![HKPC logo]

**Hong Kong
Productivity Council
香 港 生 產 力 促 進 局**

What Should We Do to Comply with GDPR

**All-round Productivity Partner
全方位企業伙伴**

Agenda

Introduction of GDPR

Potential Risks

Recommendation

Introduction of GDPR

Objectives

The General Data Protection Regulation (GDPR) is a regulation in EU law on **data protection and privacy.**

GDPR

2018	
May	25

Who — • will be protected

Where — • will be covered

What — • will be protected

Who will be Protected

Natural Persons

- It relates "to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data."
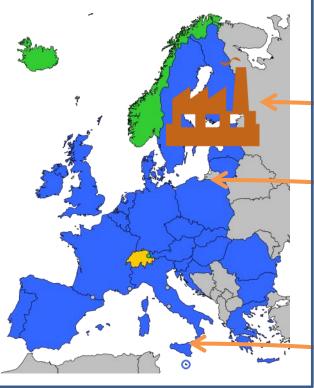
- Online Customers
- Guests
- Complainant
- Supplier Representative
- Employee

Where it will be covered
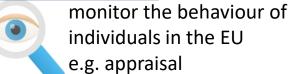

European Union

European Economic Area

has an establishment in the EU. According PCPD, examples will be :
- Presence of sales offices,
- Appointment of sales agent or representative

offer goods or services,
e.g. use of a language or a currency of one or more member states in ordering goods and services (PCPD)

monitor the behaviour of individuals in the EU
e.g. appraisal

COMPANY

Extra-territorial application of the GDPR

What it will be Protected – Personal Data

Under the GDPR, the "special categories" of personal data refer to any information relating to an identified or identifiable natural person

Identification Numbers	Name	Location Data	Health Information	Biometric data	Genetic	And …..

- online identifier
- Economic Identity
- Cultural Identity
- Social Identity…. etc.

What it will be Protected – Personal Data

7 Data Protection Principles

1. Lawfulness, Fairness And Transparency

2. Purpose Limitation

3. Data Minimization

4. Accuracy

5. Storage Limitation

6. Integrity and Confidentiality

7. Accountability

Mandatory Breach Notification

Data controller must report a personal data breach no later than

72 HOURS

to the **supervisory authority** after becoming aware of the breach, unless the breach has a low risk to the individual's rights.

Potential Risks

Loss

- €20M ，or
- 4% of global total turnover last financial year
- <u>Whichever is higher</u>

歐盟新例生效 fb及Google被指控

讚好 0 分享

歐盟實施的《一般個人資料保護規則》（General Data Protection Regulation，GDPR）昨起生效，各大企業收集個人資料時會受到更多限制，Google及Facebook等科網巨企即日已面臨指控。

在GDPR生效後不久，Facebook、Google、Instagram及WhatsApp隨即被指控它們違反GDPR，分別向奧地利、比利時、法國和德國的監管部門舉報。

On the first day of GDPR enforcement, Facebook and Google have been hit with a raft of lawsuits accusing the companies of coercing users into sharing personal data. The lawsuits, which seek to fine Facebook 3.9 billion and Google 3.7 billion euro (roughly $8.8 billion in dollars), were filed by Austrian privacy activist Max Schrems, a longtime critic of the companies' data collection practices.

