

Cloud Expo Asia

18 May 2016

**Building Trust in the Cloud Era - Protect,
Respect Personal Data**

Stephen Kai-yi Wong

Privacy Commissioner for Personal Data, Hong Kong



香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

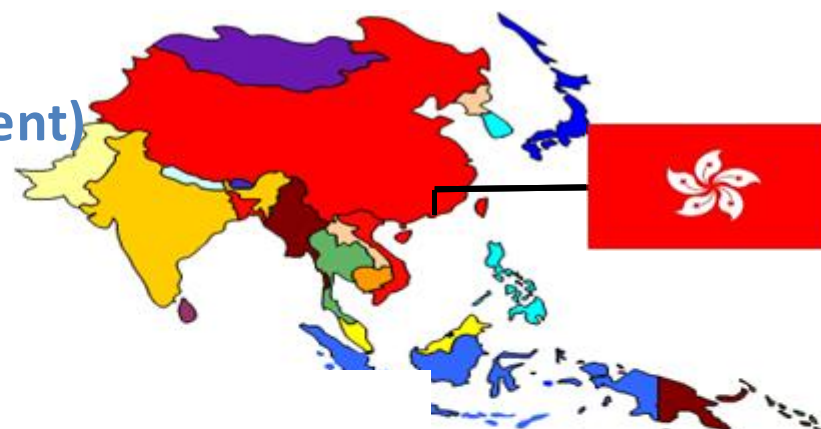
保障、尊重個人資料
Protect, Respect Personal Data

PCPD.org.hk

The Hong Kong Data Protection Law

The Personal Data (Privacy) Ordinance 1995 (the Ordinance)

- comprehensive and stand-alone
 - covering the public (government) and private sectors
- referenced to OECD Privacy Guidelines and 1995 EU Directive
- enforced by an independent statutory regulatory body – the Privacy Commissioner for Personal Data



1



香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

保障、尊重個人資料
Protect, Respect Personal Data

PCPD.org.hk

The Personal Data (Privacy) Ordinance



2



香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

保障、尊重個人資料
Protect, Respect Personal Data

PCPD.org.hk

Principle 1 – Purpose and Manner of Collection



- related purpose
- lawful and fair means
- adequate but not excessive

e.g. collection of fingerprints for attendance is excessive



3



Principle 1 – Purpose and Manner of Collection



- purposes
- classes of transferees
- obligatory/voluntary
- consequences for failure to supply when obligatory
- contact details for access/correction



4



香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

保障、尊重個人資料
Protect, Respect Personal Data

PCPD.org.hk

Principle 2 – Accuracy and Duration of Retention



- practicable steps to ensure accuracy



5



香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

保障、尊重個人資料
Protect, Respect Personal Data

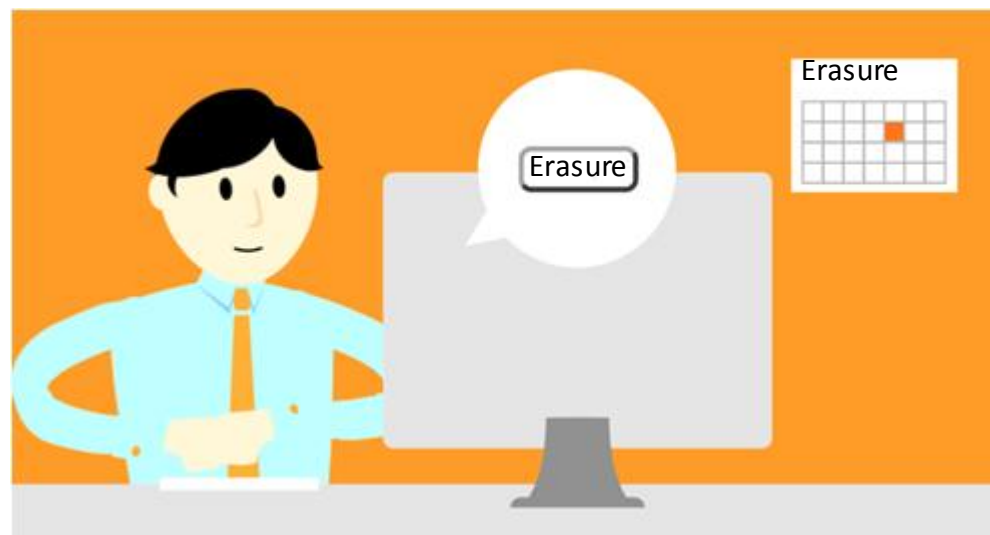
PCPD.org.hk

Principle 2 – Accuracy and Duration of Retention



- personal data not kept longer than necessary for the purpose

e.g. personal data of unsuccessful insurance applicants should not be retained by insurer indefinitely



