THE EU GENERAL DATA PROTECTION REGULATION (THE GDPR) IN APAC: WHY COMPLY ?

FROM REACTIVE TO PROACTIVE
Hong Kong – 20 November 2017

Scott Pilkington, Partner
T: +65 6411 5357
E: scott.pilkington@hfw.com

Only 186 working days until the GDPR comes into force in May 2018

1.WHAT IS IT?

2. WHAT'S NEW, AND WHAT DOES IT DO?

3. WHY SHOULD YOU CARE?

4. WHAT MUST YOU DO?


HFW
1. WHAT IS THE “GDPR”?

GDPR
IN A 'NUTSHELL'

Regulation (EU) 2016/679 "*on the protection of natural persons with regard to the processing of personal data and on the free movement of such data*"

Comes into effect on 25 May 2018

Data Subject's rights

Natural persons – *whatever their nationality or place of residence*

Duty to notify any breach

Extra territorial effect

Controllers and Processors

Data protection impact assessment

1.Are any of your vessels flagged within the EEA?

2.Is your website directed towards customers based in the EEA, for example by using an EEA currency, or a particular language?

3.Can your services be bought from within the EEA?

4.Do you have a registered establishment or an office in the EEA?

5. Is your business currently registered with an EEA data protection authority?

6. Do you use servers located in the EEA?

7. Do you monitor the behaviour of any individuals within the EEA (irrespective of their nationality or habitual residence)? For example, if your website uses tracking cookies, then you are “monitoring individuals” for the purposes of the GDPR.

If the answer to any of these questions is ‘yes’ then it is likely that the GDPR applies to you.


HFW
2. WHAT'S NEW, AND
WHAT DOES IT DO?

THE GDPR IS THE BIGGEST SHAKEUP OF DATA PROTECTION LAW IN 20 YEARS

This landmark piece of legislation will impact every entity that holds or uses European personal data.

1. **Heavy financial penalties for breaches**
2. **Overall increased focus on operational adequacy and accountability**
3. **New and enhanced citizens' rights**
4. **Mandatory breach disclosure**
5. **Sets up possible US-style class action for privacy breaches**

…and even the definition of 'personal data' has changed…

THIS IS A SIGNIFICANT STEP UP FROM THE EXISTING PRIVACY REGULATION

Understand the data they hold and how they use it.	A new "Transparency Framework"
Clear compliance steps to be taken, evidence of this is essential.	A new "Compliance Journey"
Reputation risk: non compliance fines and the potential for litigation and class action.	A new "Punishment Regime"

GDPR

CONTROLLERS, PROCESSORS AND PROCESSING

Controller:	Processor:	Processing:
"*the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data"* the Controller shall implement *appropriate technical and organisational measures* to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary. (art. 24.1)	"*a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*"	"*any operation …which is performed on personal data…,whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alternation, retrieval, consultation, use disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*"

