Building trust in digital government

Digital transformation training programme
Module #4

UNDP

ASIA AND THE PACIFIC

Regional Innovation Centre

A few zoom house rules before we start

- Make sure your name is displayed
- Keep your video on unless you have connectivity issues
- Mute if you're not speaking
- Don’t hesitate to ask questions by raising your hand or using the chat

Where we are

1. Introduction to digital government

2. Human-centred design for digital services

3. Agile and open ways of working

4. Building trust in digital government

5. Data: uses, opportunities and risks

6. Making the right tech choices

7. Hacking common barriers to digital government

Learning objectives

- ✓ Understand the common barriers and enablers to trust in digital government
- ✓ Differentiate types of data and their protection requirements
- ✓ Understand the importance of privacy and global legal frameworks around it
- ✓ Apply basic cyber hygiene principles
- ✓ Explain the concept of security by design

1. Barriers and enablers to trust

2. Categorisation of data

3. Data protection

    a. Data privacy

    b. Cyber security

1. **Barriers and enablers to trust**
2. Categorisation of data
3. Data protection
    a. Data privacy
    b. Cyber security

5-min activity

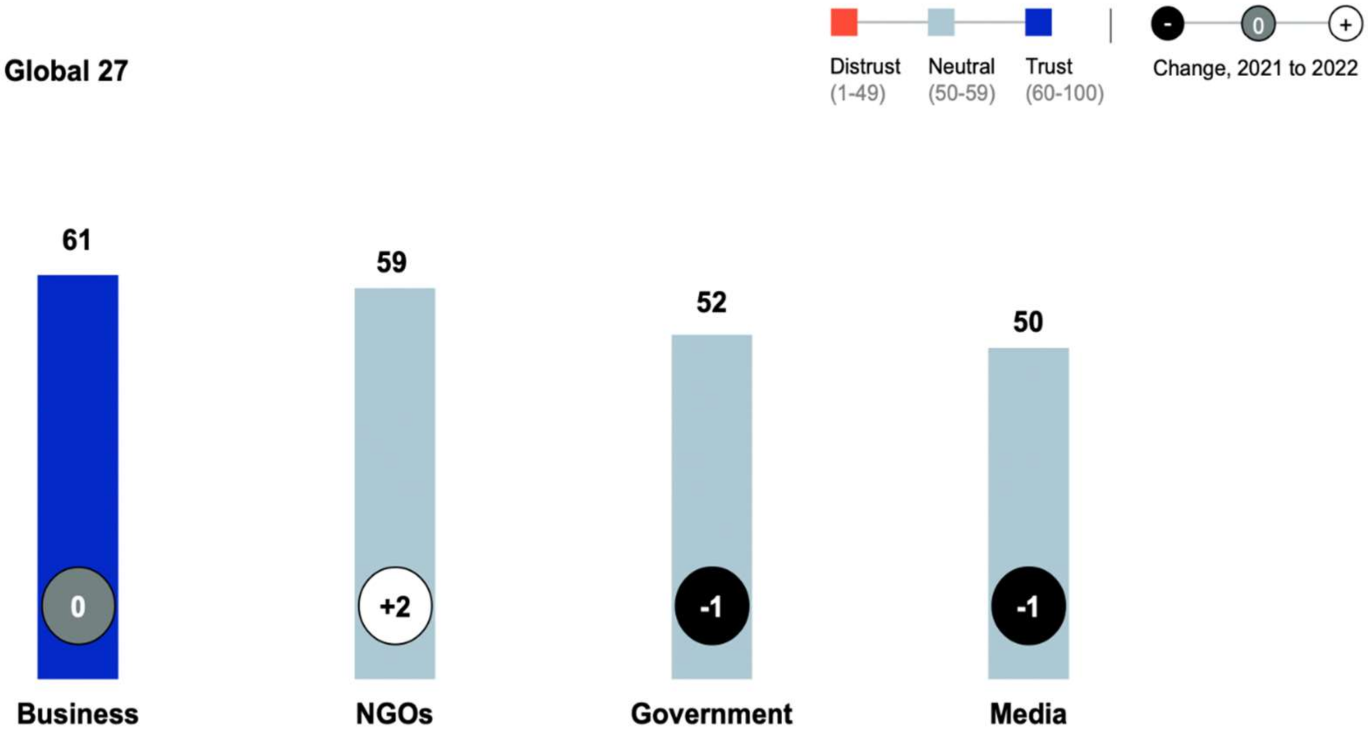
Why is trust in digital government important?

Given a situation of **uncertainty** regarding the conduct of a government, **trust** is the belief that this conduct will conform with a certain set of **positive expectations**

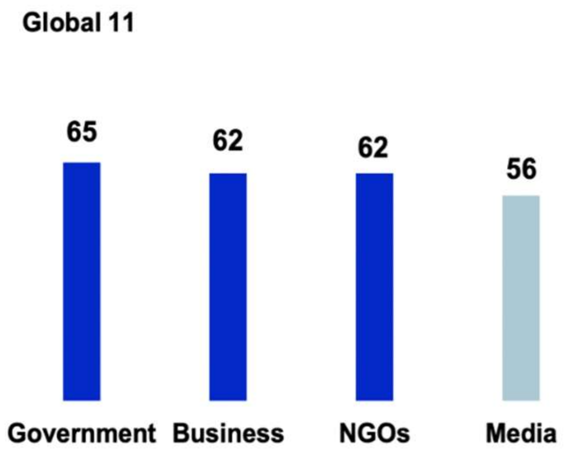
UNDP Policy brief - Trust in public institutions

TRUST DECLINES FOR GOVERNMENT AND MEDIA; BUSINESS STILL ONLY TRUSTED INSTITUTION

Percent trust

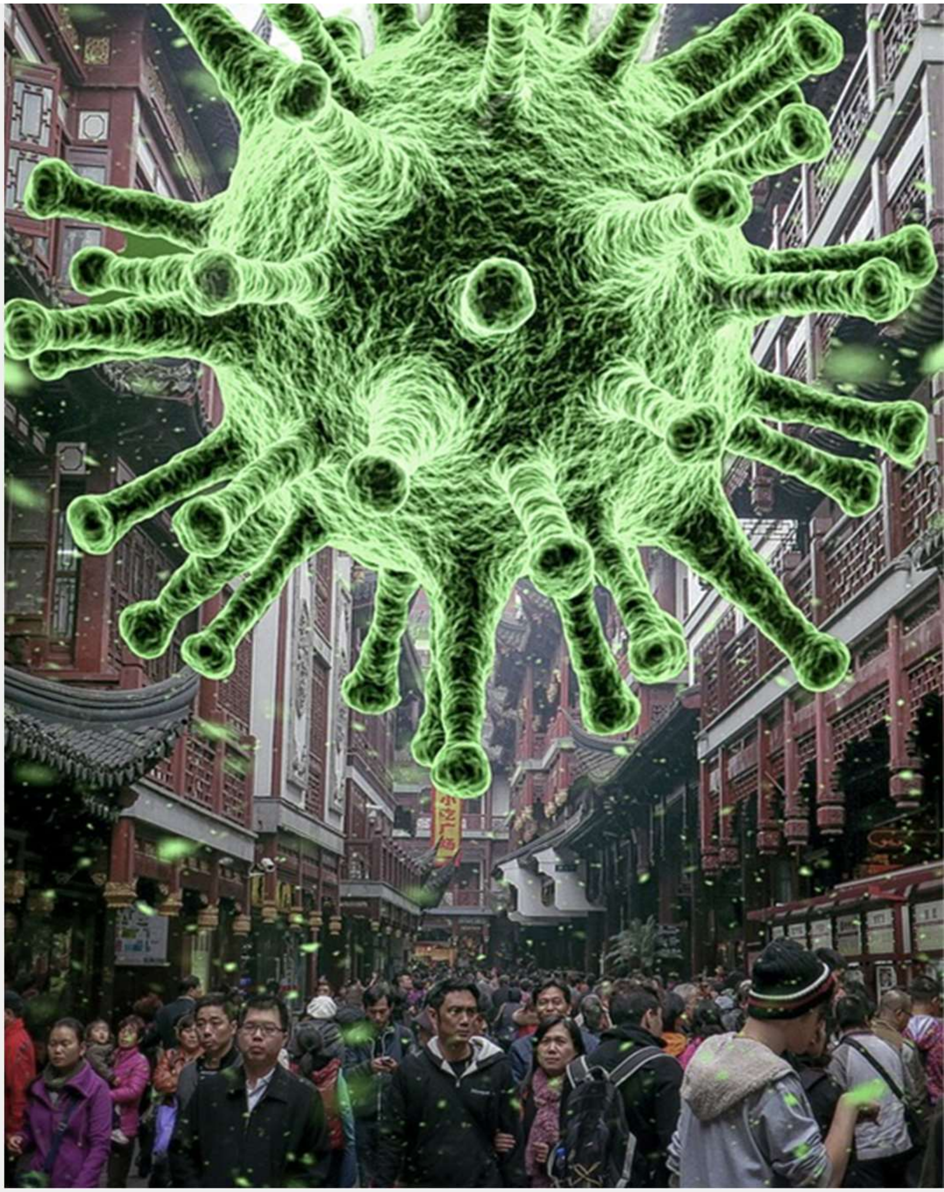


IN MAY 2020, GOVERNMENT MOST TRUSTED



Trust in digital systems was put to the test during the pandemic.

Taking rushed decisions on the use of digital may work in the short term but negatively impact **human rights** in the long term.



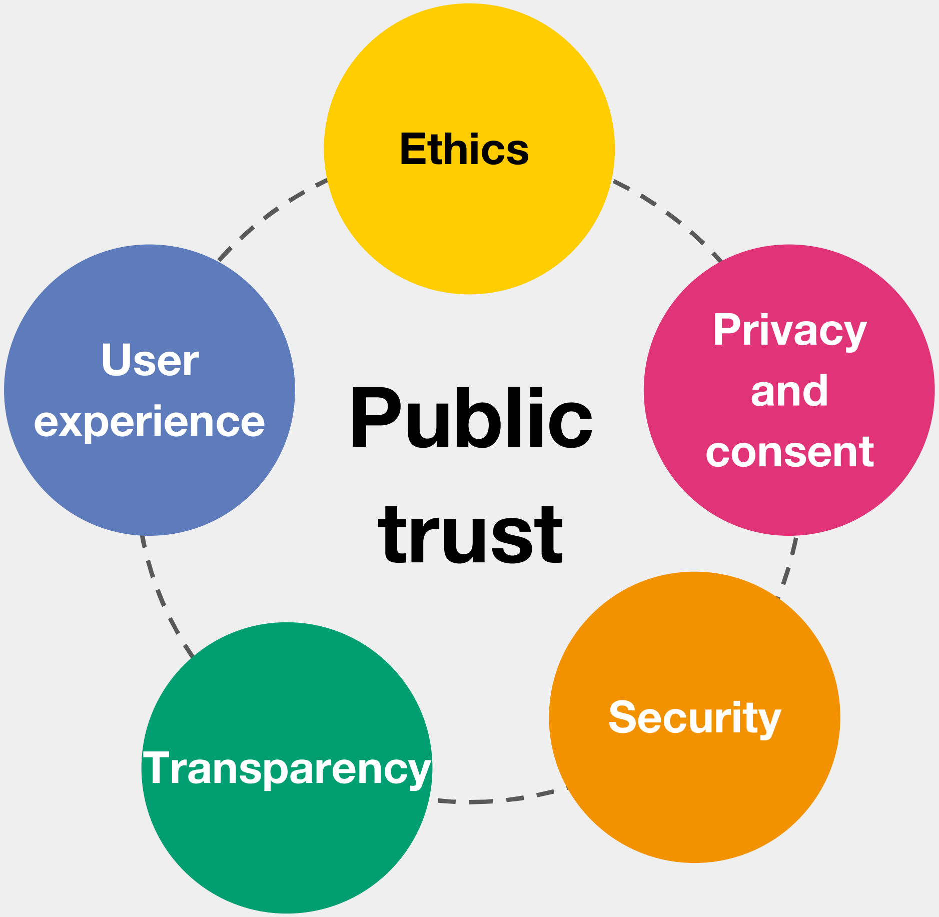
Barriers to trust in digital government

- Lack of digital awareness
- Bad experience of government, and especially of online services
- Fear of data breaches and cyber attacks
- Poor perception of government, and fear of governmental data abuse

Digital government can help build trust through:

- Increased transparency and accountability
- Responsive, effective and inclusive service delivery
- Enhanced citizen participation

