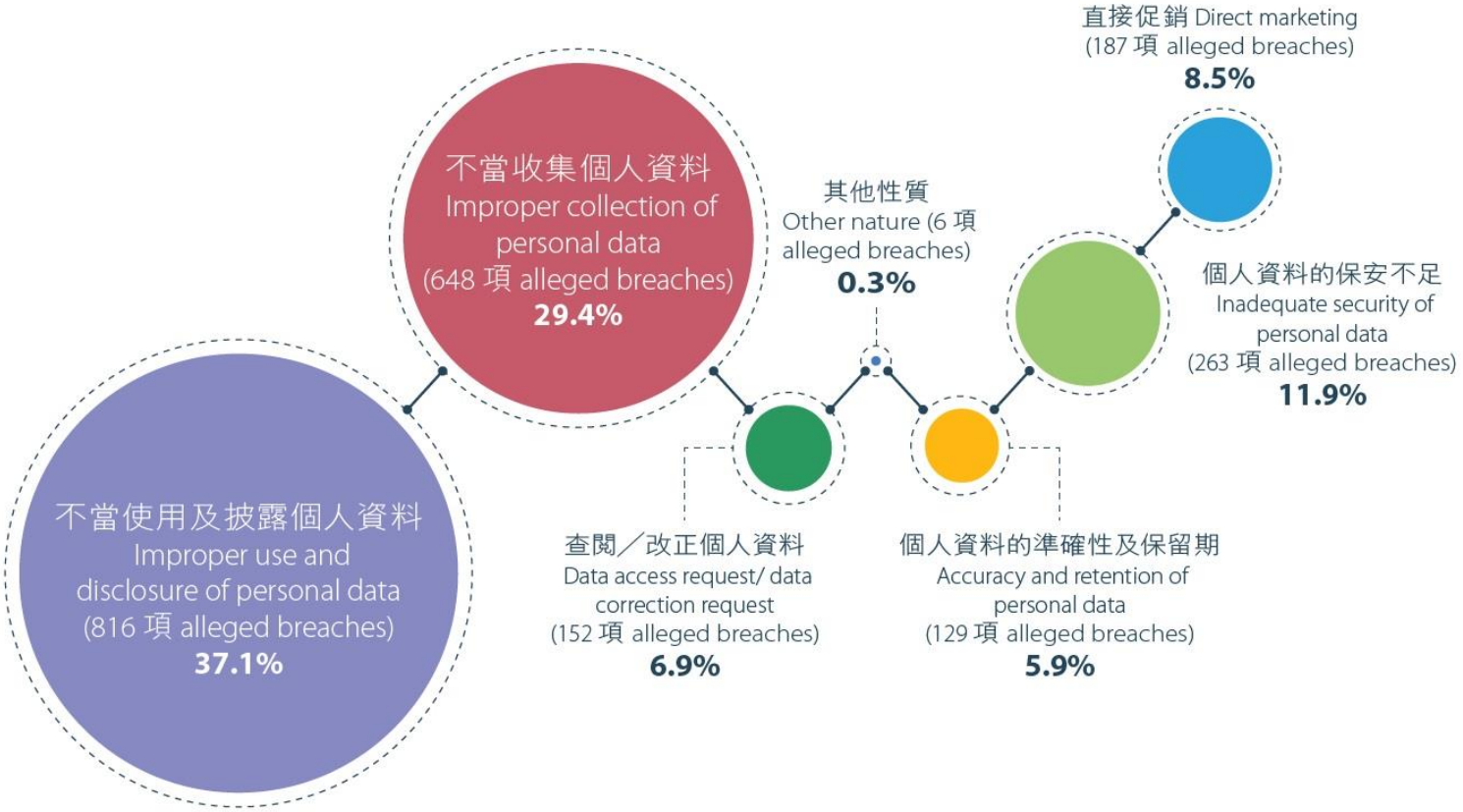
订明在不同情况下，可获豁免而不受保障资料原则所管限，当中包括:

法律条文	豁免情况	适用
第57条	由政府持有为保障香港的保安、防卫或国际关系的目的的个人资料	保障资料第3及第6原则
第58条	为防止罪行或严重不当行为等目的而持有的个人资料	保障资料第3及第6原则
第59条	关乎资料当事人的身体健康或精神健康、身份或所在的个人资料	保障资料第3及第6原则
第60条	法律专业保密权	保障资料第6原则
第61条	由从事新闻活动的资料使用者持有，或向有关资料使用者披露资料是符合公众利益	保障资料第3及第6原则
第62条	用于统计或研究而所得成果不能识辨个人身份	保障资料第3原则