6



Principle 3 – Use of Personal Data



- not being used for a new purpose without prescribed consent

e.g. posting of compliant letter openly showing details of complainant without consent may contravene DPP3



7



Principle 4 – Security of Personal Data



- practicable steps to ensure no unauthorized or accidental access, processing, erasure, loss, use and transfer
- security in the storage, processing and transmission of data



e.g. loss of unencrypted USB drive with personal data

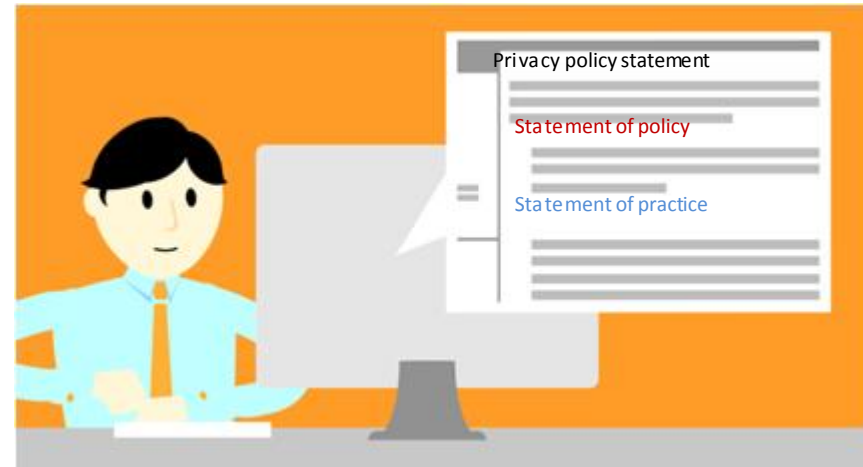
8



Principle 5 – Openness – Information be Generally Available



- policies and practices in relation to personal data
- kinds of personal data held
- main purposes for which personal data are used



e.g. apps accessing data on smartphone should show privacy policy⁹



Principle 6 – Access to Personal Data



- access right
- correction right

e.g. patients of the Electronic Health Record scheme may request access to the data shared by all their health care providers