Trustworthy use of data and technology



Ethics

Privacy and consent

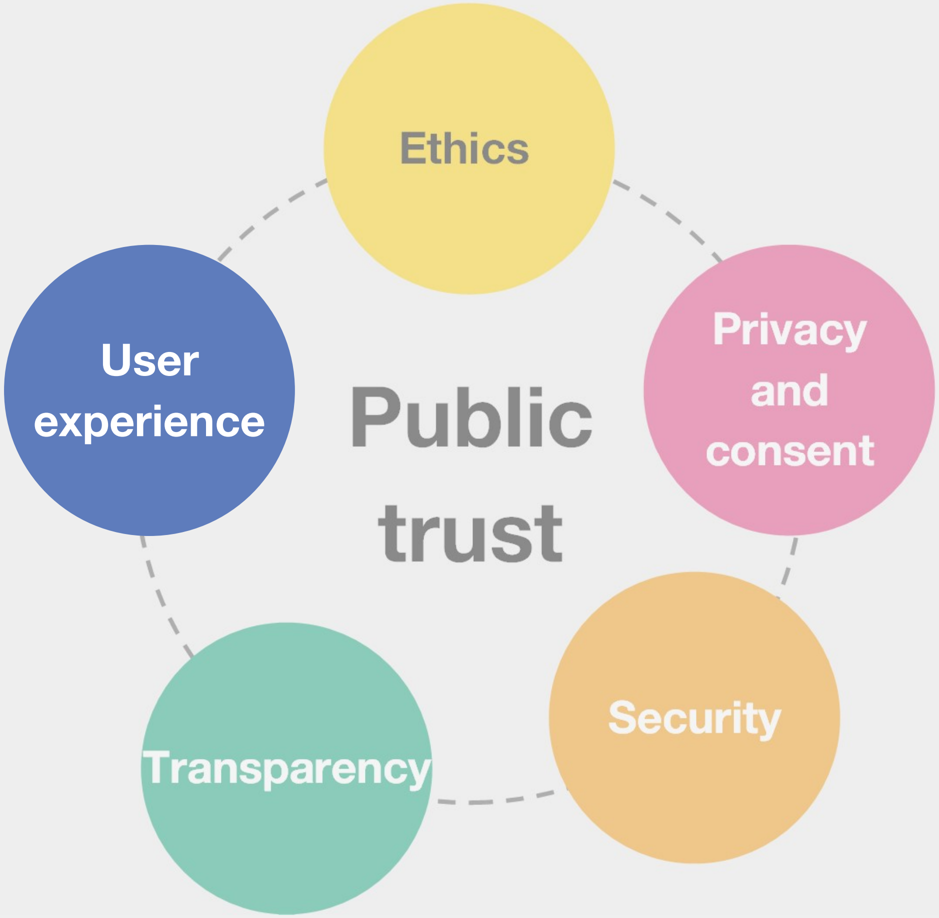
Security

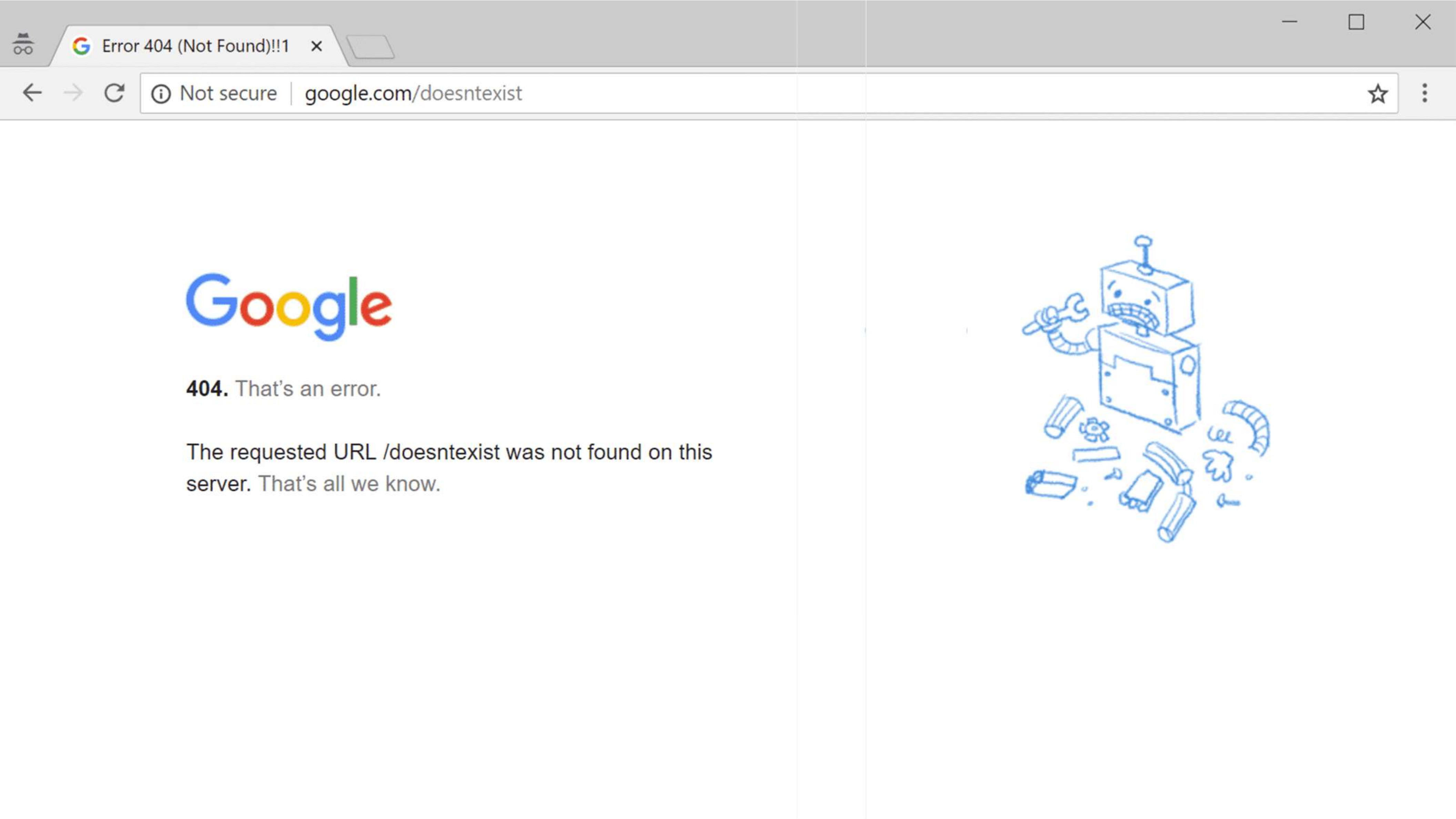
Transparency

User experience

Public trust

Trustworthy use of data and technology





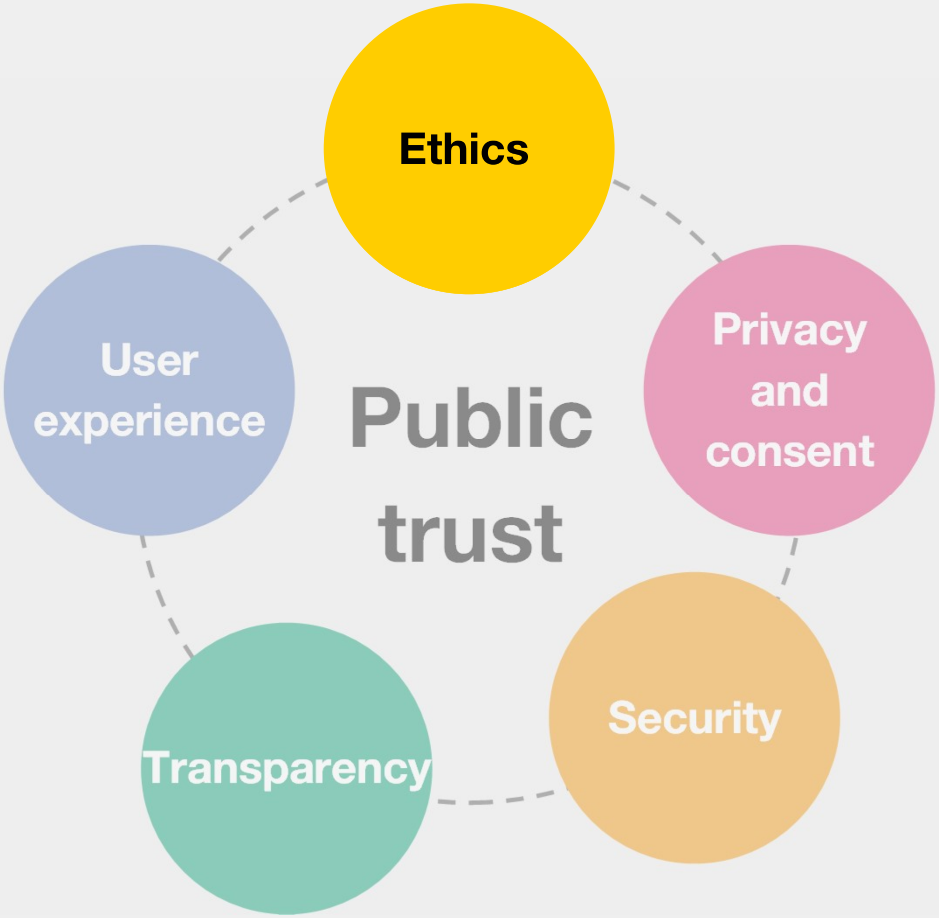
Error 404 (Not Found)!!1

Not secure | google.com/doesntexist

404. That’s an error.

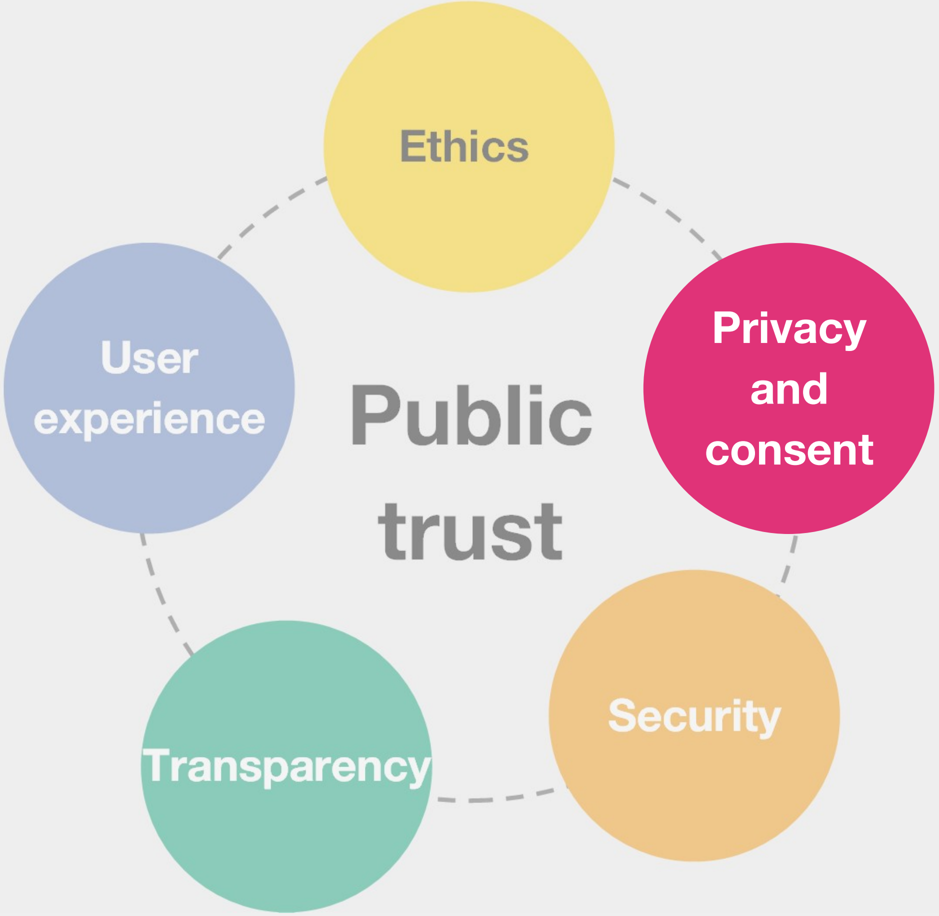
The requested URL /doesntexist was not found on this server. That’s all we know.

Trustworthy use of data and technology



OECD

Trustworthy use of data and technology



Ethics

Privacy and consent

Security

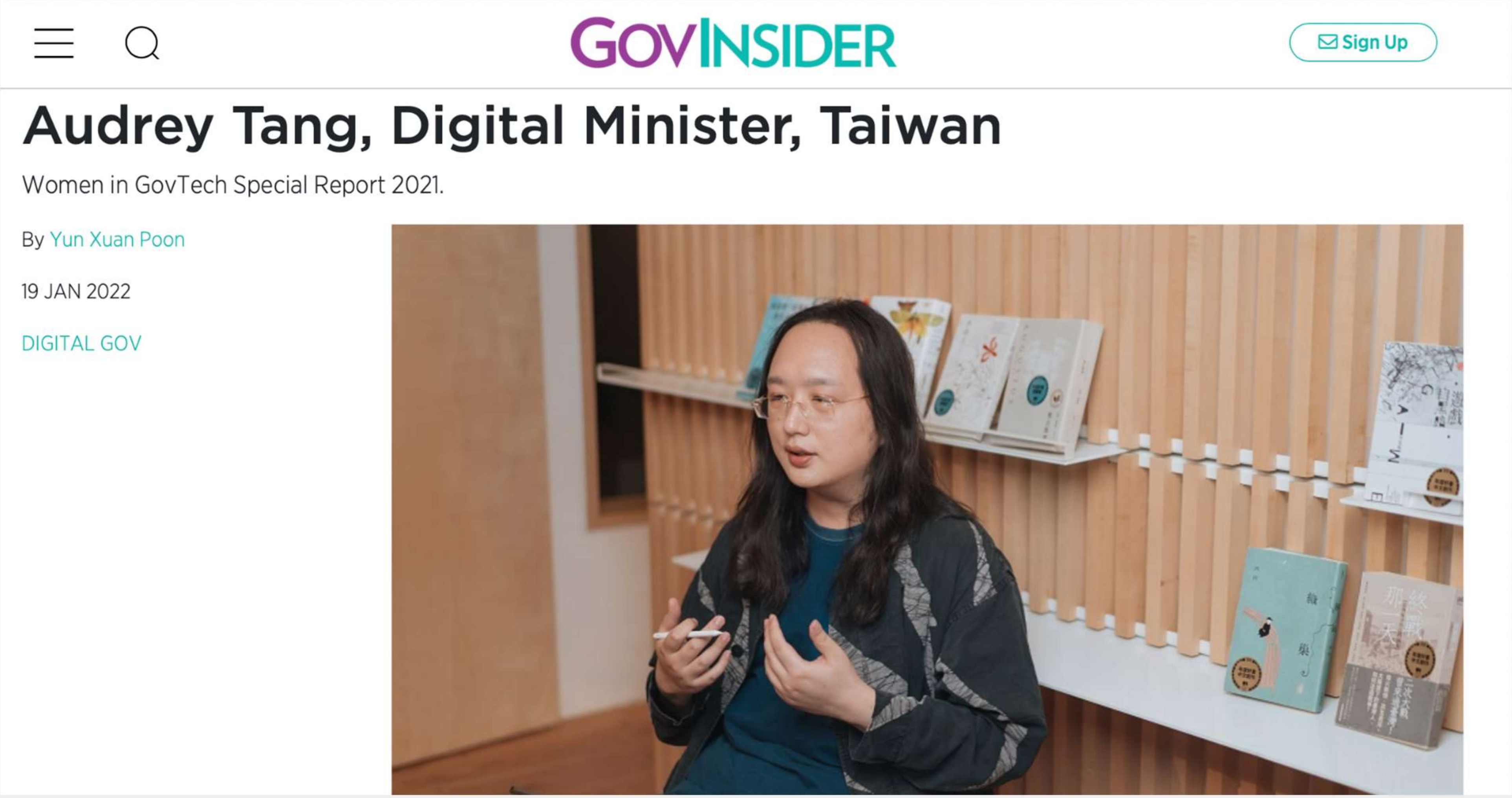
Transparency

User experience

Public trust

Data privacy is the right to have control over who can control your data, and for what purpose.

