## Symposium on Big Data and Data Governance

11/F, Cheng Yu Tong Tower, the University of Hong Kong
14 October 2016

# EU's New General Data Protection Regulation – 10 Major Changes and Possible Impacts

**Stephen Kai-yi Wong**
**Privacy Commissioner for Personal Data, Hong Kong**

# General Data Protection Regulation (GDPR)

- Passed in May 2016
- Directly enforceable in 28 EU member states and other EEA countries (e.g. Norway) in May 2018
- Will repeal EU Data Protection Directive (1995) and national data protection laws

# Major Changes Brought by GDPR

1. Wider definition of personal data and sensitive data
2. Pseudonymisation
3. More stringent requirement for consent
4. Enhanced right for data subjects
5. Direct obligation for data processors
6. Regulation on profiling
7. Increased accountability of data users/controllers
8. Mandatory data breach notification
9. Extra-territorial application
10. Heavier sanction for breach of regulation

# 1. Wider definition of personal data and sensitive data

| New Requirements | Possible Impacts |
| --- | --- |
| • "personal data" explicitly include location data and online identifier<br>• sensitive personal data extended to include genetic data, biometric data and sexual orientation | • reflect technological changes and new ways of collecting personal data<br>• data users should critically assess if information is "personal data"<br>• require higher protection to biometric data which is more widely used today |

# 2. Pseudonymisation

| New Requirements | Possible Impacts |
| --- | --- |
| • introduce a new concept of "pseudonymisation"<br>• pseudonymised data may still fall within GDPR, depending on difficulty of attributing the pseudonym to an individual | • recognise that "pseudonymisation":<br>(i) allows processing of personal data beyond original collection purposes<br>(ii) demonstrates "data protection by design"<br>(iii) helps meet data security requirements<br>• reduce privacy risk and unleash value of data |

# 3. More stringent requirement for consent

| New Requirements | Possible Impacts |
| --- | --- |
| • "consent"- agreement by a statement or a clear affirmative action<br>• must be freely given, specific, informed and unambiguous<br>• data user may not make a service conditional upon consent, unless processing is necessary for the service<br>• restrict the ability of children to give consent | • create additional hurdles for consent<br>• more efforts by data users to obtain valid consent and demonstrate compliance<br>• big data - difficult to obtain specific and informed consent |

# 4. Enhanced right for data subjects

| New Requirements | Possible Impacts |
| --- | --- |
| • "right to erasure" if:<br>(i) data is no longer needed;<br>(ii) data subjects object to processing; or<br>(iii) processing was unlawful<br>• "right to data portability": data user should provide personal data in machine-readable format and transfer that data to another data user upon request | • protect data subjects' privacy by preventing unnecessary retention of data<br>• respond to big data trend - increase user choice of online services<br>• data users need effective user interfaces to comply with data subjects' requests |

# 5. Direct obligation for data processors

| New Requirements | Possible Impacts |
| --- | --- |
| • data processors accountable for processing, and should:<br>(i) ensure security of personal data;<br>(ii) cooperate with data protection authority;<br>(iii) not act outside or contrary to lawful instructions of data users | • reduce compliance risk of data users<br>• reduce privacy risk of data subjects |

# 6. Regulation on profiling

| New Requirements | Possible Impacts |
| --- | --- |
| • "profiling" involves:<br>(i) automated processing of personal data; and<br>(ii) using that data to evaluate personal aspects<br>• require disclosure of profiling, logic and envisaged consequences<br>• right to avoid being subject to a decision based solely on profiling and with legal effects | • create hurdles for big data and artificial intelligence<br>• increase transparency of technologies and accountability of data users<br>• protect legitimate interest of data subjects |

# 7. Increased accountability of data users

| New Requirements | Possible Impacts |
| --- | --- |
| • accountability principle - data users should demonstrate compliance to processing principles by:<br>(i) implementing "data protection by design"<br>(ii) performing privacy impact assessment<br>(iii) appointing data protection officer | • increase workload for data governance<br>• demonstrate data user's accountability and increase reputation<br>• ensure higher protection to personal data and reduce risk of data breach |