最严隐私法案上线，一批新闻网站、游戏和广告公司暂停欧洲服务 《洛杉矶时报》、《芝加哥论坛报》、网游《仙境传说》

2018-05-28 18:40   游戏 / 公司 / 隐私

自上周五起，欧洲《通用数据保护条例》（简称 GDPR）正式生效。GDPR 的正式生效进一步显示了其对于广告行业、科技公司、内容出版商以及游戏业的影响力。
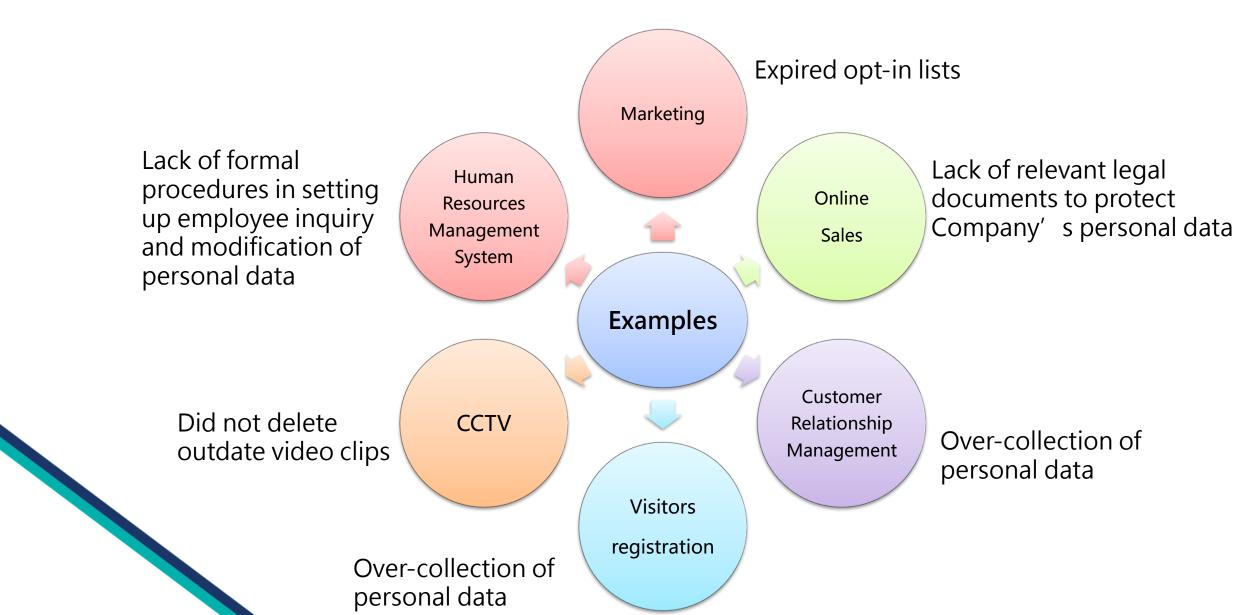

受歐盟私隱保護法影響 小米旗下智能燈停止服務

yeelight 灯泡

讚好此文 讚好 1,272 分享

五月 27, 2018 · 生活科技 ·

有沒有想過我們家中的智能家電突然停止服務，會令生活帶來多少影響？歐盟的全新私隱保護法例（GDPR）日前正式實施，竟然令小米旗下智能燈飾產品 Yeelight 在歐洲無法使用，公司宣佈由於無法滿足歐盟 GDPR 要求，所以要停止向歐洲用戶提供服務。

Potential Risks – Lack of Clear Guidelines

Potential Risks – Inappropriate Access of Personal Data

南京一公务员利用职务之便 泄露82万条公民信息

现代快报记者了解到，1965年出生的朱某是南京某机关单位的工作人员。从2010年起，朱某在南京某机关单位担任副主任科员、主任科员期间，利用职务便利，应朋友刘某、王某的要求，超越职权下载了一些公民个人信息，并将这些信息分别提供给他们使用，造成大量的公民个人信息泄露。经统计，2010年4月至2016年9月，朱某向刘某提供公民个人信息70余万条，2011年11月至2016年7月，朱某向王某提供公民个人信息12余万条。

顺丰员工出卖千万条用户信息被判刑快递信息泄露折射行业安全之痛

近日，一起侵犯公民个人信息的案件在湖北荆州中级人民法院审理宣判，判决书显示，11名顺丰员工及8名相关人员被判处侵犯公民个人信息罪，分别被处以有期徒刑10个月到3年不等。在民众日益重视信息安全的当下，这起快递公司员工"监守自盗"的案件引起了社会的关注。快递信息泄露问题层出