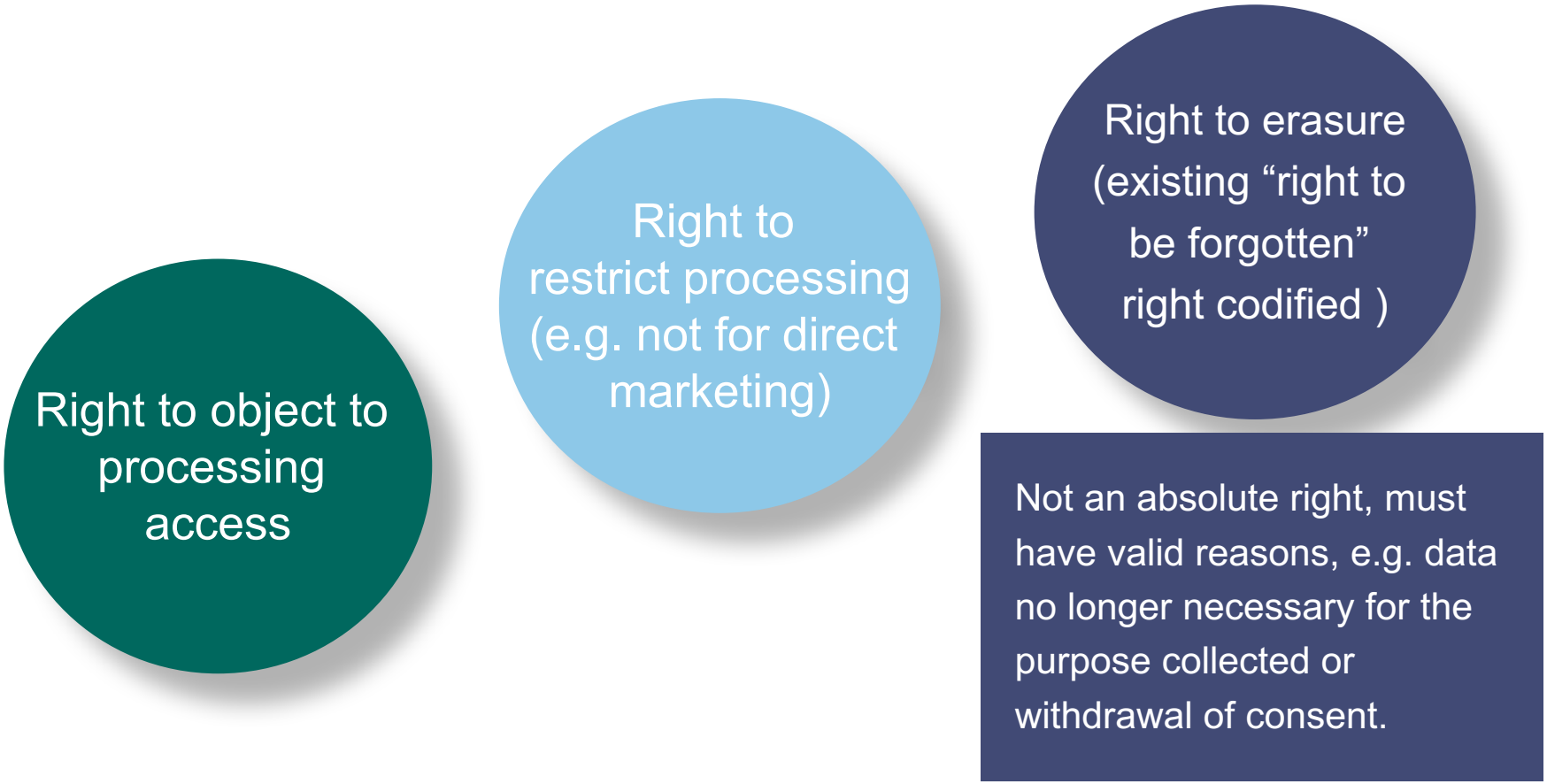
Personal Data (Article 4)

- **Any information** relating to **an identified or identifiable natural person**; an identifiable natural person ... can be identified, directly or indirectly... by reference to an **identifier** such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"
- Only relates to **living** individuals (as with current law
- Includes e.g. business emails and browsing history

Special Categories of Personal Data (Article 9)

- Very similar to current law on "sensitive personal data" but updated
- Includes personal data **revealing** racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, health data, sex life or sexual orientation
- Data on criminal convictions and offences treated under different laws

- Additional and enhanced individuals' rights including:



Continued…

Right to forbid profiling which results in significant decisions

Right to data portability

- where processing electronic and grounds for processing are consent or contract

Enhanced subject access rights (entitled to more information)

40 day response window

GDPR – KEY LEGAL OBLIGATIONS

- New focus on accountability – must keep records of processing
- Enhanced transparency requirements:
  - Privacy notices will need updating
  - Individuals must be notified when their data is received from third parties.
- Additional data breach reporting requirements
- Contracts with processors
  - *New elements must be included*


HFW
3. WHY SHOULD YOU CARE?