# 8. Mandatory data breach notification

| New Requirements | Possible Impacts |
| --- | --- |
| • notify data protection authority if likely to result in a risk to rights and freedoms of individuals<br>• notify the affected individuals if likely to result in a high risk | • raise data users' awareness to data security<br>• affected data subjects can look out for risk of identity theft and other misuse of personal data<br>• data users should ensure staff understand what data breach is "notifiable" |

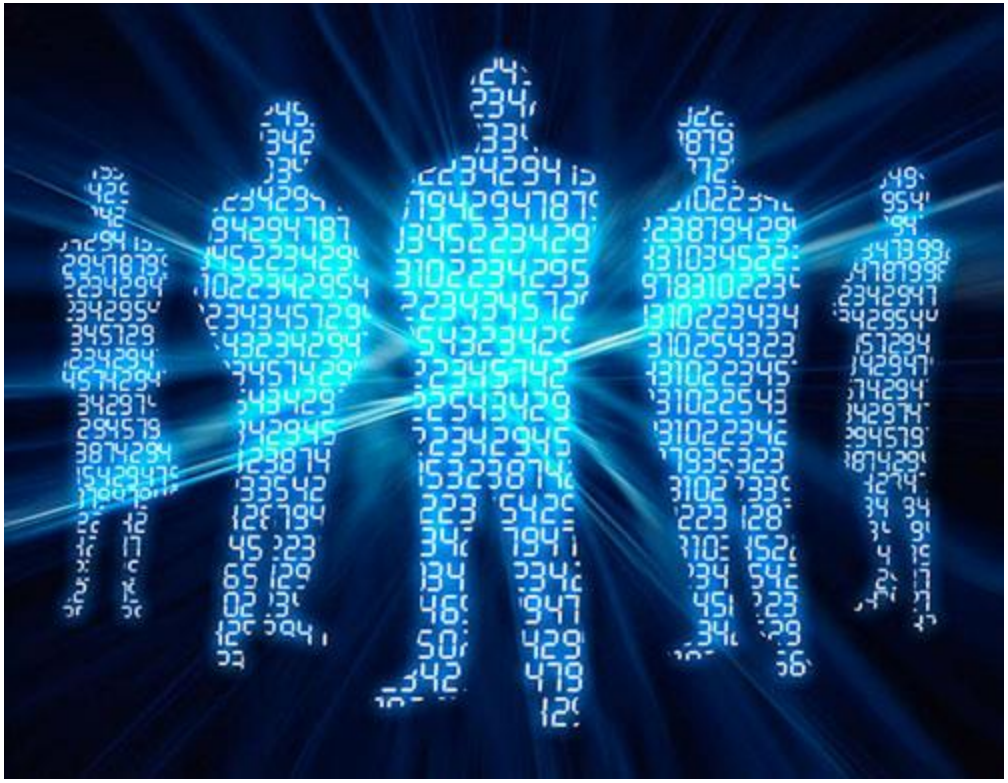
# 9. Extra-territorial application

| New Requirements | Possible Impacts |
| --- | --- |
| • extend application to non-EU data users, so long as processing activities relate to (i) offering of goods and services to data subjects in EU; or (ii) monitoring of behaviour of data subjects in EU | • data users outside the EU need to assess compliance<br>• particular implication to digital business model, e.g. e-commerce |

# 10. Heavier sanction for breach of regulation

| New Requirements | Possible Impacts |
| --- | --- |
| • data protection authorities can impose fines on data users and data processors for contravention<br>• two-tier fines:<br>(i) higher: 4% worldwide annual turnover or €20M<br>(ii) lower: 2% worldwide annual turnover or €10M | • encourage compliance by data users<br>• data users outside EU need to assess compliance |

# Is GDPR sufficient to protect privacy in the digital age?




danke
謝謝
ngiyabonga
teşekkür ederim
спасибо
dank je
thank you
gracias
tapadh leat
mochchakkeram
bedankt
hvala
mauruuru
dziękuję
go raibh maith agat
obrigado
sagolun
sukriya
kop khun krap
arigatō
takk
dakujem
grazie
мерси
terima kasih
감사합니다
merci
ευχαριστώ