# PRIVACY AND DATA PROTECTION

Andrew Ho

# DISCLAIMER

The views and comments I will present are of **my own** and do not reflect the views or comments of my employer Sanofi or any other company.

# WHAT IS PRIVACY?

**Privacy** is the ability of an individual or group to seclude themselves, or control any information about themselves, and thereby express themselves selectively.

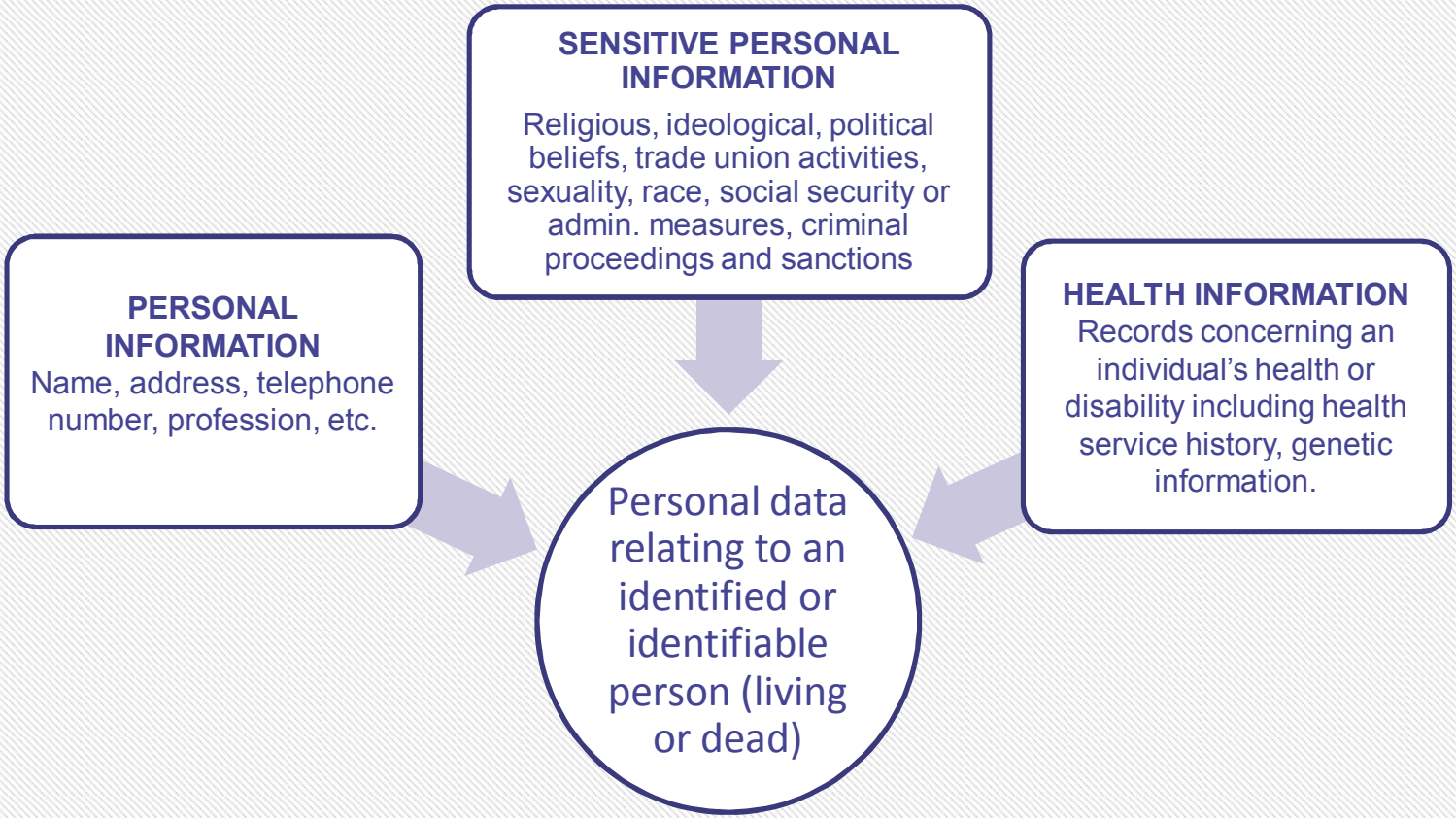
# WHAT IS DATA PROTECTION?