- **Potential fines of up to 4% of global turnover or €20 million (whichever is the greater)**
- Risk of legal challenge from individuals / class actions (enforcement/compensation)
- Reputational damage
- Affects cross border business
- Customer pressure

WHAT IS A 'BREACH'?

'***Personal data breach***' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Name, date of birth, family details (including children), medical records and other possibly sensitive information. Duty to protect, whether transmitting, *storing* or processing

Duty to notify the supervisory authority in the event of breach within 72 hours or "without delay"

Have you been "hacked"?


HFW
4. WHAT MUST YOU DO?

WHEN CAN YOU PROCESS PERSONAL DATA?

Grounds for processing similar to current law – at least one of :

1. Consent of the data subject (for the particular purpose)
2. Necessary for the performance of a contract **with data subject**
3. Necessary for compliance with a legal obligation
4. Necessary to protect “vital interests” of data subject/third party
5. Necessary for performance of a task in the public interest
6. Necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party (balancing exercise of rights) – BUT, except where overridden by the interests or fundamental rights and freedoms of the data subject

- "Consent" definition made stricter

> **...freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she by a statement or by a clear affirmative action signifies agreement ...**

- No implied consent

- Additional clarifications / obligations under GDPR:

Controller must be able to **demonstrate** that data subject has consented	Must have right to withdraw consent at any time
Where consent part of written declaration also concerning other matters, consent element must be clear and user friendly or not binding	Consent may not be "freely given" if performance of contract conditional on consent

- Consent no longer an "easy" legal ground for processing

HFW

GDPR

WHAT MUST YOU DO TO COMPLY?

1. Data audit:-

- **What personal data do you hold and what for (especially with regard to "sensitive" data)**
- **Document findings and decisions**

2. Draft or amend policies and procedures

- To deal with any breach, including reporting it without delay/within 72 hours
- When and how to conduct privacy impact assessment
- Record-keeping