处理投诉程序图


接获投诉
审阅投诉
审阅后
不再处理
处理投诉
事态严重
的个案
直接促销或没有依从查阅
/改正资料要求
警方
刑事调查
调停
成功
劝喻/警告/解决
不成功
违反条例
调查
无违反条例
警告/
执行通知
检控罪行
违反执行通知

2017-18涉嫌违反条例规定的投诉性质



处理资料外泄事故

由资料使用者通报事故

由公署主动作出(条例第8条)

循规审查 (条例第8条)
- 查找事实
- 确认原因
- 评估将/已采取的措施成效

- 有违反条例的表面证据
- 资料当事人数目众多
- 涉及敏感的个人资料
- 牵涉重大的公众利益
- 传媒广泛报道

循规调查(条件第38(b)条)

权力
- 进入资料使用者的处所视察其个人资料系统 (条例第42条)
- 进行公开聆讯及会见证人(条例第43条)
- 传召相关人士提供证据(条例第44条)

提供建议/协助

及时采取补救措施/ 作出承诺

结案

没有违反条例

调查结果 (条例第47条)

及时采取补救措施/ 作出承诺

违反条例

警告 (视乎情况需要)

执行通知 (条例第50条)
- 补救措施
- 完成日期
- 通知公署已遵行有关执行通知

牵涉公众利益

违反执行通知

结案

发表调查报告(条例第48条)

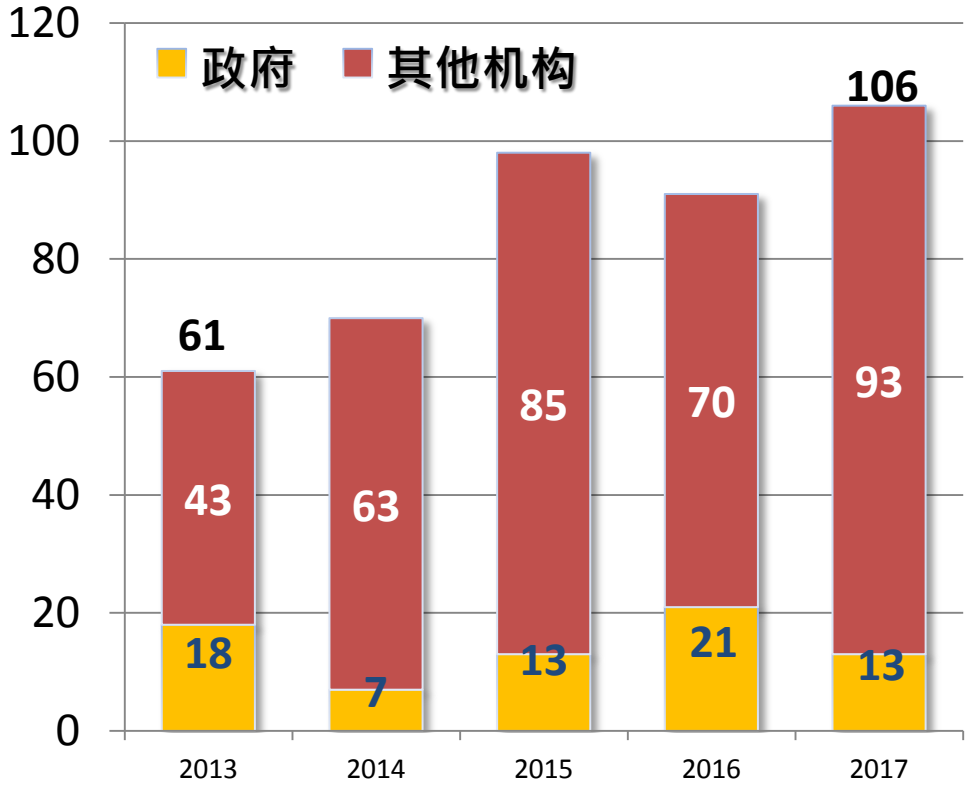
交由警方作刑事调查

征询律政司意见

结案

检控

公署接获的资料外泄通报



年度	涉及资料当事人数量
2013年	90,000
2014年	47,000
2015年	871,000
2016年	104,000
2017年	3,866,000