50亿条公民信息泄露 京东前员工牵涉其中

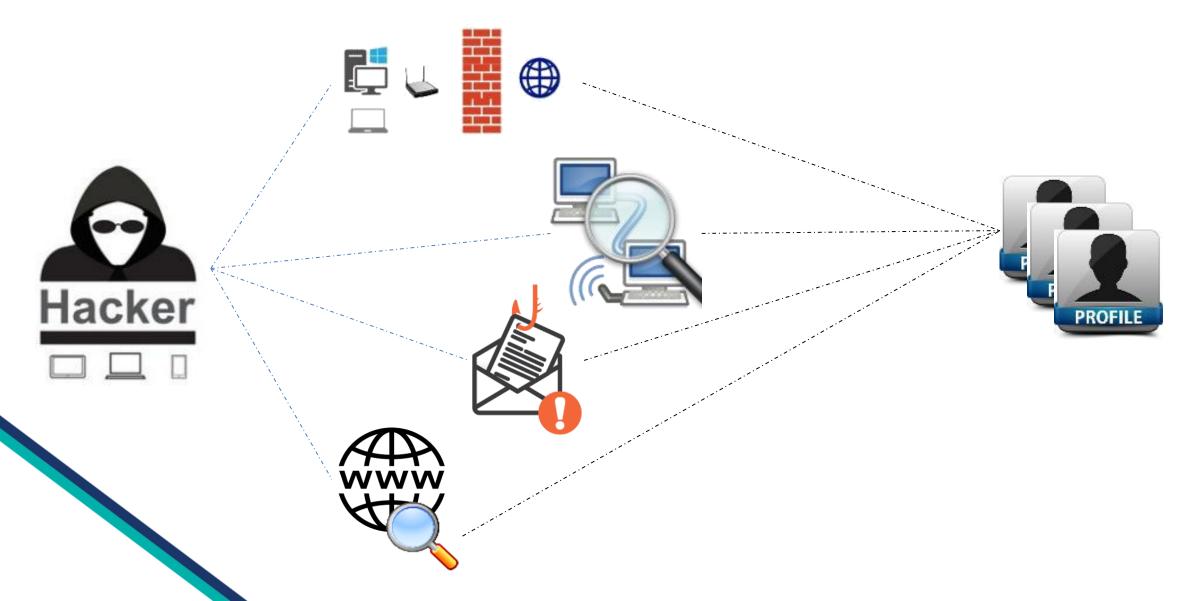有知情人士称，犯罪嫌疑人郑某鹏在加入京东之前曾在国内多家知名互联网公司工作，其泄露的50亿条公民信息中，可能包含多家互联网公司的用户信息。

可口可乐员工个人信息被泄露 人数达8000人！

A5创业网（公众号：iadmin5）5月28日报道，可口可乐近日对外宣布一起数据泄露事件，他们在前员工的个人硬盘中，发现大量现有员工的个人数据。这些数据是该员工从可口可乐违规挪用的，涉及人员达8000人。

Potential Risks - Hacking

Potential Risks – Competitors

European capital Law GDPR was officially launched. There are non-official groups have lodge complaints to Google, Facebook, WhatsApp and Instagram. In other words, **anyone, including competitors can file a complaint.**
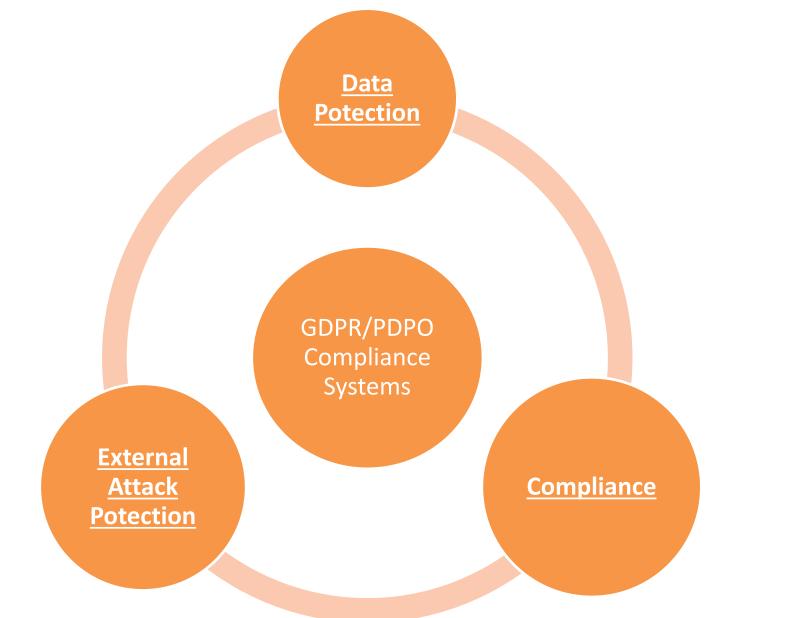
澳洲隱私權律師Max Schrems旗下非營利法律網站noyb.eu，在四項控訴案中代表用戶控訴Google及臉書強迫使用者同意他們蒐集及處理用戶資料的條款。他向法國隱私主管機關CNIL控告Google，而其他三項申訴案則分別向奧地利、德國漢堡及比利時主管機關針對臉書、WhatsApp及Instagram三項產品控告。