Example



Audrey Tang, Digital Minister, Taiwan

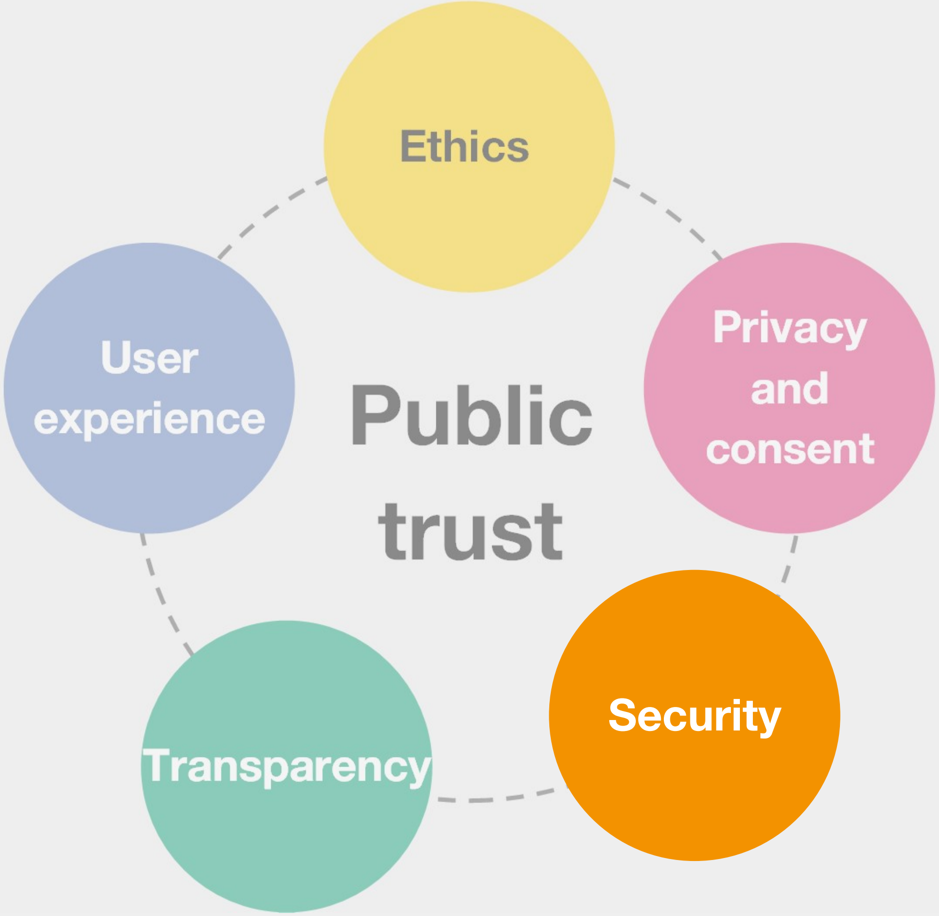
Women in GovTech Special Report 2021.

By Yun Xuan Poon

19 JAN 2022

DIGITAL GOV

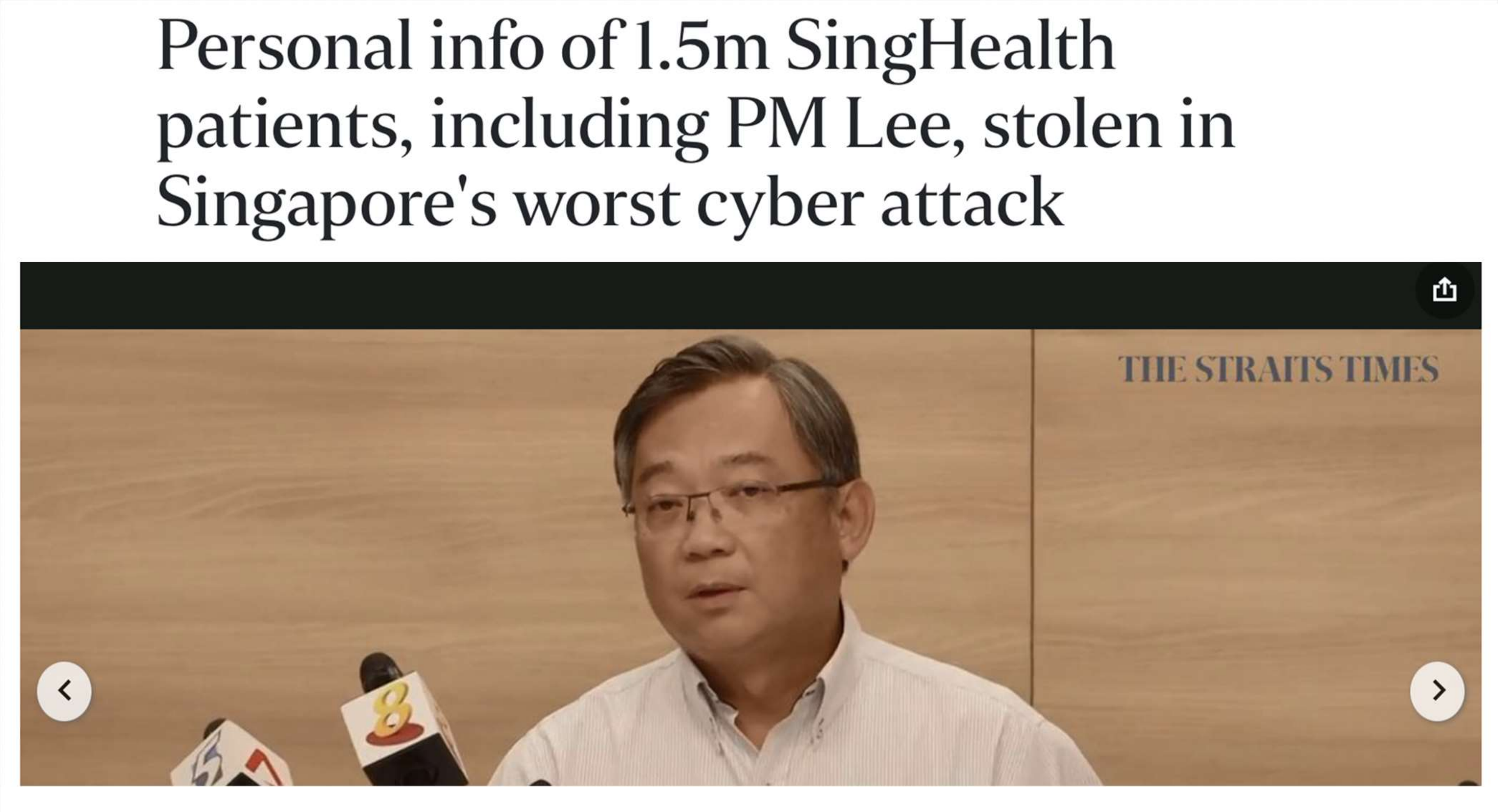
Trustworthy use of data and technology



OECD

Data security refers to the measures taken to prevent unauthorised access or use of data.

Example



Personal info of 1.5m SingHealth patients, including PM Lee, stolen in Singapore's worst cyber attack

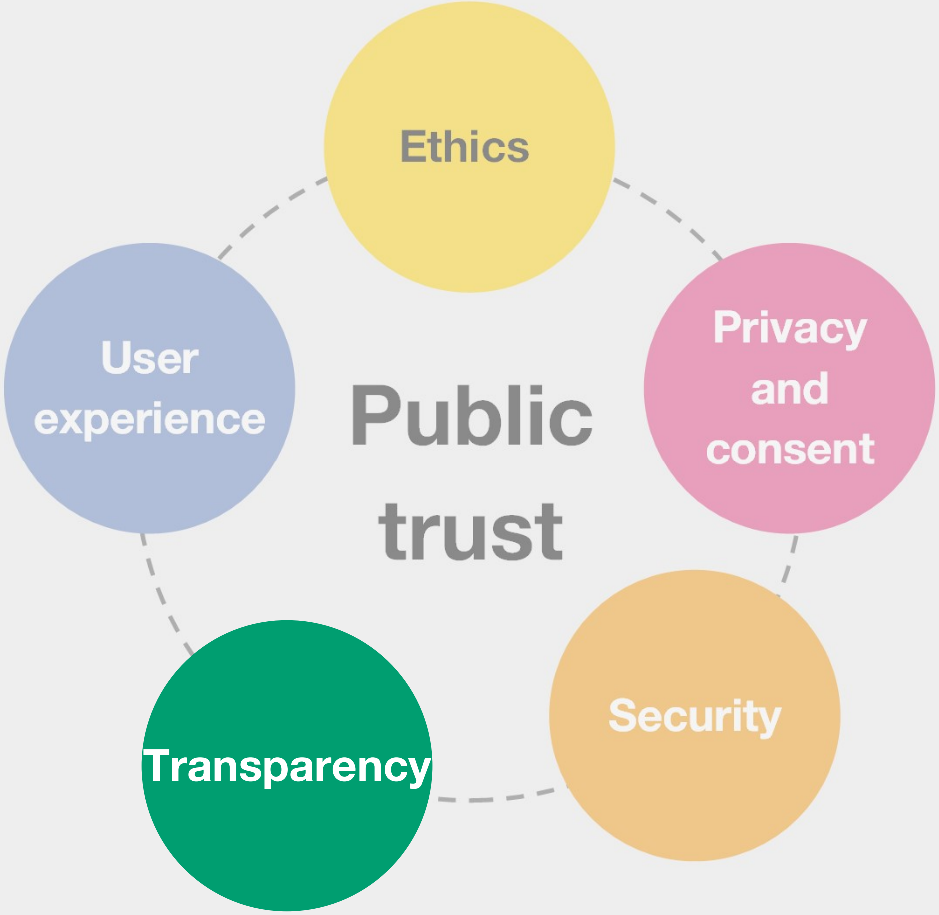
Example

Axa division in Asia hit by ransomware cyber attack

Stages in a cyber attack

Survey	Delivery	Breach	Affect
Investigating and analysing available information in order to identify potential vulnerabilities	Getting to the point in a system where you have an initial foothold in the system	Exploit vulnerability and gain unauthorised access	Carrying out activities within a system that achieve the attacker’s goal

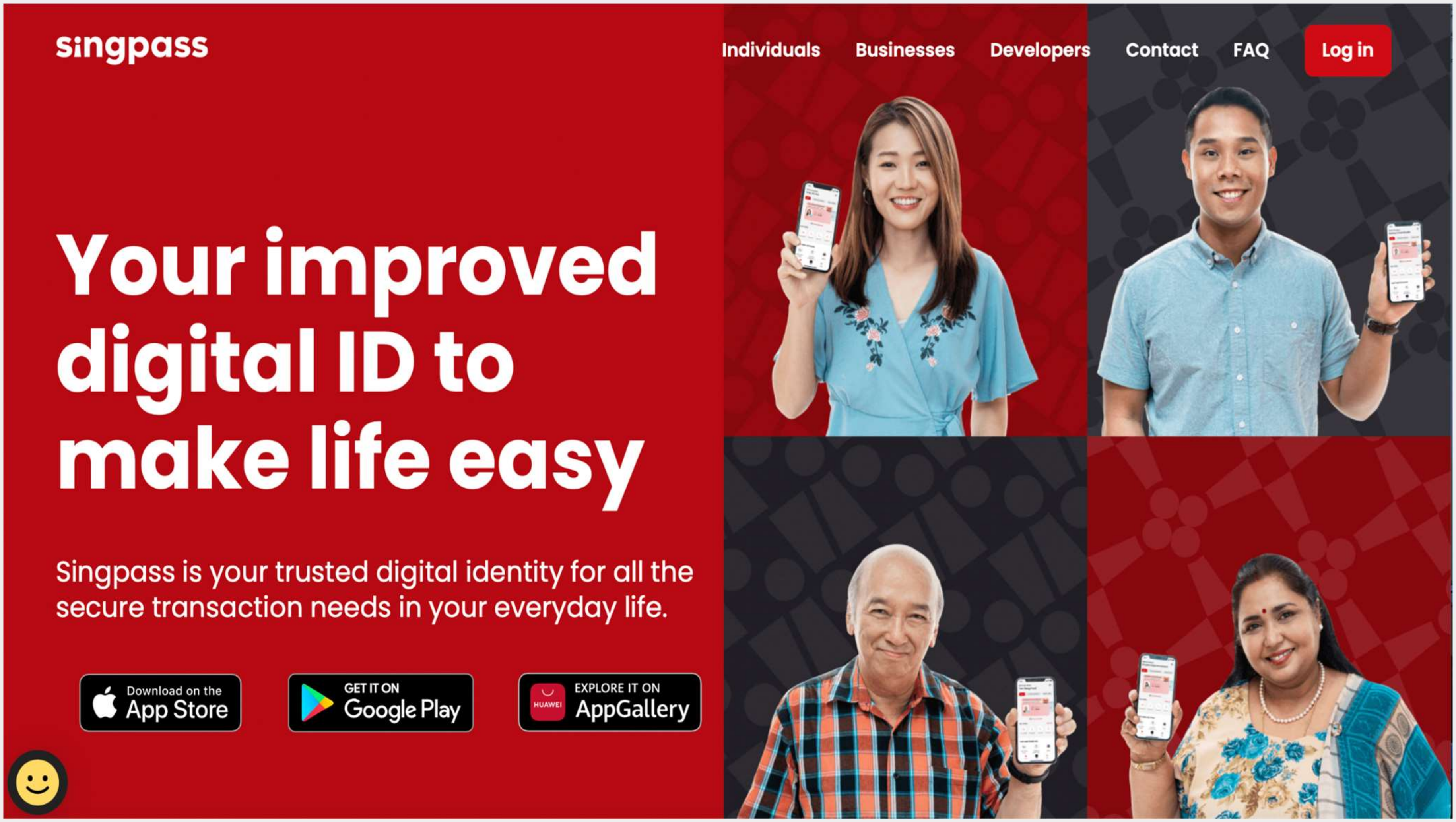
Trustworthy use of data and technology



What people need to know

- For what purpose their data is being used
- How their data is being used
- Who uses their data, and is responsible for it
- If their data was breached

Example

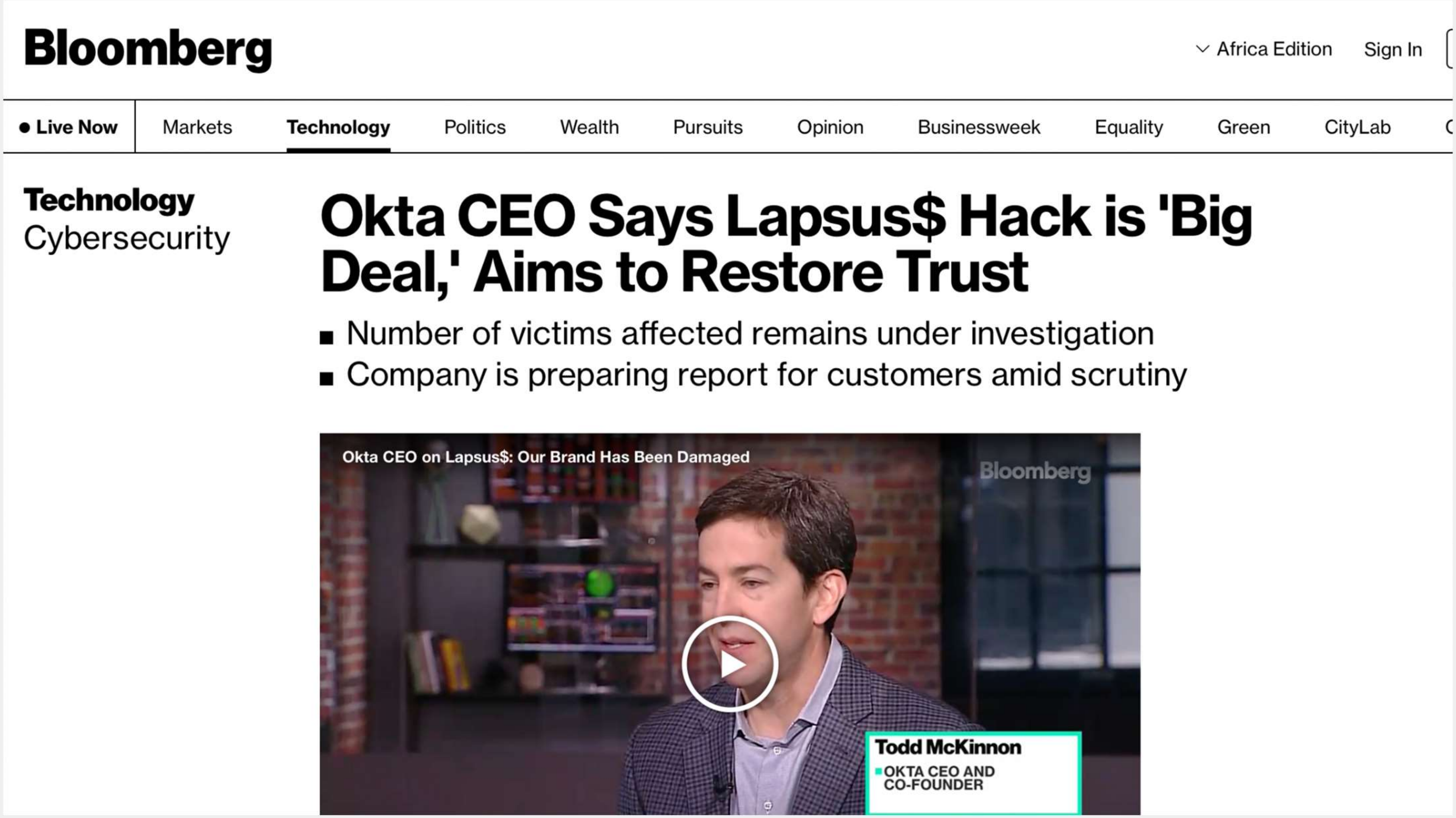


Your improved digital ID to make life easy

Singpass is your trusted digital identity for all the secure transaction needs in your everyday life.