**Data protection** is commonly defined as the law designed to protect your personal information, which is collected, processed and stored by “automated” means or intended to be part of a filing system.

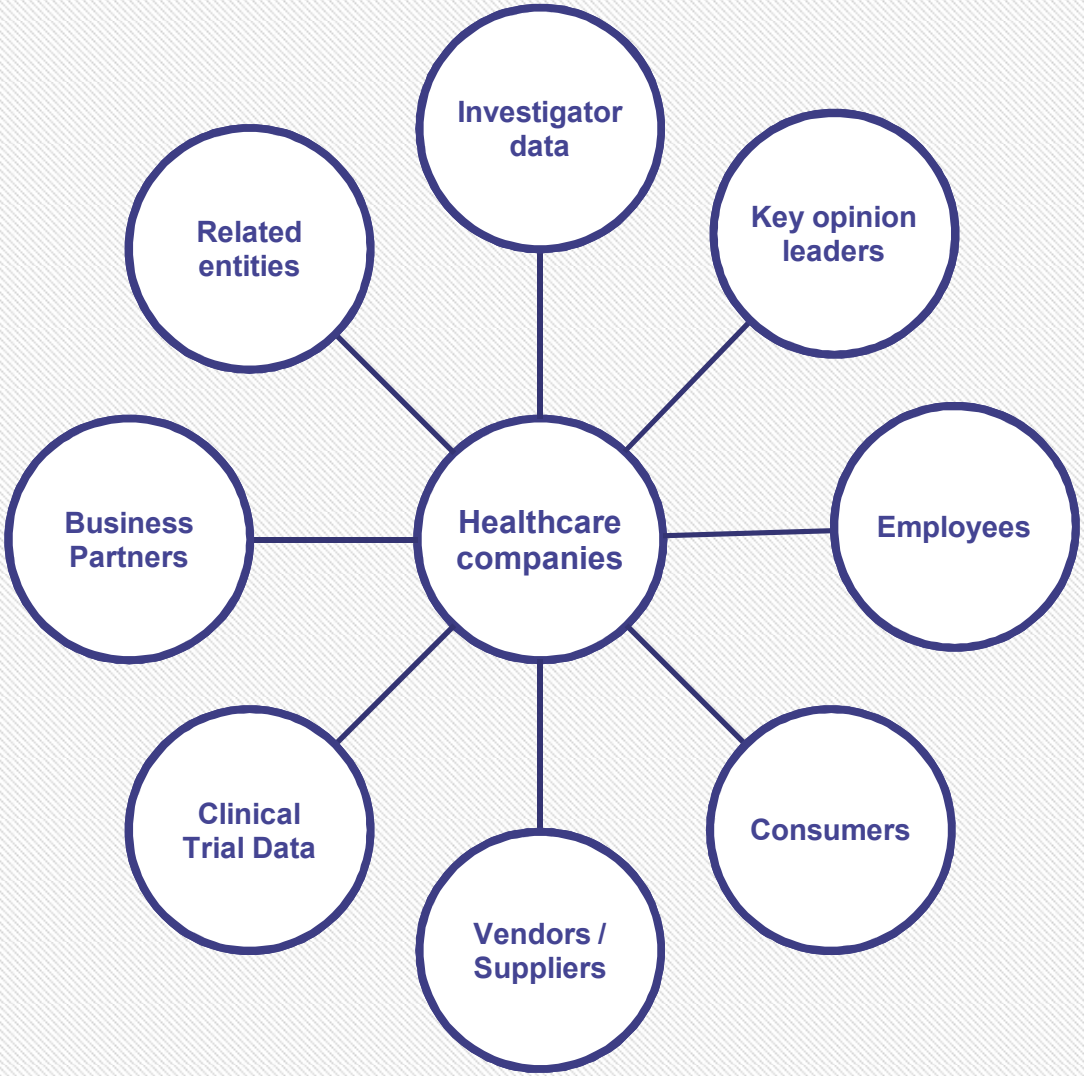
**Data Protection** ensures that data collected by a company was collected transparently, used for the correct agreed purpose and protected against any potential breach or misuse.