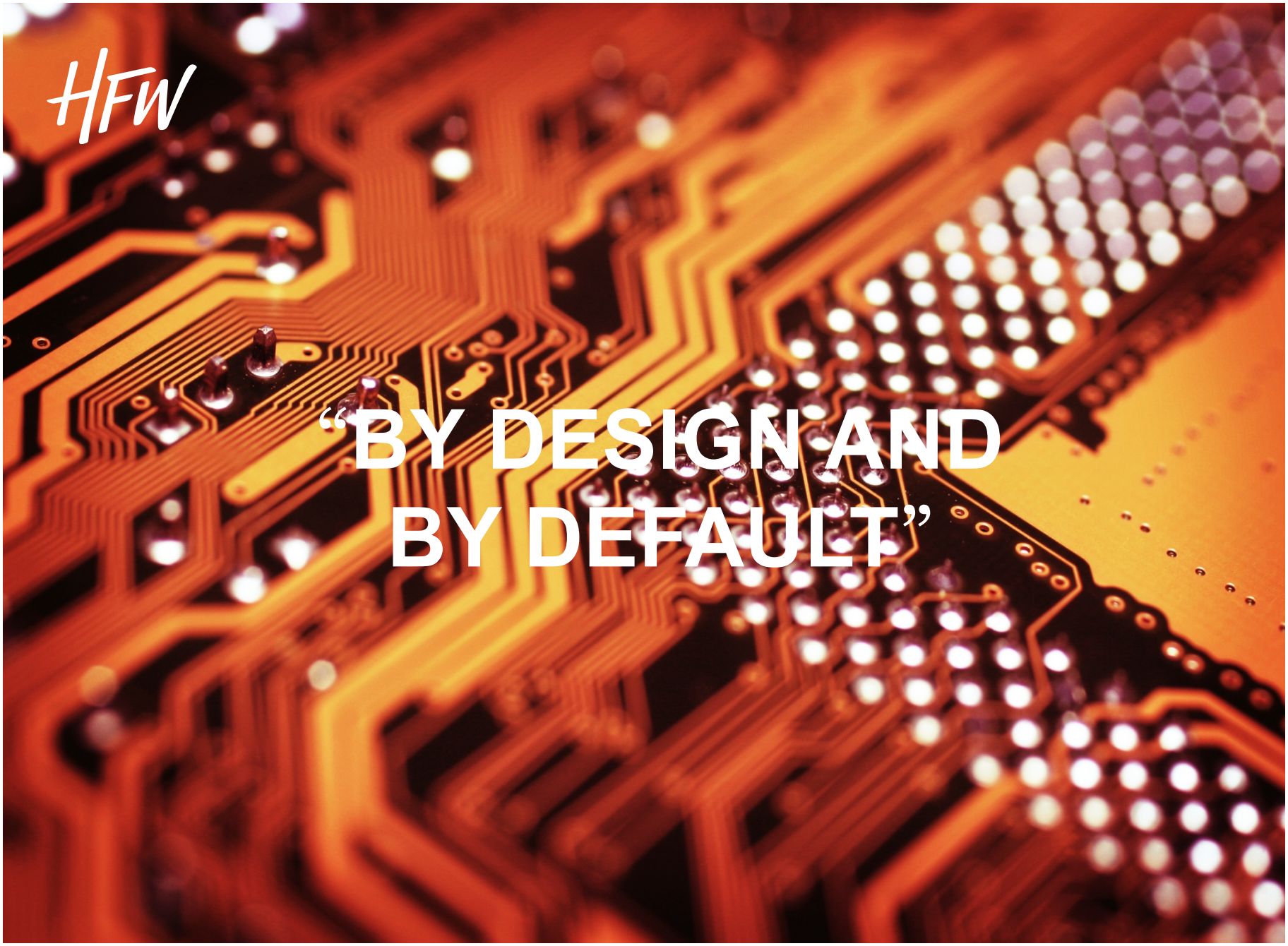
3. Inform individuals about processing

- Check and update existing draft privacy notification forms or draft new ones

4. Amend or put contracts in place with data processors – indemnities…

5. Appoint a data protection officer?

- Do you need to? May choose to do so voluntarily, given the increased risks involved.


HFW
“BY DESIGN AND
BY DEFAULT”

"Data Minimization"

"*The Controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to:*

the amount of personal data collected	**the period of their storage; and**
the extent of their processing	**their accessibility**

In particular such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons."

THE GDPR 'LEGISLATIVE COMPLIANCE JOURNEY

The GDPR defines a 'compliance approach' through the full lifecycle, from data analysis to dealing with failures.

1. Analyse	What data will you process, how and why? [A.22]
2. Risk assess	What are the risks and what harms can be caused? [A.33]
3. Consult	Which stakeholders do you need to consult with? [A.34]
4. Design	How will you build in data protection from the beginning of processing? [A.23]
5. Document	How will you prove compliance? [A.7,8,22,28]
6. Engage	What information should you give to the public and what consents do you need? [A.7,8,12,14]
7. Challenge	How will you handle incidents, problems and complaints? [A.31,32]
8. Supervision	How will you handle the use of legal rights and supervisory powers? [A.15,16,17,18,19,52,53,73]
9. Sanctions and litigation	How will you cope with the most serious regulatory sanction and civil litigation? [A.75,77,79]

HFW

GDPR: WHY SHOULD I CARE?

KEY ELEMENTS THAT THE REGULATORS WILL EXPECT

- an organisational view on what Privacy means to you
- a clear understanding of what data is held, why you have it, where it is and who has access to it
- understand and manage the risks introduced to the data by third parties
- Privacy model is designed with agility in mind given the ever changing Privacy landscape
- understand how Privacy and Data Protection fit into your overall business strategy
- know how well you are protecting the data, and where you are not
- using the data for the purpose that you have committed to and nothing more
- help to empower individuals, so they can control the use of their data better

1.WHAT IS IT?

2. WHAT'S NEW, AND WHAT DOES IT DO?

3. WHY SHOULD YOU CARE?

4. WHAT MUST YOU DO?

Thank you

Scott Pilkington, Partner
T: +65 6411 5357
E: scott.pilkington@hfw.com

Only 186 working days until the GDPR comes into force in May 2018