Preparedness and **incident response** are as important as preventive cyber security measures.

Example



Technology
Cybersecurity

Okta CEO Says Lapsus$ Hack is 'Big Deal,' Aims to Restore Trust

- Number of victims affected remains under investigation
- Company is preparing report for customers amid scrutiny

⏱ 15-min group discussion

1. What are the risks associated with the increased use of data in the public sector?
2. What do you think are the barriers to trust?

1. Barriers and enablers to trust

2. Categorisation of data

3. Data protection

    a. Data privacy

    b. Cyber security

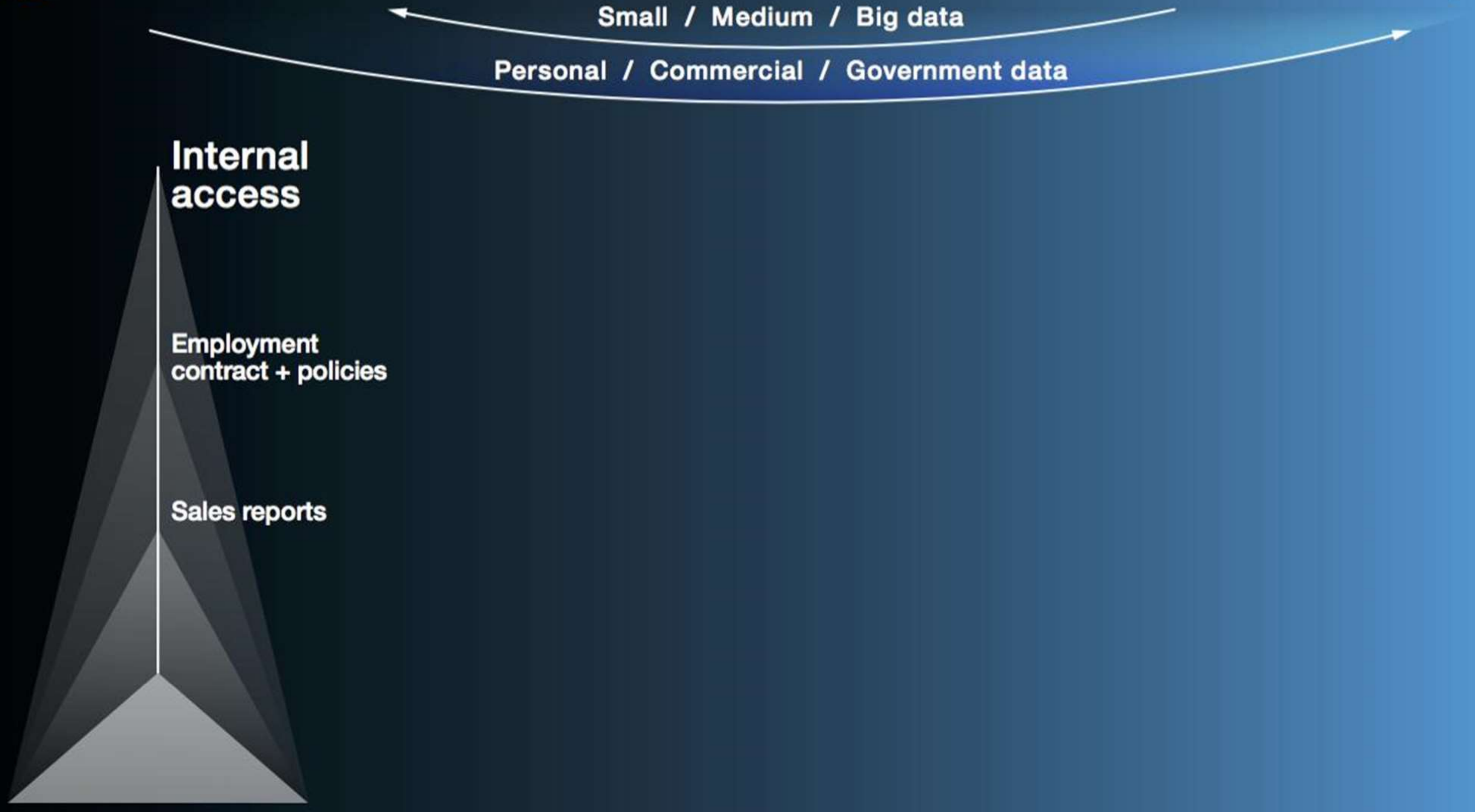
Different types of data require different levels of protection

Why categorise data?

- Understand the different types of data
- Understand what is being done with which data
- Understand how to protect which data

Data exists on a spectrum from **closed** to **open**.