**Source:** privacyinternational.org

# WHAT KIND OF INFORMATION IS IN SCOPE?



# PERSONAL DATA CAN COME FROM ALL AREAS

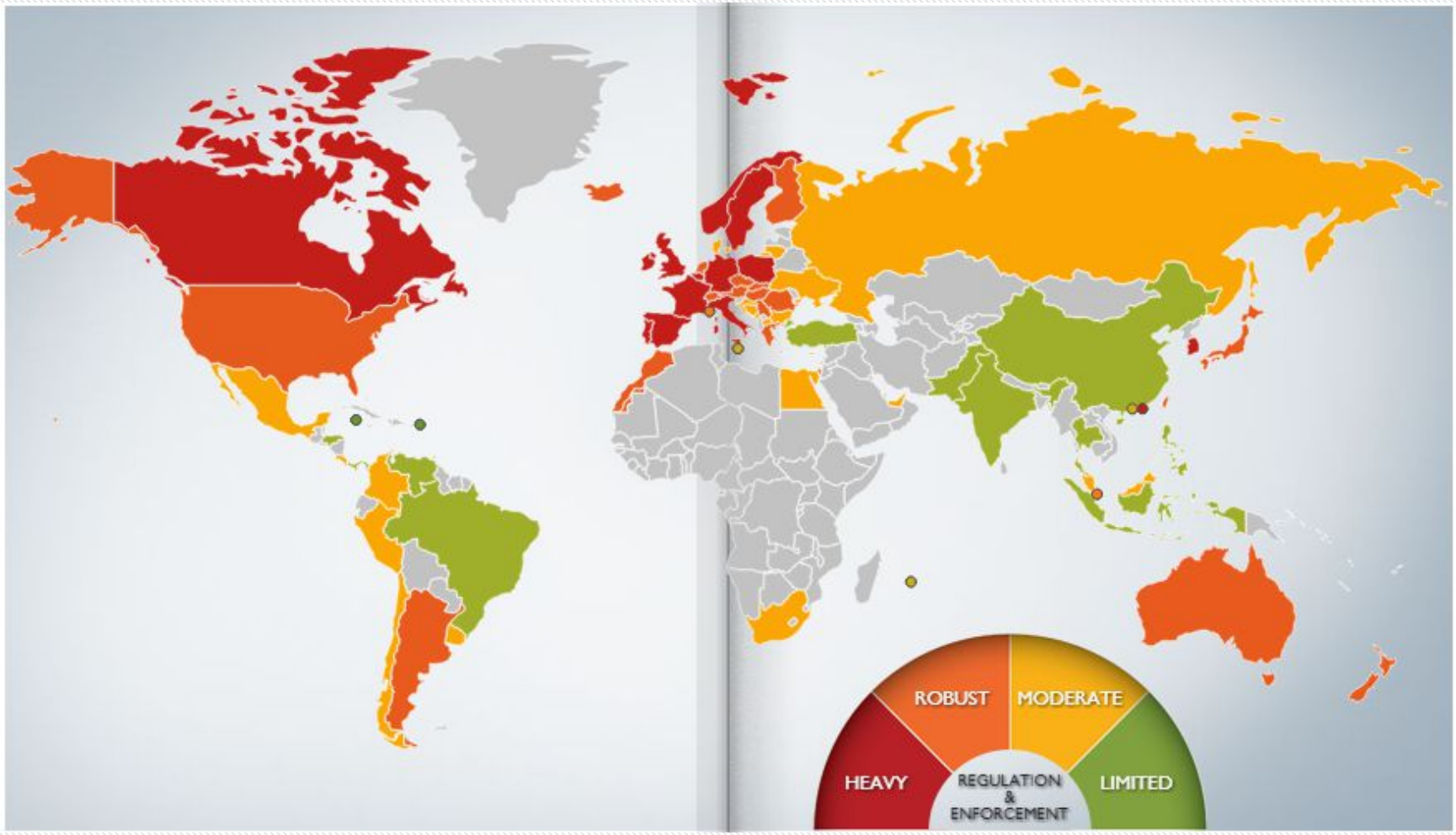


# WHY IS PERSONAL DATA PROTECTION SO IMPORTANT IN HEALTHCARE?

- **WE'RE AN INDUSTRY FOUNDED ON TRUST AND INTEGRITY.**
- **ENABLES CLINICAL TRIALS AND MARKET RESEARCH**. Individuals are more likely to participate research if they believe that their privacy is being protected.
- **SENSITIVITY OF HEALTH INFORMATION.** Degree of harm and reputational damage from health information being leaked is extreme.
- **NECESSARY BUSINESS FUNCTIONS** E.g. Call notes, Adverse event reporting, transparency.

# CONSIDERATIONS IN HEALTHCARE

- **Patient data in Clinical Trials, e.g. use of analytics**
- **Employee HR data, e.g. sickness, involvement in compliance investigations**
- **Internal / external Reporting Lines**
- **Case notes regarding compliance investigations, whether proven or not**
- **HCP data in Field Automation Systems / Reps' "little black books"…**
- **Disclosures / Transparency Reporting for HCP Transfers of Value**
- **"Bad documents"**




**Source:**
http://dlapiperdataprotection.com/#handbook/world-map-section/c1_AU

# WHAT COULD GO WRONG?

## Telstra fined, warned after new privacy breach

THE AUSTRALIAN | MARCH 11, 2014 10:20AM

SAVE

Mitchell Bingemann
Reporter
Sydney

Follow @Mitch_Hell

**TELSTRA has been fined $10,200 and warned over privacy breaches after an information leak exposed almost 16,000 of its customers' private data online.**

In a joint investigation by the federal Privacy Commissioner and the communications watchdog, Telstra was found to have breached the Privacy Act by exposing online the data of some 15,775 Telstra customers, including 1257 silent line customers, when the telco giant failed to adequately protect the information.

The breach, discovered in May last year, meant that private customer data including names, telephone numbers and home and business addresses could be found through simple Google searches.

# 12 tips to implementing a robust and compliant Personal Data Protection Program

# 1. Have a detailed Data Protection Policy

Having a robust Data Protection Policy will allow you and your company to know the limitations of how personal data can be used and should be protected.

# 2. Know when Privacy and Data Protection rules KICKS IN

Basically anytime when the company collects  or use an individual's personal data (including images and recordings).

Ensure that all activities involving data collection is reviewed prior to the activity commencing.


# 3. Be TRANSPARENT!

Let our stakeholders know why we are collecting this information and how we will use their information!

# 4. CONSENT is KING

Companies can use an individual's personal data in many ways as long as informed consent is given.

# 5. Know the LIMITS of your CONSENT

No consent. No usage. So know upfront what you need consent for because re-consenting is very difficult.