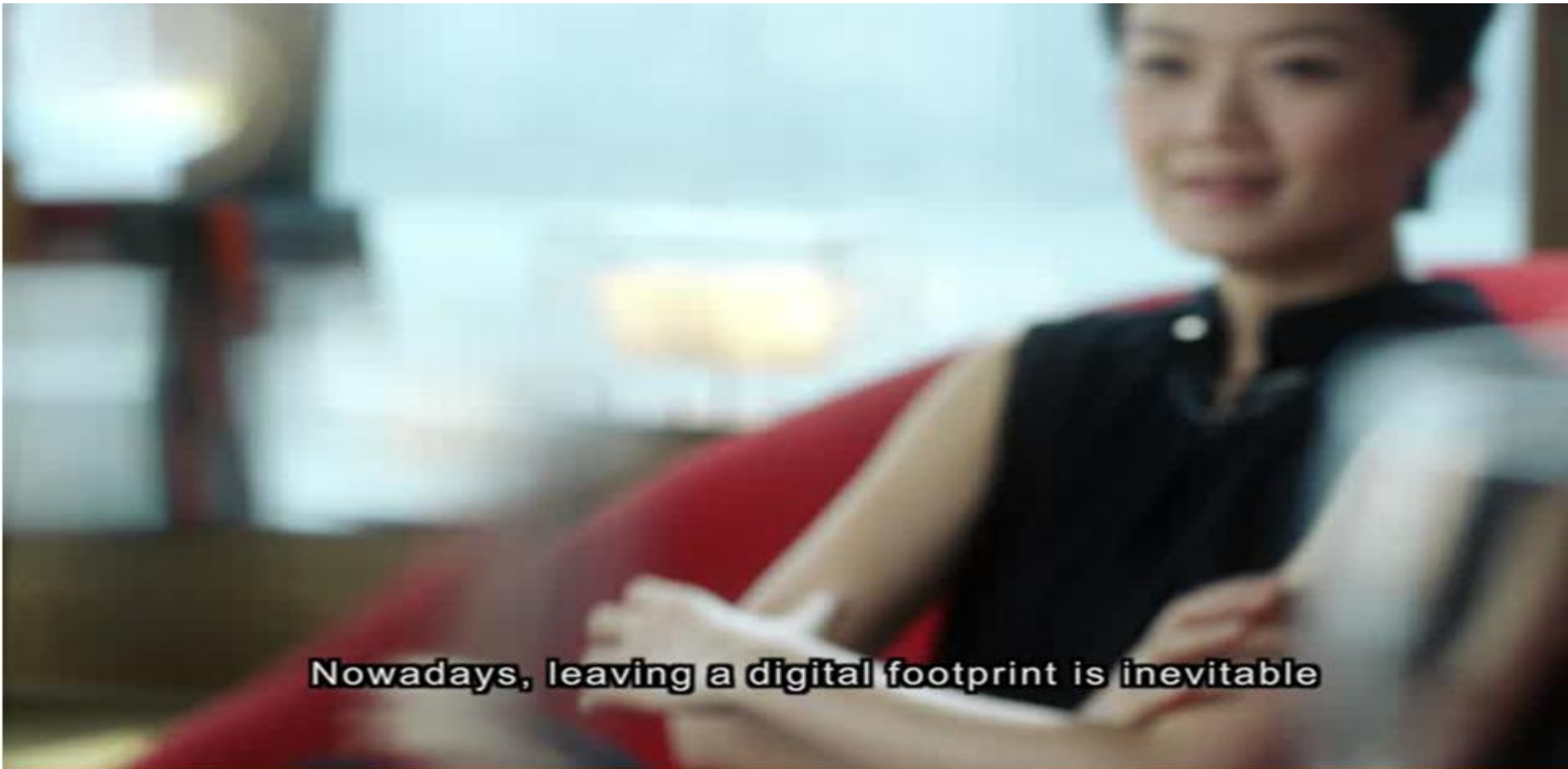
10



香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

保障、尊重個人資料
Protect, Respect Personal Data

PCPD.org.hk



Nowadays, leaving a digital footprint is inevitable



香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

保障、尊重個人資料
Protect, Respect Personal Data

PCPD.org.hk

Cloud Computing and Personal Data Privacy

- cloud computing leaflet issued 2012 and updated 2015



Cloud Computing

This information leaflet aims to advise organisations on the factors they should take into account in considering engaging cloud computing. It explains the relevance of the Personal Data (Privacy) Ordinance (the "Ordinance") to cloud computing. It highlights the importance for a data user to fully assess the benefits and risks of engaging cloud computing and understand the implications for safeguarding personal data privacy.

What is Cloud Computing?

There is no universally accepted definition of cloud computing. For the purpose of this leaflet, it is referred to as a pool of on-demand, shared and configurable computing resources that can be rapidly provided to customers with minimal management efforts or service provider interaction. The cost model is usually based on usage and rental, without any capital investment.

Cloud Computing Engagement and the Ordinance

12



Cloud Computing and Personal Data Privacy

- consistent with Article 29 Working Party's opinion on Cloud Computing, Berlin Group's Working Paper on Cloud Computing - Privacy and Data Protection Issues

ARTICLE 29 DATA PROTECTION WORKING PARTY

01037/12/EN
WP 196

International Working Group
on Data Protection
in Telecommunications

675.44.8 24 April 2012

Working Paper
on
Cloud Computing - Privacy and data protection issues
- "Sopot Memorandum" -
51st meeting, 23-24 April 2012, Sopot (Poland)

Scope

This working paper specifically examines the processing of personal data in cloud computing environments.

The working paper does not examine a situation in which all end users, the controller, the processor and all of its subcontractors are subject to the same data protection legislation and are physically

Adopted July 1st 2012

13



Cloud Computing and Personal Data Privacy

Bottom lines:

- organisations need to maintain controls
- organisations fully responsible for personal data protection
- outsourcing data processing \neq outsourcing legal responsibility



Cloud Computing and Personal Data Privacy

Potential privacy issues related to cloud's business model

- rapid transborder data flow
- loose outsourcing arrangements
- standard contract terms



Cloud Computing and Personal Data Privacy

Rapid transborder data flow. Do organisations know:

- where personal data will be stored?
- if and what legal protection is afforded in the location?
- how to explain to customer the risk of storing data overseas?

Data user needs to know storage locations, have consent, ensures comparable law, or exercises due diligence etc.

16



Cloud Computing and Personal Data Privacy

Loose outsourcing arrangements. Do organisations know:

- if there is subcontracting arrangements by the cloud provider?
- if their requirements on cloud providers are observed by their subcontractors?