The Data Spectrum



Small / Medium / Big data

Personal / Commercial / Government data

Internal access

Employment contract + policies

Sales reports

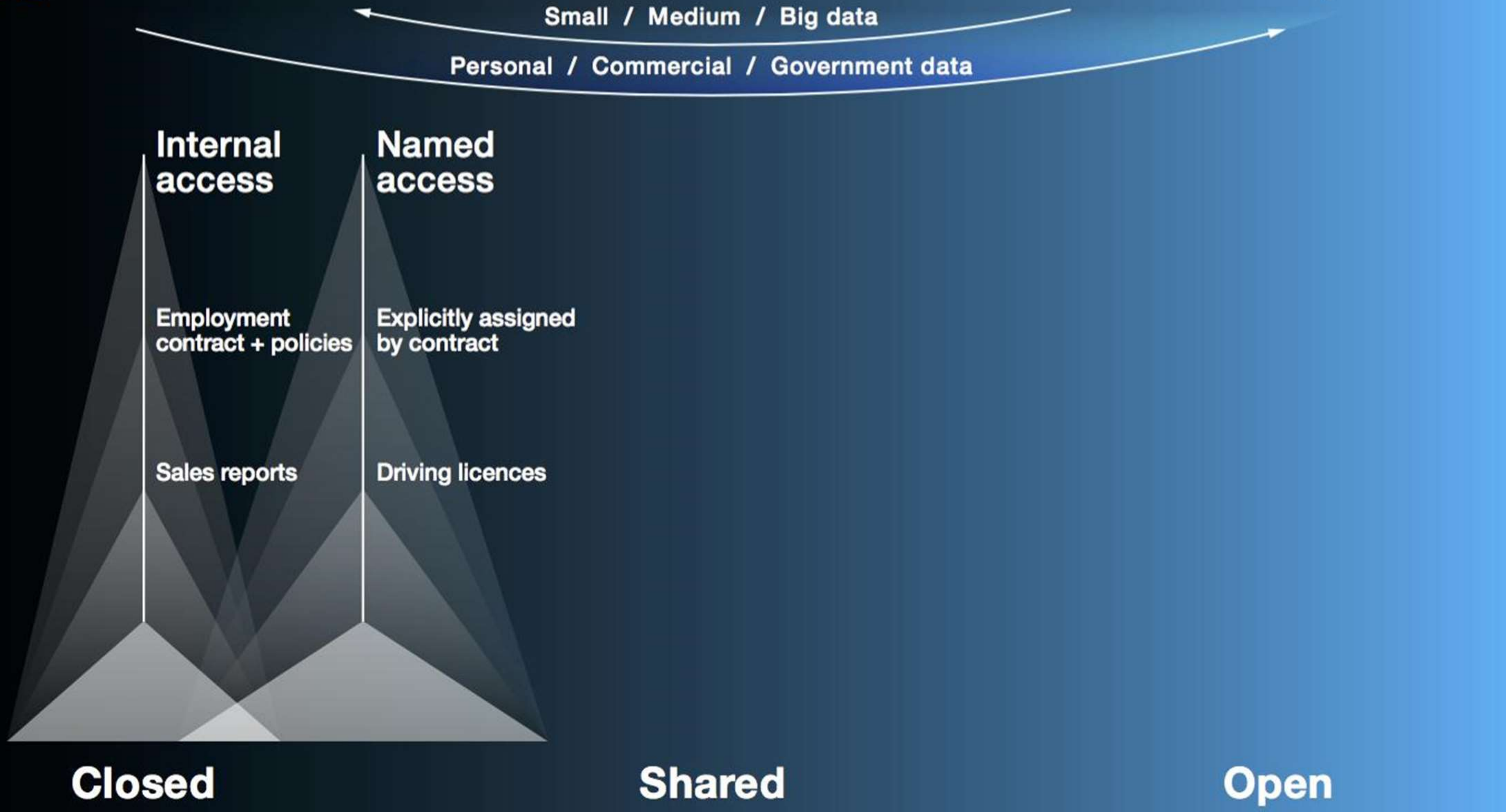
Closed

Shared

Open

theodi.org/data-spectrum

The Data Spectrum



Small / Medium / Big data

Personal / Commercial / Government data

Internal access

Employment contract + policies

Sales reports

Named access

Explicitly assigned by contract

Driving licences

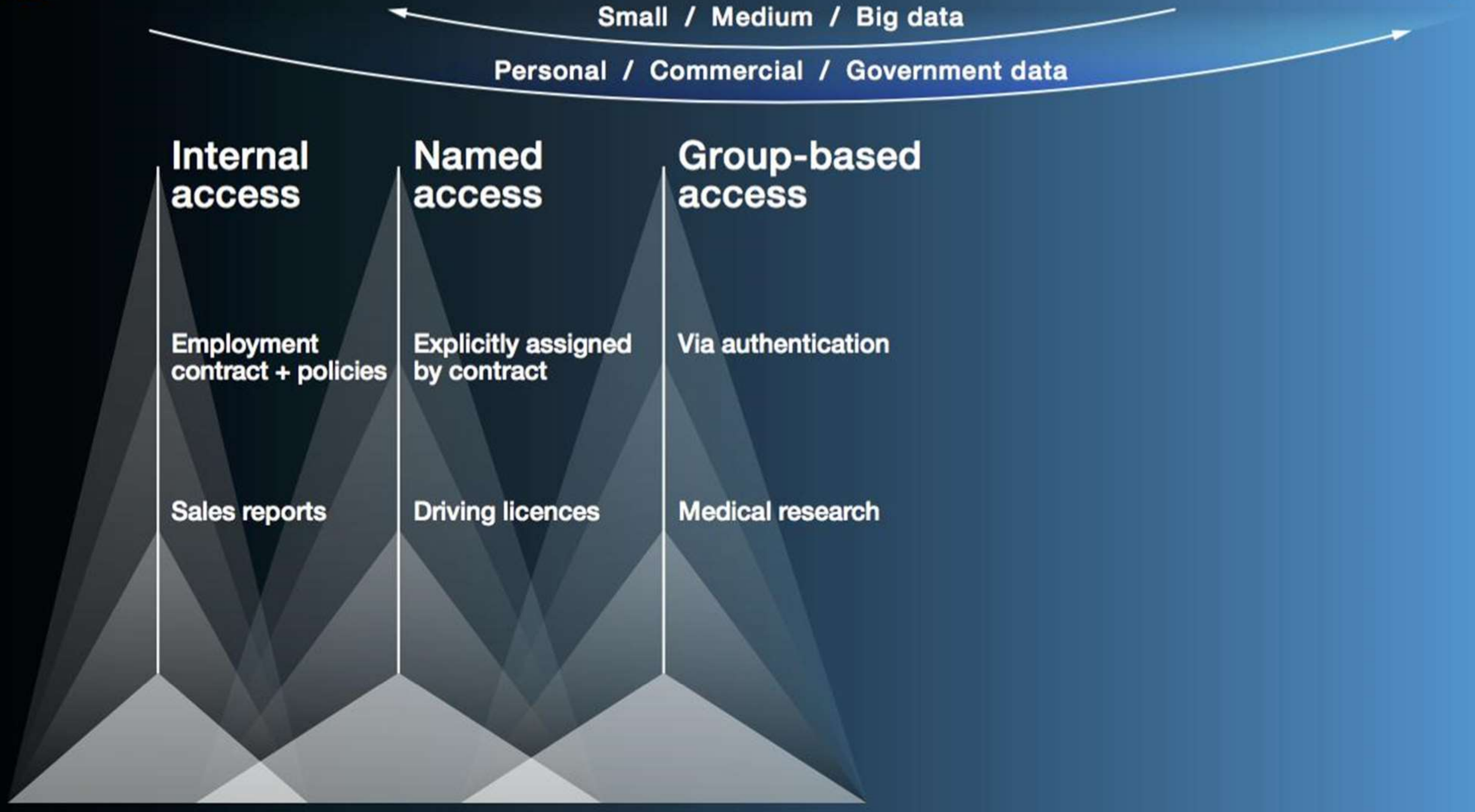
Closed

Shared

Open

theodi.org/data-spectrum

The Data Spectrum



Small / Medium / Big data

Personal / Commercial / Government data

Internal access

Employment contract + policies

Sales reports

Named access

Explicitly assigned by contract

Driving licences

Group-based access

Via authentication

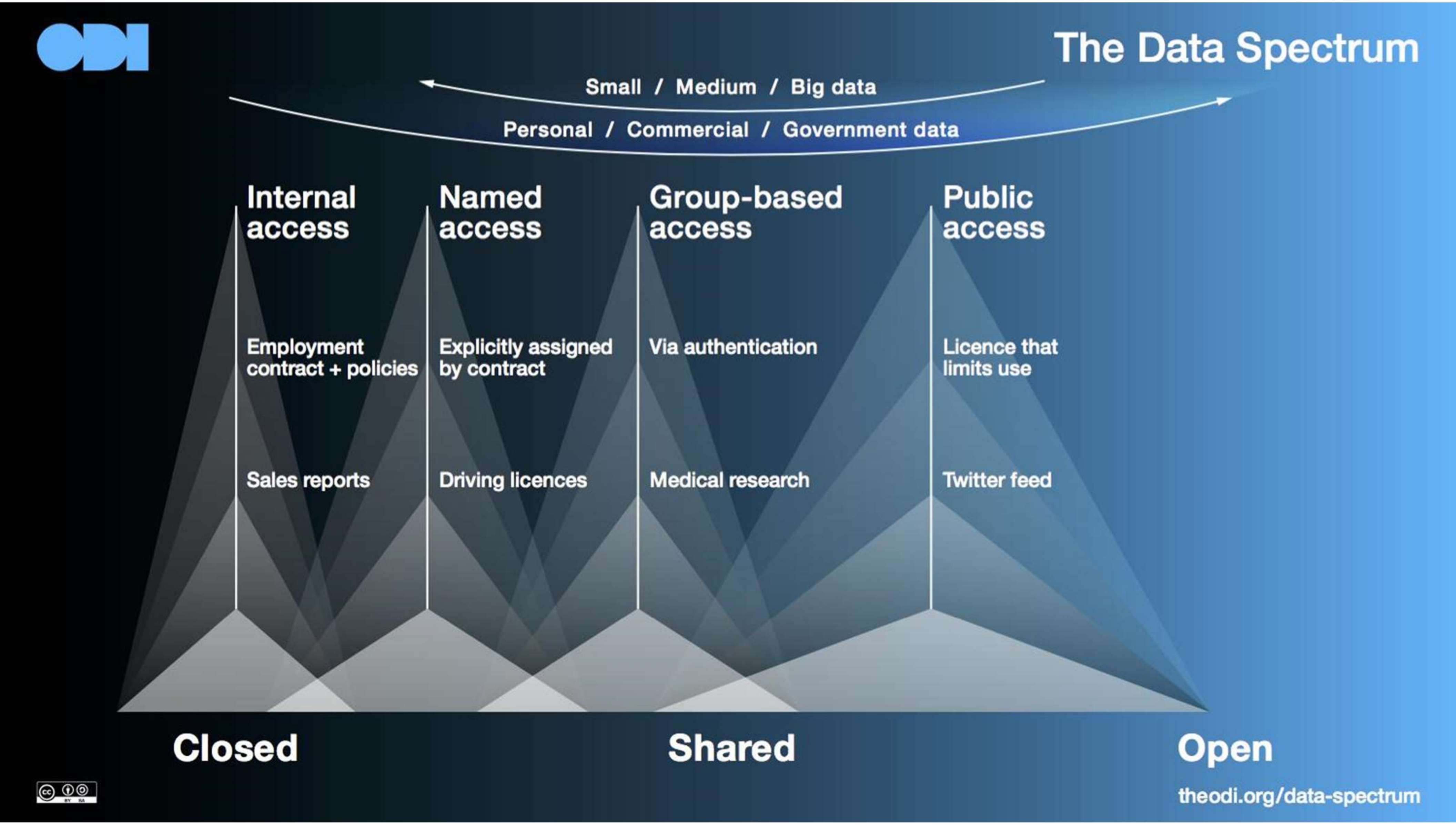
Medical research

Closed

Shared

Open

theodi.org/data-spectrum



The Data Spectrum

Small / Medium / Big data

Personal / Commercial / Government data

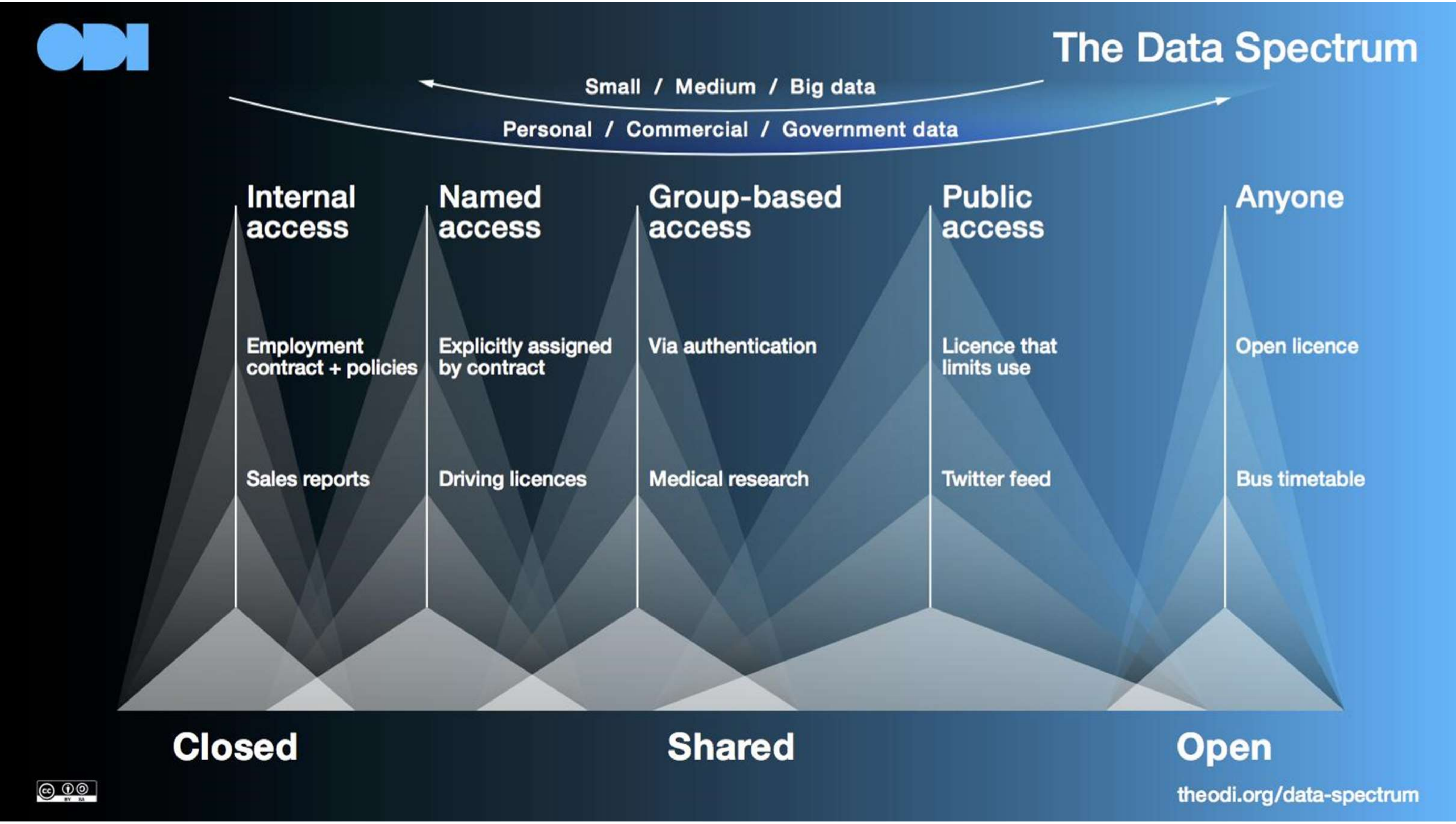
Internal access	Named access	Group-based access	Public access
Employment contract + policies	Explicitly assigned by contract	Via authentication	Licence that limits use
Sales reports	Driving licences	Medical research	Twitter feed

Closed

Shared

Open

theodi.org/data-spectrum



The Data Spectrum

Small / Medium / Big data

Personal / Commercial / Government data

Internal access	Named access	Group-based access	Public access	Anyone
Employment contract + policies	Explicitly assigned by contract	Via authentication	Licence that limits use	Open licence
Sales reports	Driving licences	Medical research	Twitter feed	Bus timetable

Closed

Shared

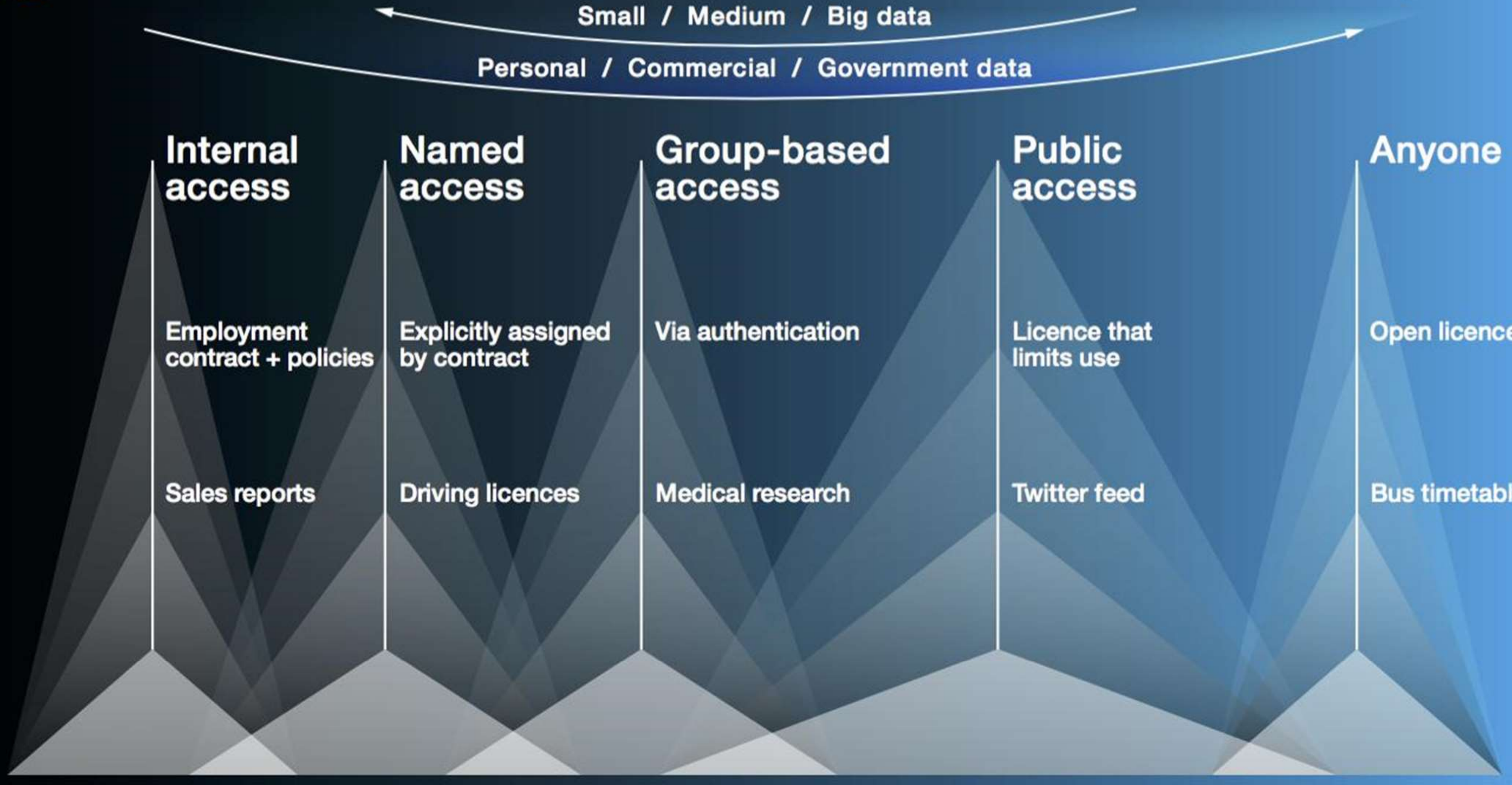
Open

theodi.org/data-spectrum

⏱ 15-min group discussion

1. Locate your organisation’s data on the ODI data spectrum.
2. What is your own assessment of how your organisation is protecting these different categories of data?

The Data Spectrum



Small / Medium / Big data

Personal / Commercial / Government data

Internal access	Named access	Group-based access	Public access	Anyone
Employment contract + policies	Explicitly assigned by contract	Via authentication	Licence that limits use	Open licence
Sales reports	Driving licences	Medical research	Twitter feed	Bus timetable

Closed — **Shared** — **Open**

theodi.org/data-spectrum

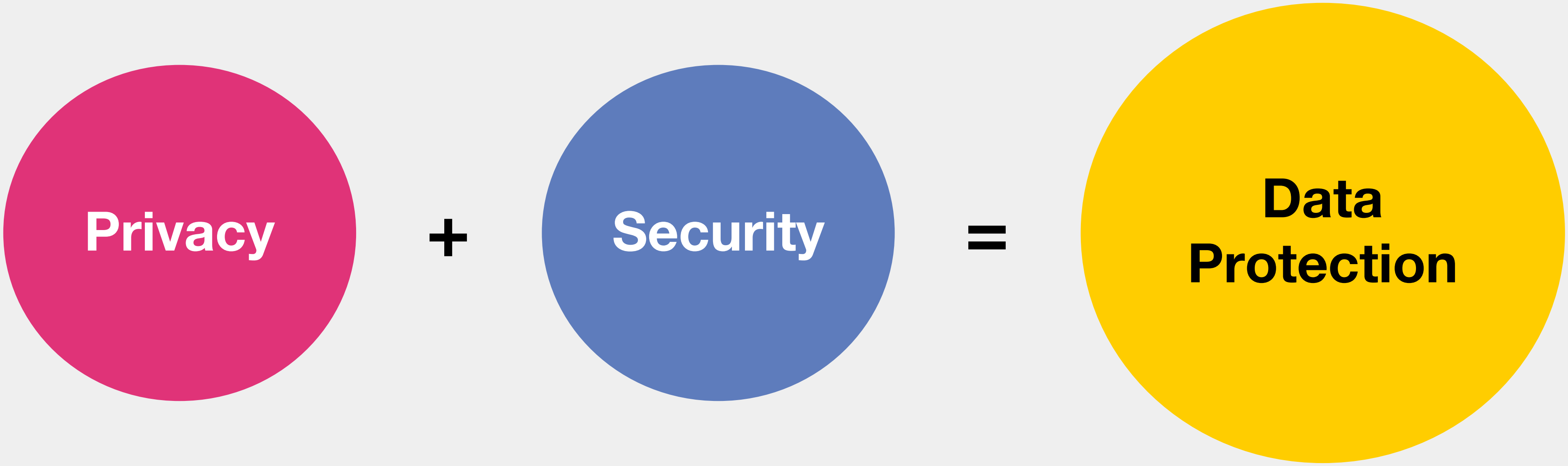
1. Barriers and enablers to trust

2. Categorisation of data

3. **Data protection**

    a. Data privacy

    b. Cyber security



Privacy + Security = Data Protection

1. Barriers and enablers to trust

2. Categorisation of data

3. Data protection

    a. Data privacy

    b. Cyber security

> ‘No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.’