# 6. Be sure to know where your information is going

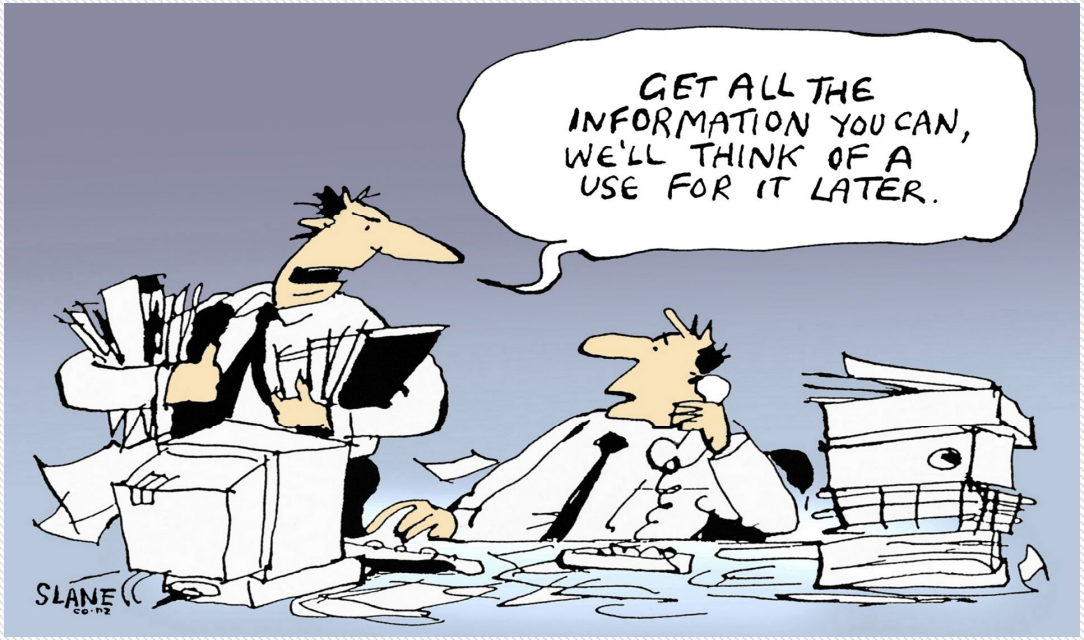
Internally your information may be protected but how about to third-parties that may come in contact with your data?

# 7. Look into whether De-identified information can be used instead?

Information which is sufficiently de-identified may not need the same information protection requirements.

# 8. Be responsive to queries and complaints

No in-house Privacy and Data Protection Program is perfect. However it is how we respond to complaints that could make the difference between a fine or a warning.




# 9. Be careful what you collect

Data must be for a business purpose and the individual must be aware that you are collecting this. You should be able to justify everything that you collect.

# 10. Have a designated Data Protection Officer

A Data Protection Officer can provide the business with the right guidance on how to collect and handle personal data and respond to queries or complaints in a quick and effective manner.

# 11. PROTECT, PROTECT, PROTECT!

Ensure that any system/database used to keep personal information is safely secure and protected from unwanted individuals. This includes anybody who has no purpose accessing this information.

# 12. Conduct a yearly audit of all sources of personal infomation

Annual audits ensure that any personal information being kept still has a use, is securely protected and still used within the confines of the original consent.

# 12 PRIVACY AND DATA PROTECTION TIPS

1. Have a detailed Privacy Policy.
2. Know when Privacy KICKS IN
3. Be Transparent
4. Consent is King
5. Know the Limits of your Consent
6. Be sure to know where your information is going to
7. Can de-identified information be used instead?
8. Be responsive to queries and complaints
9. Be careful what you collect
10. Ensure there is a Privacy Officer in place.

# IF UNSURE…

If you are unsure about how compliant your organisation is with Privacy and Data Protection then there are several free tools which allow you to assess the level of maturity within your organisation.

# DATA PRIVACY SCOREBOX

## Your privacy compliance checklist

Based on your results, the following key action points have been identified. Please note that this non-exhaustive list has been generated automatically and that it is not a substitute for legal advice. Should you require any further assistance, please do not hesitate to contact us at dataprivacy@dlapiper.com or get in touch with one of the key contacts mentioned on the first page of this report.

### Transparency

- [ ] Analyse your processing operations and verify whether your privacy notice(s) are complete and detailed enough.
- [ ] Verify regularly whether your privacy notice(s) require(s) updating.

### Categories of personal data

- [ ] Verify whether any legal restrictions exist with respect to the processing of certain categories of personal data.

# QUESTIONS?

Any questions you can also contact me via my email:
nyc2k3@gmail.com