2

数据保障法规的最新发展

资料保护格局概述

欧盟

- 《通用数据保障条例》于2018年5月25日生效
- 严格而全面的资料保护法

美国

- 联邦级别没有全面的数据保护法
- 较强的行业性法规（例如，健康数据，信用数据）
- 所有州都有强制性资料外泄通报制度

亚洲

- 数据保障法规的数目正增加
- 一般参照欧盟的模式，但相对宽松

GDPR 通用数据保障条例

对自己的个人资料有更多的控制权

适用于在欧盟运营的所有公司的一套规则

企业受益于公平的竞争环境

GDPR 技术和数数据自由流动

GDPR 序言 6:

"Rapid technological developments and globalisation have brought new challenges for the protection of personal data. … Technology… should further facilitate the free flow of personal data … while ensuring a high level of the protection of personal data."

GDPR – 主要目标

The digital information ecosystem farms people for their attention, ideas and data in exchange for so called 'free' services. …[The GDPR] aims to restore a sense of trust and control over what happens to our online lives.

Giovanni Buttarelli,
European Data Protection Supervisor

Source:
https://edps.europa.eu/press-publications/press-news/blog/accept-and-continue-billions-are-clocking-digital-sweat-factories_en

GDPR – 主要目标

*[The GDPR] is about **putting the rights of individuals first** and upgrading the EU data protection rules so that they are efficient and ready for the future.*

Andrea Jelinek,
Chair of the European Data Protection Board

Source:
https://edpb.europa.eu/news/news/2018/europes-new-data-protection-rules-and-edpb-giving-individuals-greater-control_en

GDPR – 主要目标

The GDPR gives consumers more control over their data. … But arguably the biggest change is around accountability. … The GDPR mandates organisations to put into place comprehensive but proportionate governance measures.

Elizabeth Denham,
Information Commissioner of the UK

Source:
https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/01/gdpr-and-accountability/