Article 12 of the 1948 Universal Declaration of Human Rights

The Guardian

For 200 years

Monday
19 July 2021
£2.50 | €2.90
From £1.75 for subscribers

A Guardian special investigation

The Pegasus project

Revealed
Huge leak uncovers global abuse of spy weapon

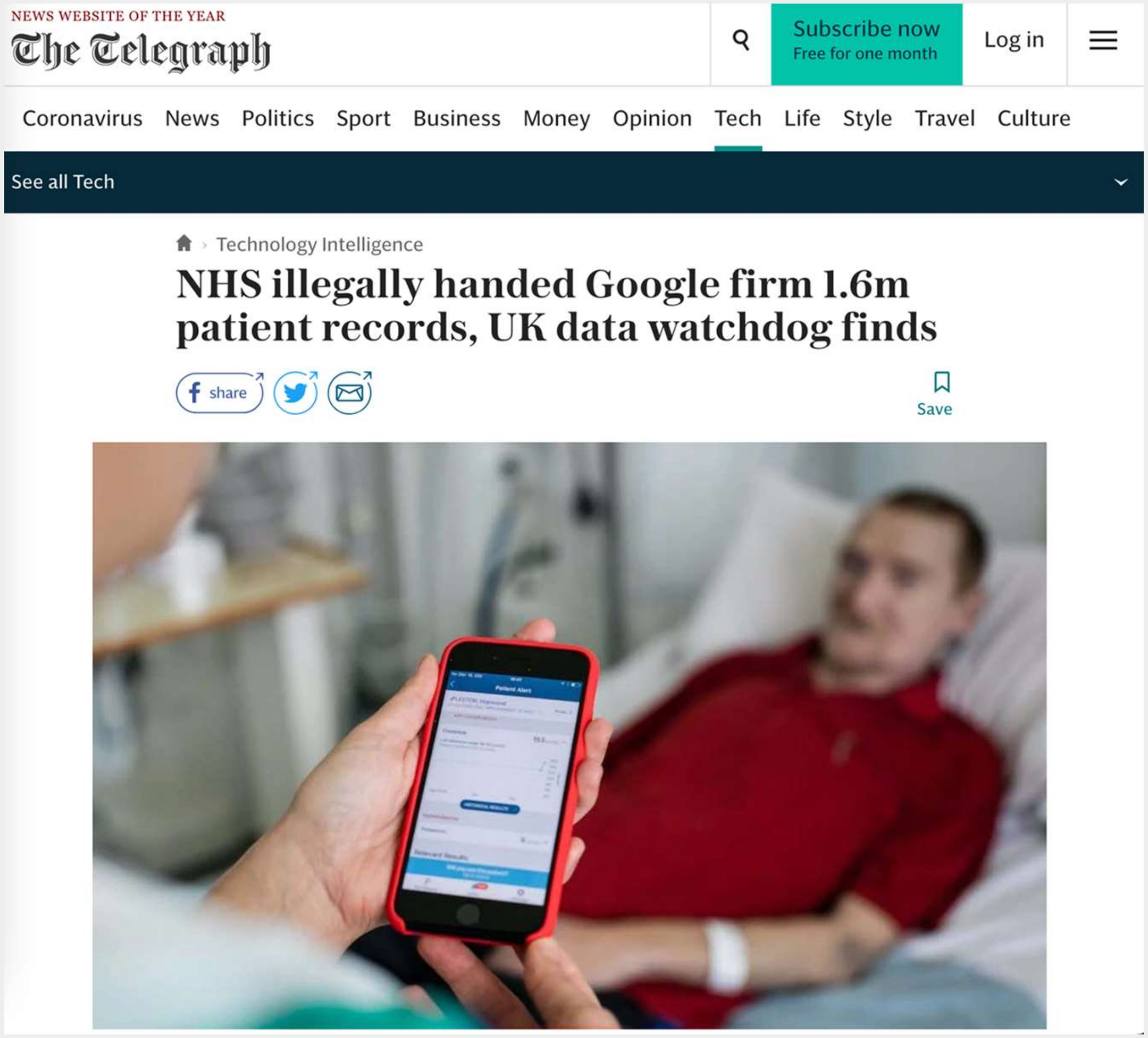
'It's heinous' Activists and journalists among thousands on list

Jamal Khashoggi Associates targeted after his death

Hungary How Orbán declared war on the media using tool

Day one
How autocratic governments target opponents
Pages 2-9

Example



Technology Intelligence

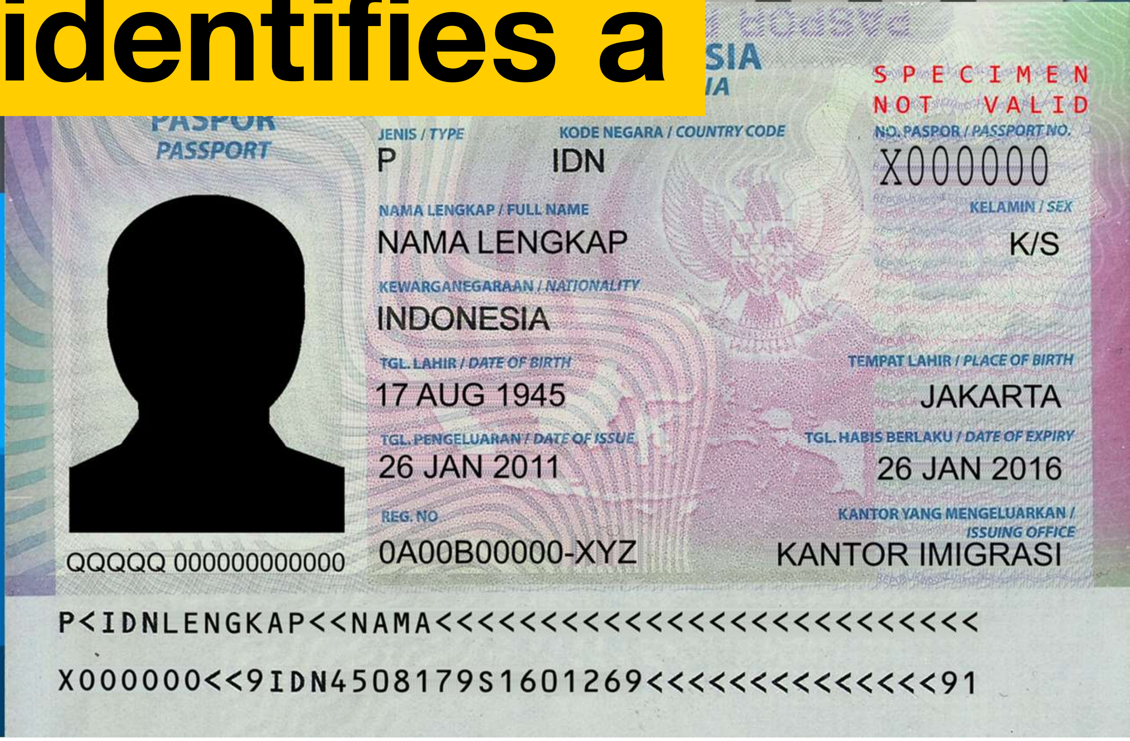
NHS illegally handed Google firm 1.6m patient records, UK data watchdog finds

GDPR
EU data
protection regime

Data subjects are the people whose data is being processed.

Data controllers determine the purposes and means for processing personal data.

Personal data identifies a person



SPECIMEN
NOT VALID

PASPOR
PASSPORT

JENIS / TYPE
P

KODE NEGARA / COUNTRY CODE
IDN

NO. PASPOR / PASSPORT NO.
X000000

NAMA LENGKAP / FULL NAME
NAMA LENGKAP

KELAMIN / SEX
K/S

KEWARGANEGARAAN / NATIONALITY
INDONESIA

TGL. LAHIR / DATE OF BIRTH
17 AUG 1945

TEMPAT LAHIR / PLACE OF BIRTH
JAKARTA

TGL. PENGELUARAN / DATE OF ISSUE
26 JAN 2011

TGL. HABIS BERLAKU / DATE OF EXPIRY
26 JAN 2016

REG. NO
0A00B00000-XYZ

KANTOR YANG MENGELUARKAN / ISSUING OFFICE
KANTOR IMIGRASI

QQQQQ 000000000000

```
P<IDNLENGKAP<<NAMA<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
X000000<<9IDN4508179S1601269<<<<<<<<<<<<<<<91
```

The General Data Protection Regulation (GDPR) has strengthened conditions for **consent**.

Rights of data subjects

- Access

Rights of data subjects

- Access
- Rectification

Rights of data subjects

- Access
- Rectification
- Be forgotten

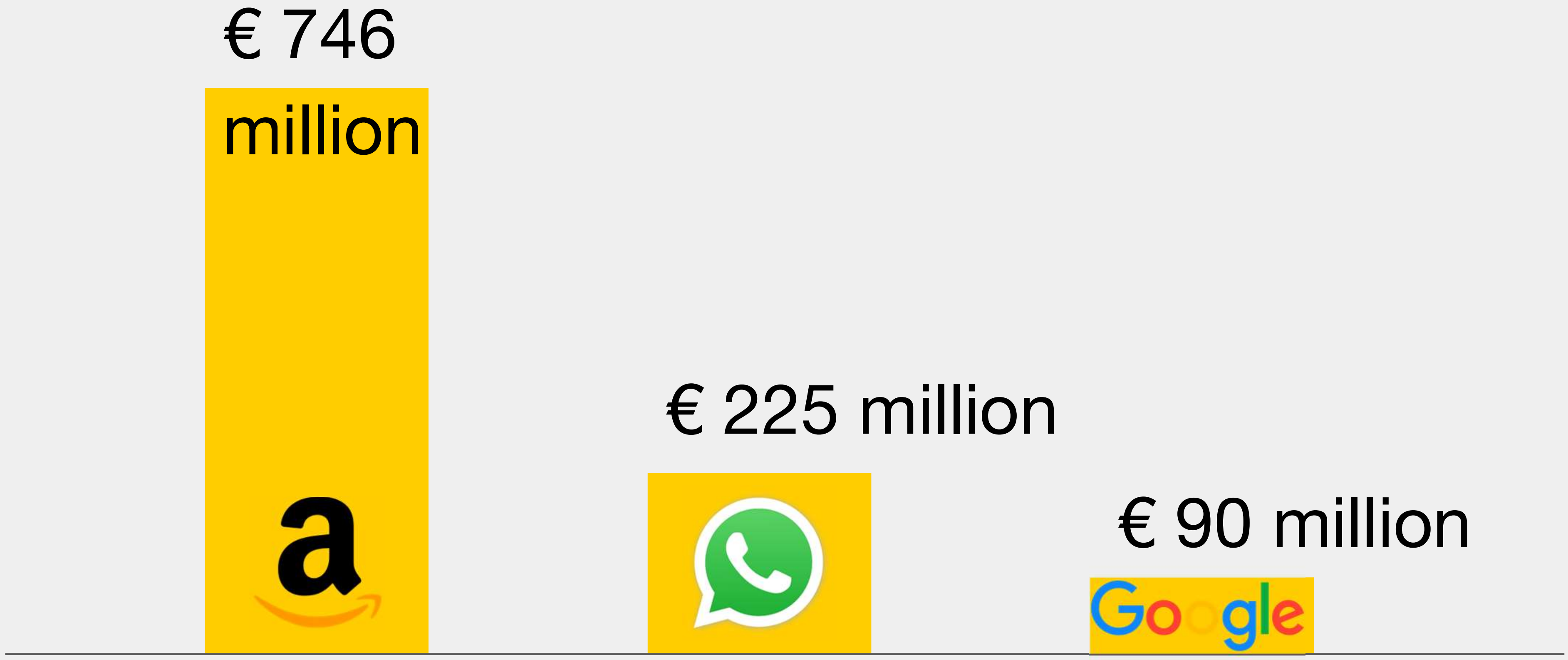
Rights of data subjects

- Access
- Rectification
- Be forgotten
- Restrict processing

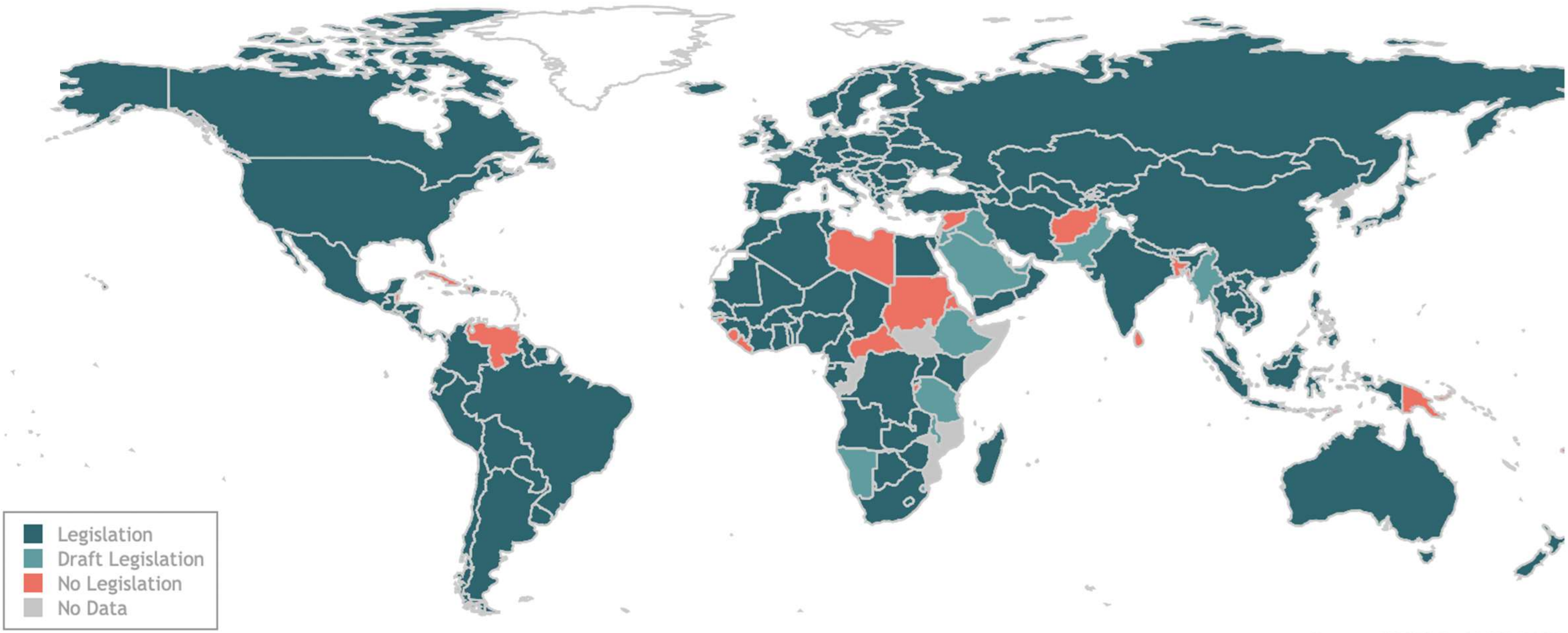
Rights of data subjects

- Access
- Rectification
- Be forgotten
- Restrict processing
- Data portability

Biggest GDPR fines



Data Protection and Privacy Legislation Worldwide



Source: UNCTAD, 14/12/2021

71% of countries have legislation

9% draft legislation

13% no legislation

5% no data

⏱️ 15-min group discussion

1. How would you assess your current services in terms of individual privacy rights that we discussed: right to access, right to rectification, right to be forgotten, right to restrict processing and data portability
2. What could be done better?