Cloud service provider needs to be transparent on outsourcing practice and have sufficient controls in place

17



香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

保障、尊重個人資料
Protect, Respect Personal Data

PCPD.org.hk

Cloud Computing and Personal Data Privacy

Standard contract terms. Do organisations know:

- what to do if standard contract terms are inferior to requirements?
- how to monitor the compliance of standard/customised terms?

Ensure requirements are addressed in contract and enforced

18



香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

保障、尊重個人資料
Protect, Respect Personal Data

PCPD.org.hk

Cloud Computing and Personal Data Privacy



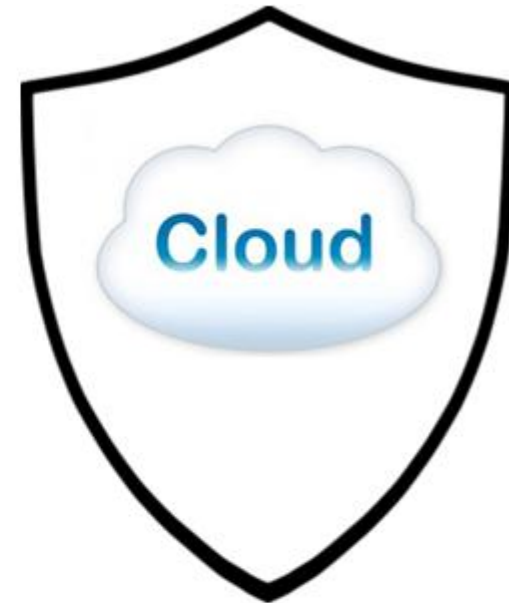
Data user



Cloud Computing and Personal Data Privacy



Data user



ISO 27018

20



香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

保障、尊重個人資料
Protect, Respect Personal Data

PCPD.org.hk

Cloud Computing and Personal Data Privacy

ISO 27018 has two parts:

- specific ISO 27002 security controls applicable to cloud
- Specific ISO 29100 privacy framework applicable to cloud



Cloud Computing and Personal Data Privacy

ISO 27018 addresses (to name a few) personal data privacy:

- transparency on storage location
- transparency on outsourcing arrangements
- commitments on data re-use, retention, disclosure, data breach notification, security, encryption, etc.