GDPR - 将控制权归还给个人

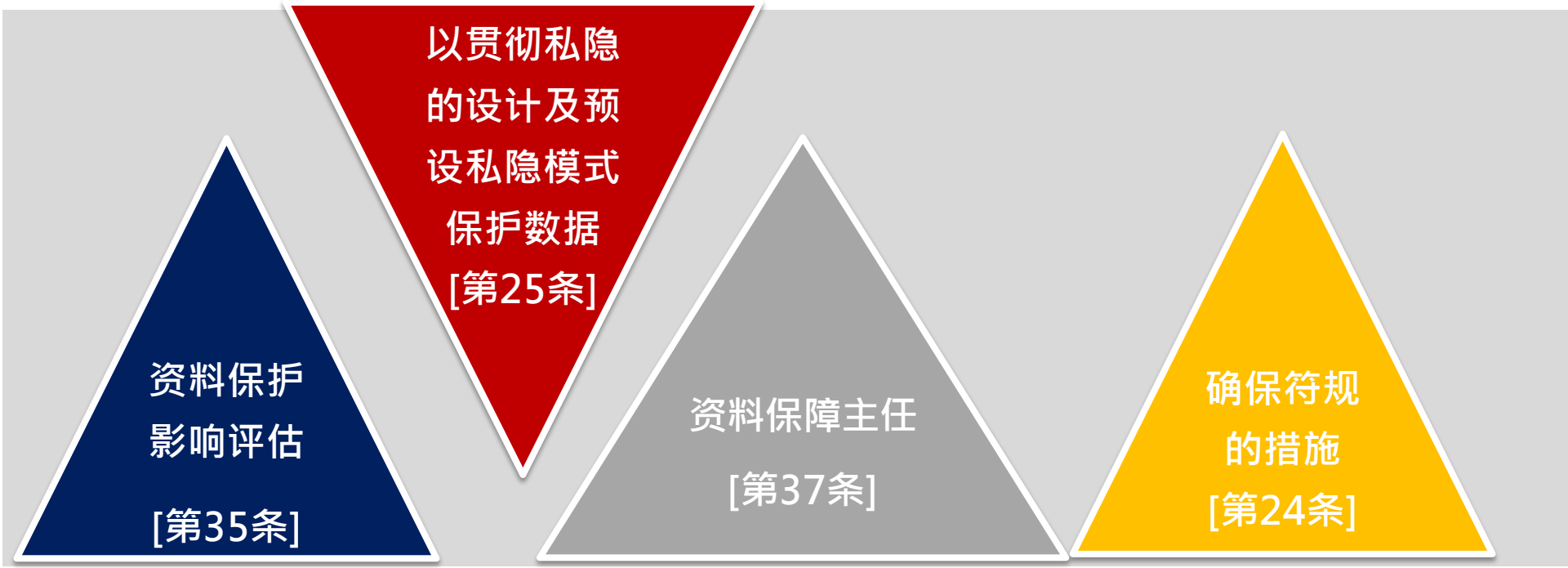
- 被遗忘权
- 资料可携权
- 反对处理权等

增强权利

- 知情
- 明确
- 自愿给予
- 具体

加强同意

GDPR - 问责性


以贯彻私隐的设计及预设私隐模式保护数据 [第25条]
资料保护影响评估 [第35条]
资料保障主任 [第37条]
确保符规的措施 [第24条]

GDPR

强制资料外泄通报

- 风险为本

- 72小时内

GDPR

行政 罚款

最高为营业额的4% 或

2000万欧元

1. 适用范围 (境外执法权)

欧盟通用数据保护条例	香港个人资料（私隐）条例
• 适用于资料控制者与资料处理者 • 涵盖在欧盟设立的机构，以及在欧盟之外设立，但有向欧盟的个人提供商品或服务，或监控欧盟个人的行为的机构 [第3条]	• 只适用于资料使用者 • 资料使用者必须在或从香港控制个人资料的收集、持有、处理或使用。[第2(1)条]

2. 问责和管治

欧盟通用数据保护条例	香港个人资料（私隐）条例
订立基于风险的问责制度，资料控制者需要： • 实施措施以确保合规 [第 24条] • 采用「贯彻私隐的设计」(Privacy by Design) 及「预设私隐模式」(Privacy by Default) [第25条] • 对高危的资料处理进行资料保护影响评估[第35条] • (对于某些类别的组织机构) 委任资料保障官 [第37条]	并无规定执行问责制及相关的私隐管理工具 私隐专员倡导「私隐管理系统」，体现问责原则，当中资料保障官的任命和私隐影响评估的实施被推荐为实现问责制的良好实践 

3. 强制资料外泄通报

欧盟通用数据保护条例	香港个人资料（私隐）条例

• 除例外情况(如有关泄露不会构成私隐风险），资料控制者必须在没有不适当延迟的情况下：
  • 向资料保障机关通报资料外泄事故
  • 通知受影响的资料当事人
[第33-34条]
	• 没有强制要求通报资料外泄事故
	• 采取自愿通报制度

4. 敏感个人信息

欧盟通用数据保护条例	香港个人资料（私隐）条例
• 扩大敏感个人数据的类别（如基因和生物辨识资料） • 只有在特定的情况下（例如资料当事人明确同意）才允许对敏感的个人资料进行处理 [第9条]	• 没有区分敏感的和非敏感的个人资料

5. 同意

欧盟通用数据保护条例	香港个人资料（私隐）条例
同意必须 • 在自愿和知情下给予 • 通过声明或明确的肯定行动以表达资料当事人的意愿 [第4(1)条]	• 同意并不是收集和使用个人资料的先决条件，除非个人资料被用于新的目的 [保障资料第1 及 3原则]

6. 资料处理者的责任

欧盟通用数据保护条例	香港个人资料（私隐）条例
• 资料处理者被附加了额外的义务，例如： ✓维护资料处理纪录 ✓确保资料保安 ✓作资料外泄通报 ✓委任资料保护官 [第30, 32-33, 37条]	• 资料处理者不受直接规管 • 资料使用者需要采用契约或其他方式来确保资料处理者在资料保安和资料保存期方面合规 [保障资料第2及4原则]

7. 资料当事人的新增或强化权利

欧盟一般数据保护法规	香港个人资料（私隐）条例
• 要求删除个人资料的权利 (也被称为“被遗忘权”) [第17条] • 资料转移权[第20条] • 反对处理的权利[第21条] • 对「汇编个人档案」(profiling) 作出定义及进行规管 [第4(4)条] • 增加了须向资料当事人提供的信息（例如个人资料的来源及资料保存期限）[第13、14条]	• 一般没有要求删除资料的权利，但资料使用者不得保存个人资料超过必要的期限[第26 条及保障资料第2原则] • 没有数据转移的权利 • 没有反对处理资料的权利，但是资料当事人可以选择拒收直销信息[第35G & 35L条]