1. Barriers and enablers to trust

2. Categorisation of data

3. Data protection

    a. Data privacy

    b. Cyber security

⏱ 5-min group discussion

What comes to your mind when asked how you would **secure** a digital service?

85% of data breaches are caused by **human error**.

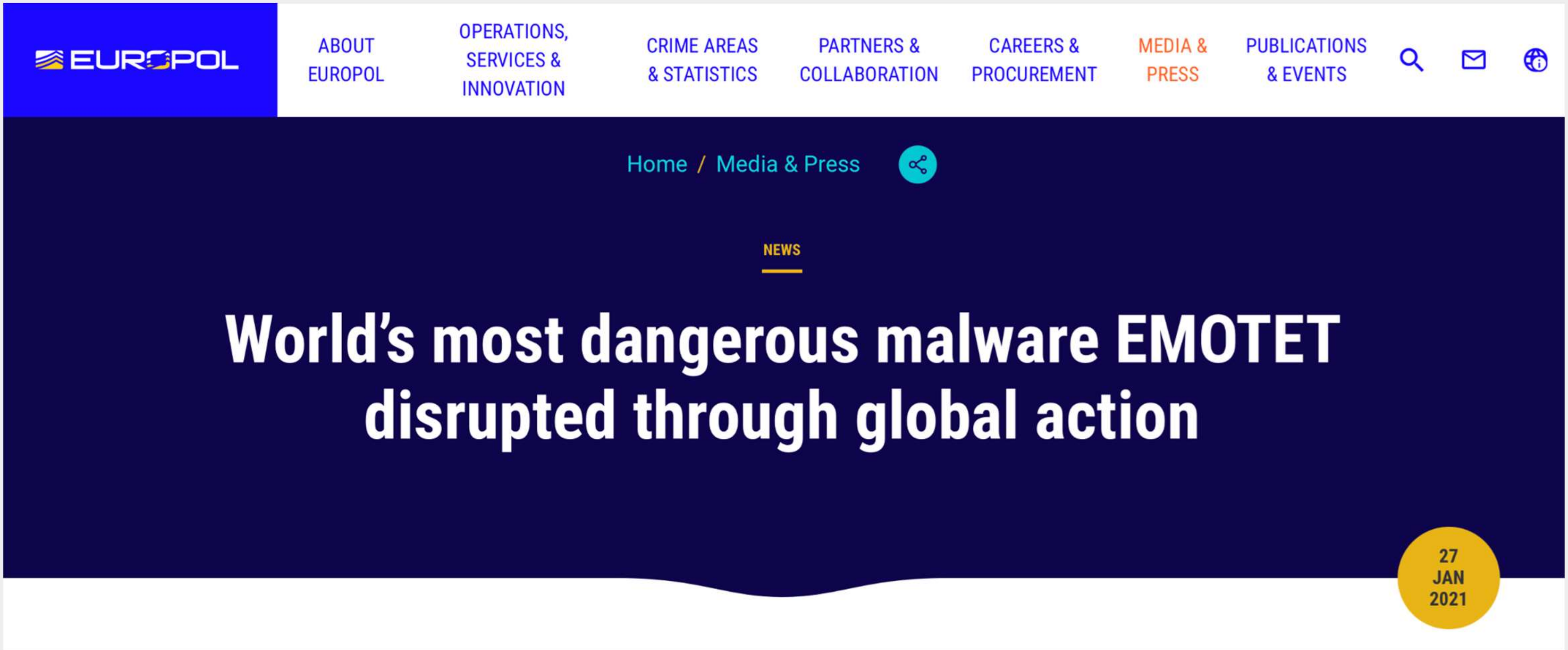
Confidentiality

Integrity

Availability

MALWARE

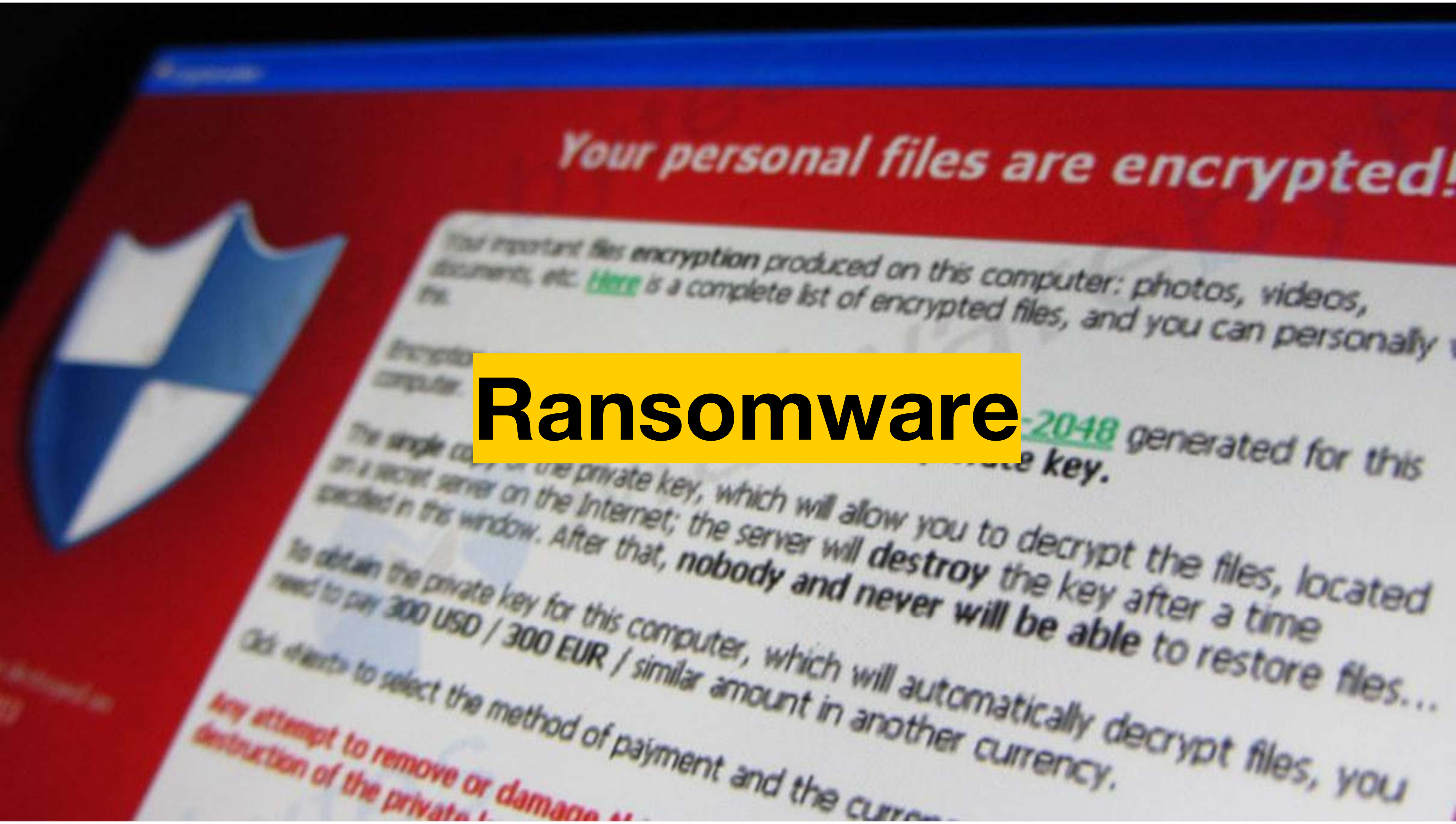
Example



World’s most dangerous malware EMOTET disrupted through global action

27 JAN 2021

Ransomware



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally v this.

Encryption computer.

-2048 generated for this key.

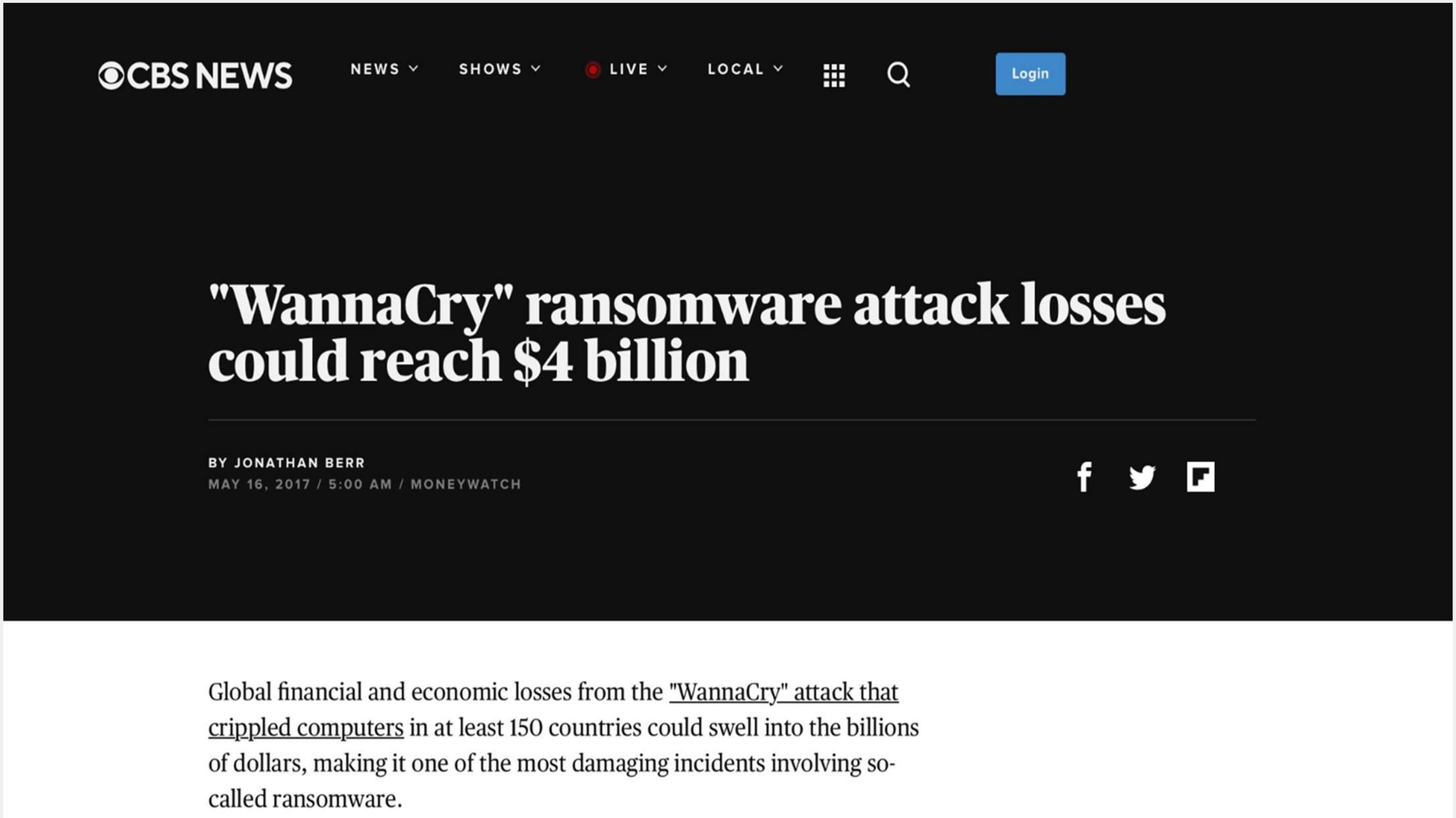
The **single** copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment and the curren

Any attempt to remove or damage th destruction of the private k

Example



"WannaCry" ransomware attack losses could reach $4 billion

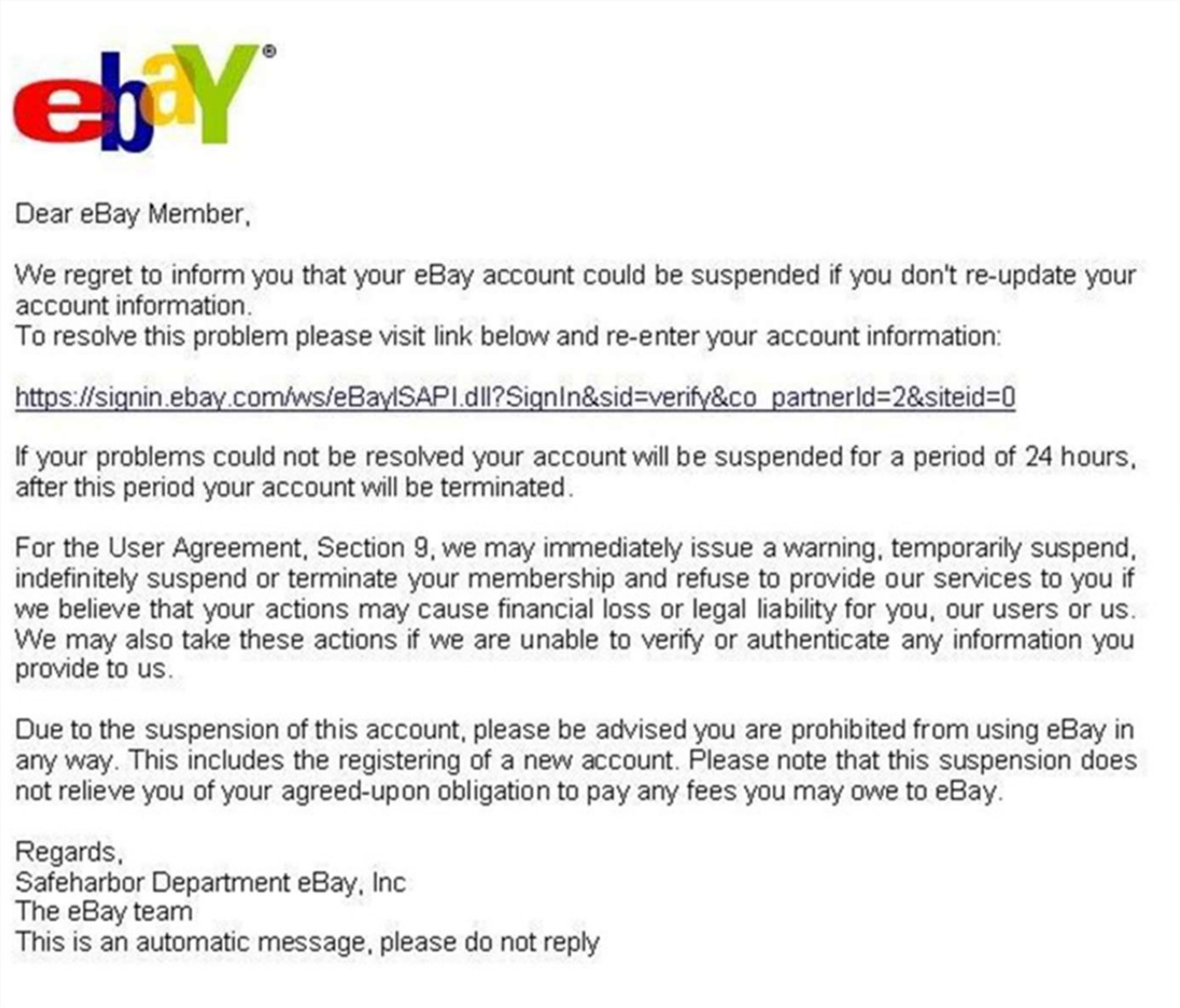
BY JONATHAN BERR

MAY 16, 2017 / 5:00 AM / MONEYWATCH

Global financial and economic losses from the "WannaCry" attack that crippled computers in at least 150 countries could swell into the billions of dollars, making it one of the most damaging incidents involving so-called ransomware.