22

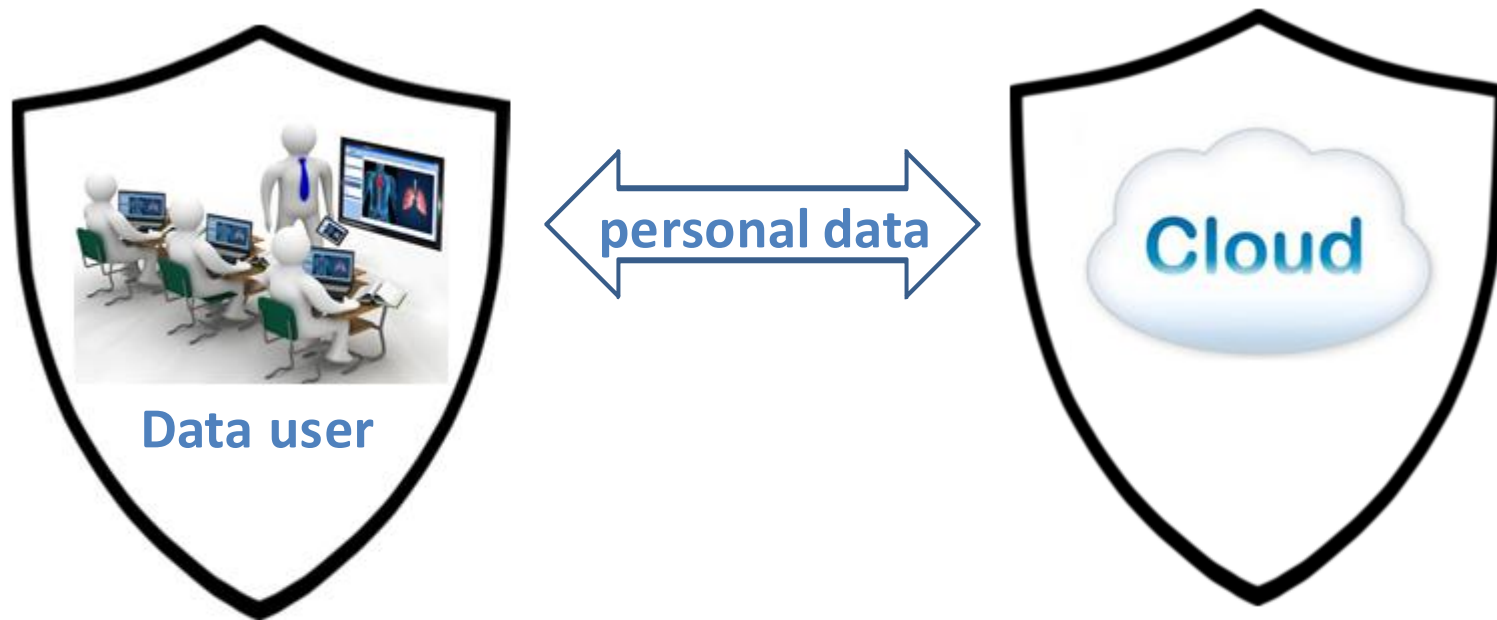


香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

保障、尊重個人資料
Protect, Respect Personal Data

PCPD.org.hk

Cloud Computing and Personal Data Privacy



Privacy Management Programme

ISO 27018

23



香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

保障、尊重個人資料
Protect, Respect Personal Data

PCPD.org.hk

Privacy Management Programme (PMP)

- encourage organisations to embrace personal data privacy protection as part of their corporate governance responsibilities and apply it as a top-down business imperative throughout the organisation

Compliance



accountability

24



香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

保障、尊重個人資料
Protect, Respect Personal Data

PCPD.org.hk

Privacy Management Programme (PMP)

- strategic framework
- good corporate governance
- trust building
- transparency
- 3 organisational commitments,
7 bottom-up controls and
2 review processes



25



PMP Best Practice Guide Framework

Three top-down management commitments

- top management buy-in of the PMP
- appointment of a Data Protection Officer or Office
- internal reporting mechanism

Privacy Management Programme – At A Glance

Part A Baseline Fundamentals

Organisational Commitment		
Buy-in from the Top	Data Protection Officer/Office	Reporting
<ul style="list-style-type: none"> Top management support is key to a successful privacy management programme and essential for privacy-respectful culture 	<ul style="list-style-type: none"> Role exists and is involved where appropriate in the organisation's decision-making process Role and responsibilities for monitoring compliance of the Personal Data (Privacy) Ordinance are clearly identified and communicated throughout the organisation Responsible for the development and implementation of the programme controls and their ongoing assessment and revision Policy and procedures are in place to incorporate personal data protection into every major function involving the use of personal data 	<ul style="list-style-type: none"> Reporting mechanisms need to be established, and they need to be reflected in the organisation's programme controls
Programme Controls		
The following programme controls are in place:		
Personal Data Inventory	Policies	Risk Assessment Tools
<ul style="list-style-type: none"> The organisation is able to identify the personal data in its custody or control The organisation is able to identify the reasons for the collection, use and disclosure of the personal data 	Covering: <ul style="list-style-type: none"> Collection of personal data Accuracy and retention of personal data Use of personal data including the requirements of consent Security of personal data Transparency of organisations' personal data policies and practices Access to and correction of personal data 	<ul style="list-style-type: none"> Training & Education Requirements Breach Handling Data Processor Management Communication

Part B Ongoing Assessment and Revision

Oversight & Review Plan
<ul style="list-style-type: none"> Develop an oversight and review plan Data Protection Officer or Data Protection Office should develop an oversight and review plan on a periodic basis that sets out how the effectiveness of the organisation's programme controls will be monitored and assessed.
Assess & Revise Programme Controls Where Necessary
<ul style="list-style-type: none"> Update personal data inventory Revise policies Treat risk assessment tools as evergreen Update training and education Adapt breach and incident response protocols Fine-tune data processor management Improve communication

26



香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

保障、尊重個人資料
Protect, Respect Personal Data

PCPD.org.hk

PMP Best Practice Guide Framework

Seven bottom-up programme controls

- a personal data inventory
- internal policies (DPPs)
- risk assessment
- up-to-date training and education
- procedure of notification (data breach)
- obligations for data processor
- communication with employees and customers

Two on-going monitoring processes

- documented process
- regular execution

27



Paradigm Shift

Compliance approach:

- passive
- reactive
- remedial
- problem-based
- handled by legal/compliance
- minimum legal requirement
- bottom-up

Accountability approach:

- active
- proactive
- preventative
- based on customer expectation
- directed by top-management
- reputation building
- top-down

*From Compliance
to Accountability*

28



Effect of Paradigm Shift

Liability



Asset



Effect of Paradigm Shift



Building Trust in the Cloud Era – Protect, Respect Personal Data