「數位權利中心」（Center of Digital Rights）也正準備控告網路公司非法將用戶資料用於發送廣告，或是單純將用戶使用廠商網頁認定為同意他們處理用戶資料。

Recommendation

System Check-up & Data Protection Tools

Data Potection

GDPR/PDPO Compliance Systems

External Attack Potection

Compliance

Data Protection

Whose	• personal data is collected
What	• personal data is collected
When	• personal data is collected
Where	• the personal data is stored
How	• the personal data is collected, proceeded and protected

Comply with GDPR?

7 Data Protection Principle

1. Lawfulness, Fairness And Transparency
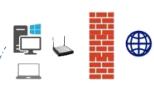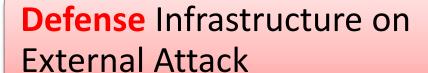
2. Purpose Limitation
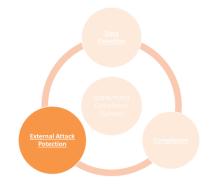
3. Data Minimization

4. Accuracy

5. Storage Limitation
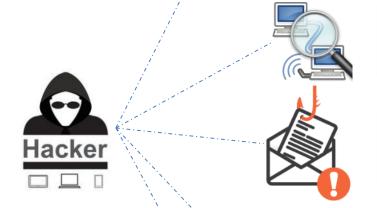
6. Integrity and Confidentiality

7. Accountability

External Attack Protection

Defense Infrastructure on External Attack

Control on Vulnerability
(e.g. Missing Patches, Weak or default passwords)

Prevent leakage through fake email
(e.g. Phishing email)

Protect Web Site
(e.g. e-shop is attacked by SQL injection)

Enforce Awareness

Policy Compliance (GDPR) Procedure

Personal data collection statement for customers

Personal data collection statement for employees

Consent form for obtaining data subject's consent to the processing of their personal data
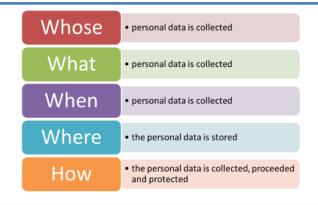
Data breach notification form to a competent supervisory authority

Data breach notification form to an affected data subject

HKPC Personal & Privacy Data Compliance & Protection Services

1. Personal Data Protection Assessment

Discover : Personal Data Inventory

Whose	• personal data is collected
What	• personal data is collected
When	• personal data is collected
Where	• the personal data is stored
How	• the personal data is collected, proceeded and protected

Assess : Privacy Impact Assessment

7 Data Protection Principle

1. Lawfulness, Fairness And Transparency
2. Purpose Limitation
3. Data Minimization
4. Accuracy
5. Storage Limitation
6. Integrity and Confidentiality
7. Accountability

HKPC Personal & Privacy Data Compliance & Protection Services

2. External Attack Protection & Awareness Training

Defense : Review Infrastructure Protection

Protect: Web Site Security Scanning

Control: Network Vulnerability Scanning

Prevent: Phishing Mail Test

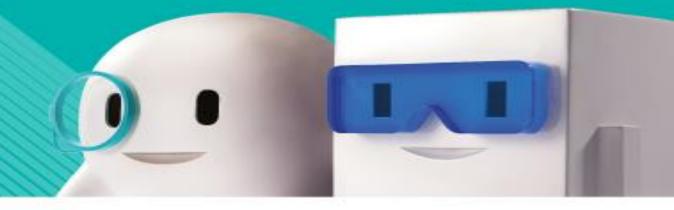**Enforce** : Staff Awareness Training

Thank you!

Terrence Cheung
Consultant / IT Division
Hong Kong Productivity Council
Tel.: 2788-5969
Email: terrencecheung@hkpc.org

All-round Productivity Partner
全方位企業伙伴