8. 验证机制及跨境资料转移

欧盟通用数据保护条例	香港个人资料（私隐）条例
• 明确认可私隐保障验证机制，以证明资料控制者和处理者在处理个人资料方面的合规性 [第42条] • 认可以符合验证作为跨境资料转移的法律基础之一 [第46条]	• 没有验证机制

9. 制裁

欧盟通用数据保护条例	香港个人资料（私隐）条例
• 资料保障机关可对资料控制者和处理者处以行政罚款。[第58条] • 根据违规的性质，罚款可能高达2000万欧元，或全球年度营业额的4%。[第83条]	• 私隐专员无权征收行政罚款 • 私隐专员可向违规的资料使用者发出执行通知。

3

从合规到问责和伦理道德

数字经济中的隐私挑战

- “资料垄断者”滥用主导地位
- 消费者缺乏控制权和真正的选择

竞争

隐私

- 过度及隐蔽式的资料收集
- 敏感信息曝光
- 非预期，不公平/歧视性地使用资讯
- 没有意义的同意

资料安全

跨范畴和跨境问题

- 黑客入侵
- 资料外泄

- 消费者保护
- 跨境数据流通

解决方案：问责制和伦理道德

以风险为本的问责制

"GDPR 带来的最大变化是围绕问责制"
Elizabeth Denham, Information Commissioner of the UK

"GDPR旨在恢复我们对网络生活中所发生的事情的信任和控制."
Giovanni Buttarelli, European Data Protection Supervisor

问责制：隐私管理系统（PMP）

好处

- 有效管理个人资料
- 最大限度地降低隐私风险
- 有效处理资料外泄事件
- 展示符规和问责性

PMP – 主要组件

1. 機構的決心

- 1.1 最高管理層的支持
- 1.2 委任保障資料主任 / 設立保障資料部門
- 1.3 建立匯報機制

PMP – 主要组件

2. 系統管控措施

- **2.1** 個人資料庫存
- **2.2** 處理個人資料的內部政策
- **2.3** 風險評估工具
- **2.4** 培訓及教育推廣
- **2.5** 資料外洩事故的處理
- **2.6** 對資料處理者的管理
- **2.7** 溝通

PMP – 主要组件

3. 持續評估及修訂

3.1 制定監督及檢討計劃 ..... 3.2 評估及修訂系統管控措施

《资料保障．利便营商 — 给中小企的纲领提示》

- 协助中小企了解私隐条例的规定
- 深入浅出解释相关法规
- 提供切合中小企运作模式的具体合规例子和实用建议

伦理道德与信任

提倡伦理道德：“处理数据的正当性计划”

顾问公司的研究方向

(2018年10月23日在比利时布鲁塞尔发布)

找出数据伦理道德的含义及核心价值

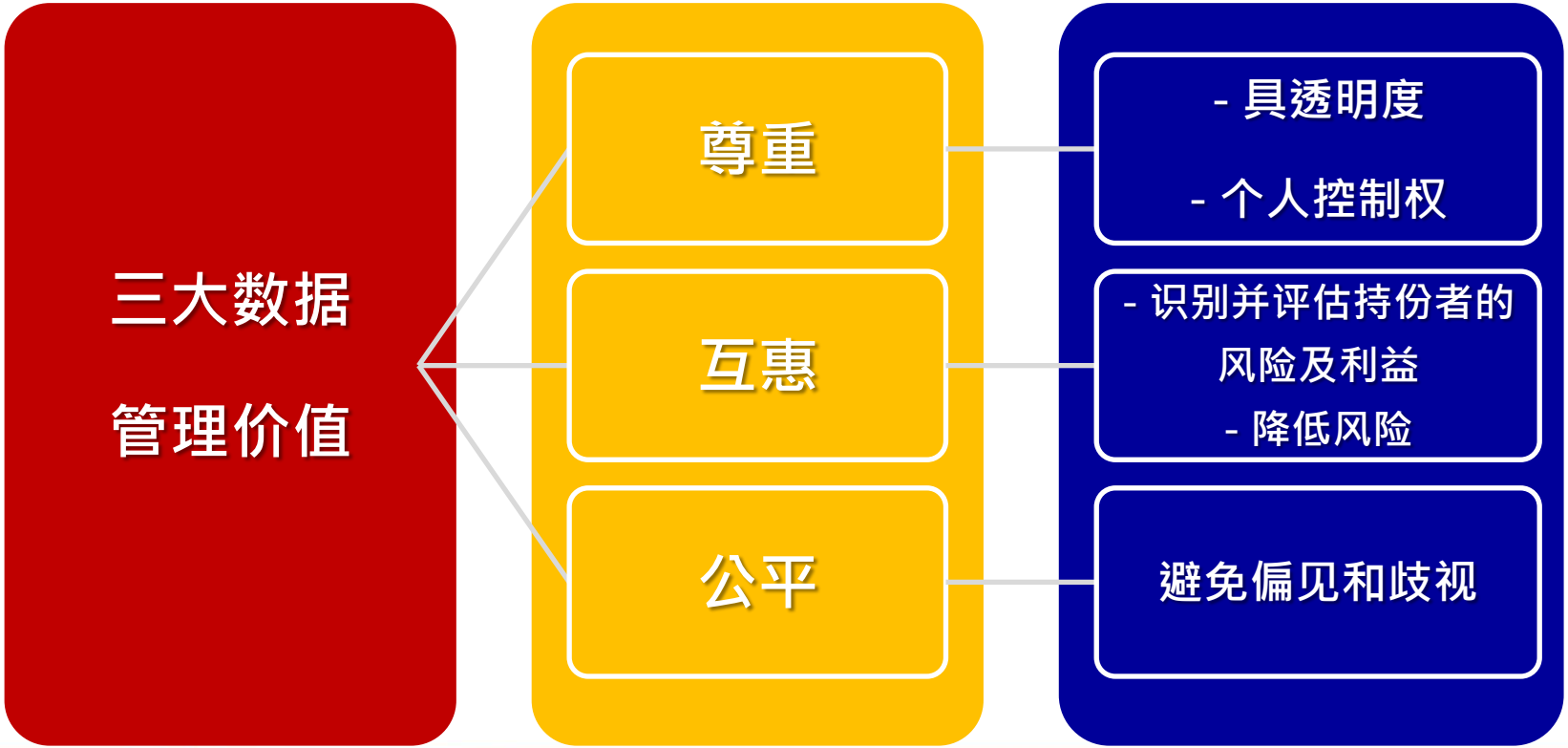
提供将数据伦理道德核心价值付诸实践的工具

鼓励企业在日常运营中恪守数据伦理道德

伦理道德	• 一套文化规范，当中结合群体的共同价值和指导信念
价值	• 个人及社会秉持及使用的核心信念和理想 — 以商业机构而言，则为其经营的目标
原则	• 在营商或投资策略的环境下的价值观表述，并会引申为机构的政策及营运指引
执行	• 政策、程序、培训、工具、行为 / 实务守则
核实	道德数据影响评估模式 / 流程监督模式

有道德的数据管理问责

核心价值



实用工具

- “我们必须确保科技是为人类服务，而非相反情况。”
- “没有人民对科技的完全信任，我们永远不能获取科技的真正潜能。”
- “我们不应因为有须要做而做，我们因为应当做所以才去做。”

苹果公司首席执行官 库克

第四十届国际资料保障及私隐专员会议（布鲁塞尔）演说

“信任是新的黃金”

Andrea Jelinek,
Chair of European Data Protection Board

公署的策略重点

推动、鼓励

提供诱因

尊重私隐
文化


私隱管理系統
Privacy Management Programme
最佳行事方式指引
A Best Practice Guide
「处理数据的正当性」
研究报告
欧洲联盟
《通用数据保障条例》
2016
6 保障資料原則
Data Protection Principles
PCPD.org.hk
1 收集目的及方式 Collection Purpose & Means
2 準確性、儲存及保留 Accuracy & Retention
3 使用 Use
4 保安措施 Security
5 透明度 Openness
6 查閱及更正 Data Access & Correction
香港個人資料私隱專員公署
Privacy Commissioner for Personal Data, Hong Kong
「处理数据的正当性」
新闻稿

谢谢！