Phishing

Example



Dear eBay Member,

We regret to inform you that your eBay account could be suspended if you don't re-update your account information.
To resolve this problem please visit link below and re-enter your account information:

https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerId=2&siteid=0

If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

Regards,
Safeharbor Department eBay, Inc
The eBay team
This is an automatic message, please do not reply

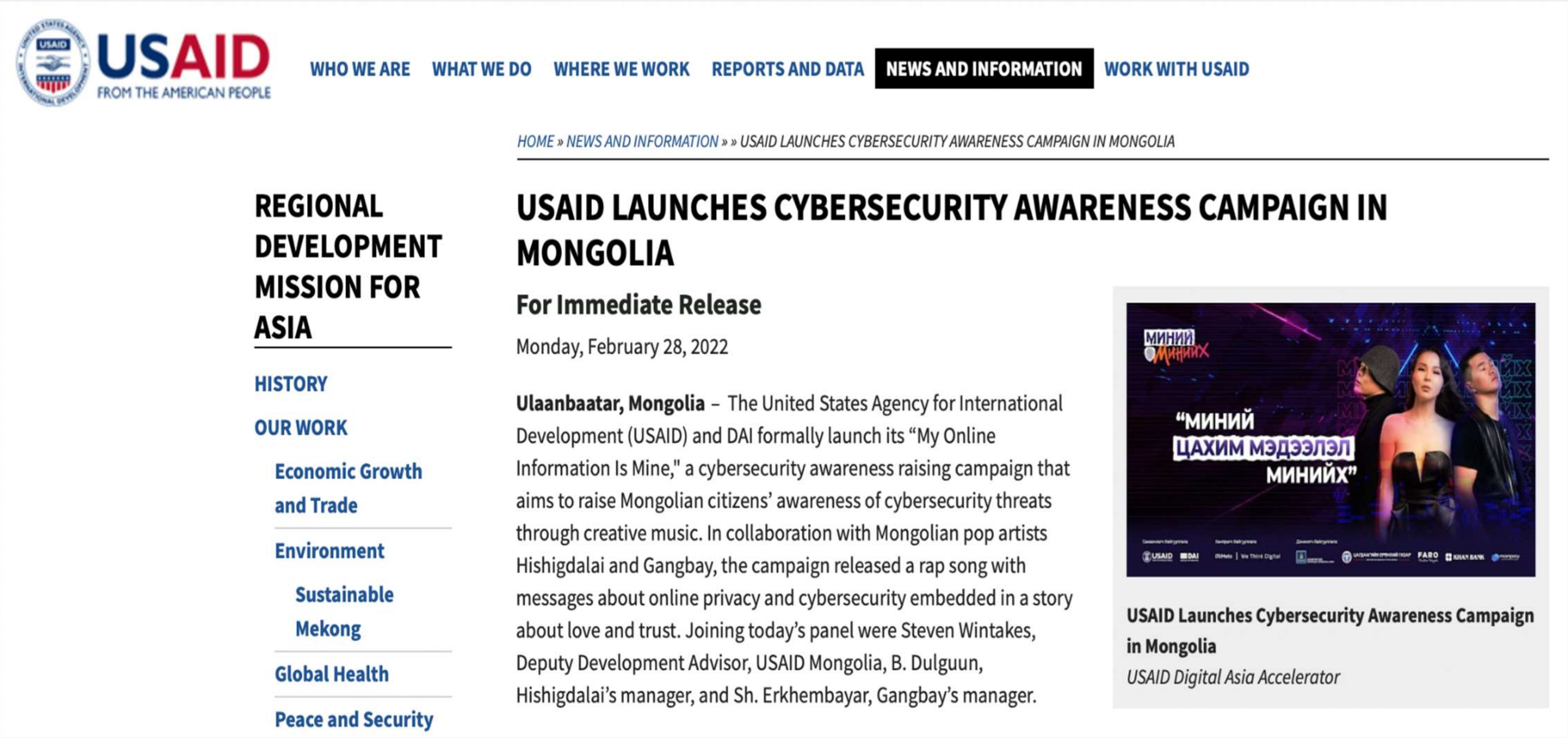
Cyber hygiene tips

- Update software regularly
- If in doubt, do not click or open
- Use strong passwords and multi-factor authentication
- Don’t send sensitive information unencrypted by mail
- Protect your devices with antivirus software
- Check the security policy for accessing government information

What can governments do?

- Increase cyber security awareness

Example



USAID LAUNCHES CYBERSECURITY AWARENESS CAMPAIGN IN MONGOLIA

For Immediate Release

Monday, February 28, 2022

Ulaanbaatar, Mongolia – The United States Agency for International Development (USAID) and DAI formally launch its “My Online Information Is Mine," a cybersecurity awareness raising campaign that aims to raise Mongolian citizens’ awareness of cybersecurity threats through creative music. In collaboration with Mongolian pop artists Hishigdalai and Gangbay, the campaign released a rap song with messages about online privacy and cybersecurity embedded in a story about love and trust. Joining today’s panel were Steven Wintakes, Deputy Development Advisor, USAID Mongolia, B. Dulguun, Hishigdalai’s manager, and Sh. Erkhembayar, Gangbay’s manager.

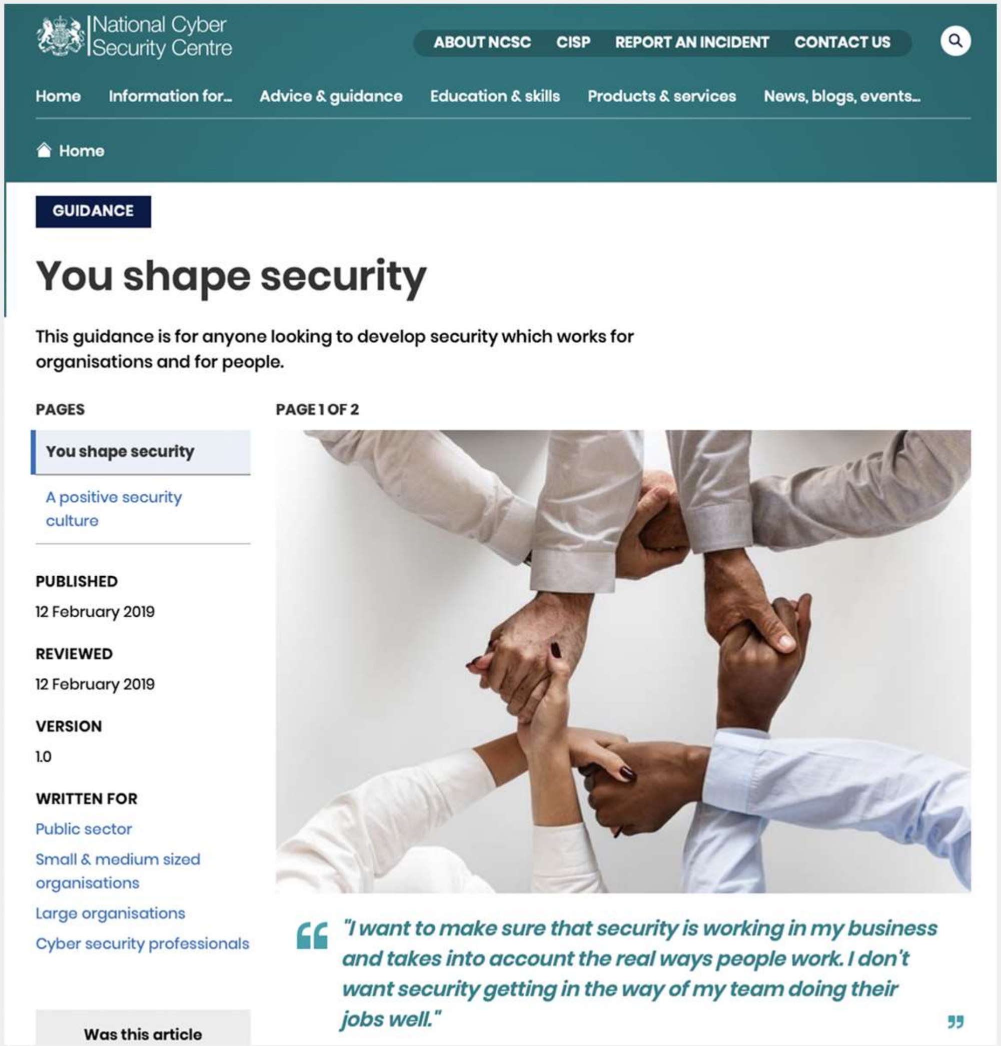
USAID Launches Cybersecurity Awareness Campaign in Mongolia

USAID Digital Asia Accelerator

What can governments do?

- Increase cyber security awareness
- Adopt a human-centred approach to cyber security

Example



You shape security

This guidance is for anyone looking to develop security which works for organisations and for people.

PAGES

- You shape security
- A positive security culture

PAGE 1 OF 2

PUBLISHED
12 February 2019

REVIEWED
12 February 2019

VERSION
1.0

WRITTEN FOR
Public sector
Small & medium sized organisations
Large organisations
Cyber security professionals

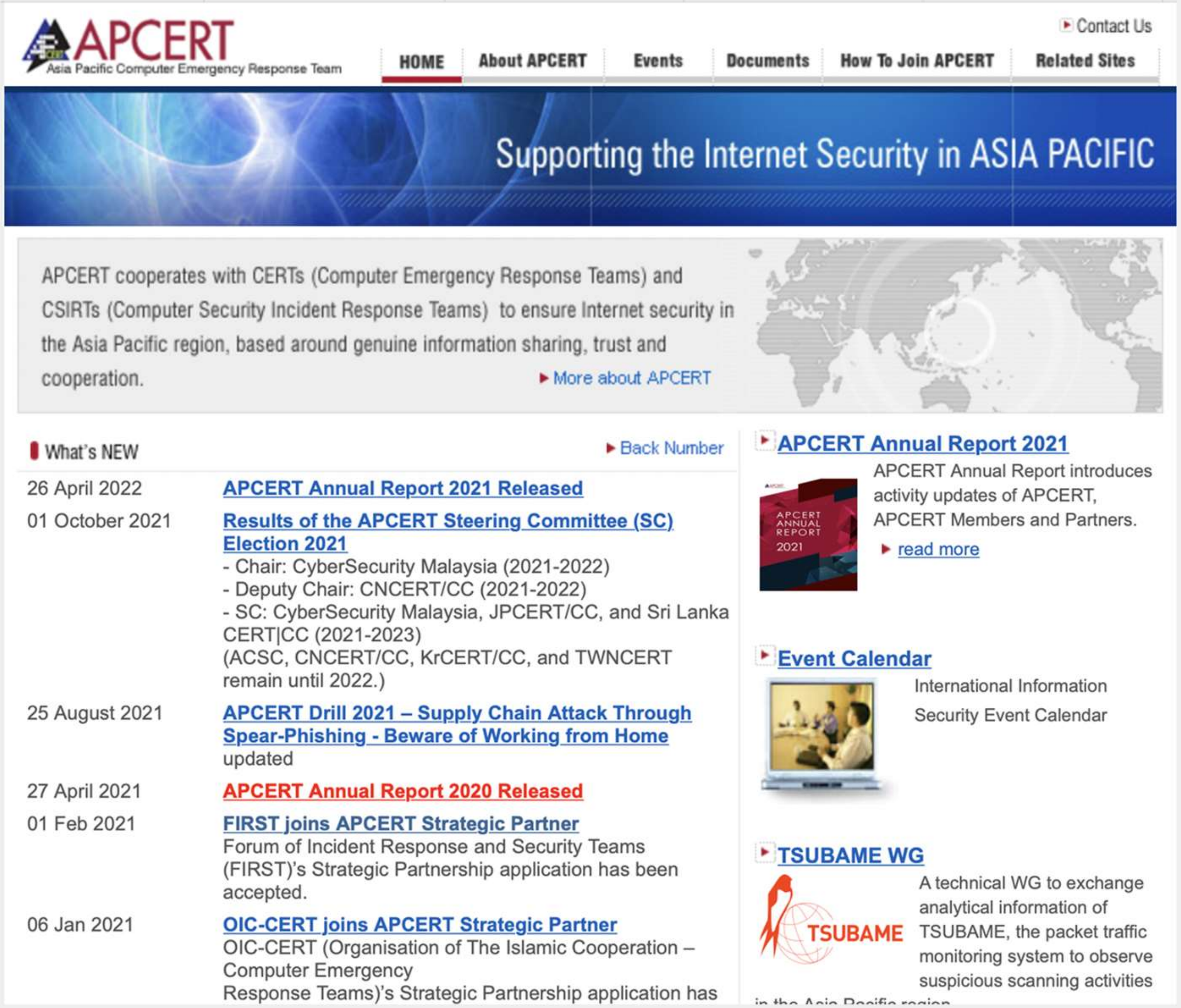
> *"I want to make sure that security is working in my business and takes into account the real ways people work. I don't want security getting in the way of my team doing their jobs well."*

Was this article

What can governments do?

- Increase cyber security awareness
- Adopt a human-centred approach to cyber security
- Build incident response capabilities

Example


APCERT
Asia Pacific Computer Emergency Response Team
Contact Us
HOME
About APCERT
Events
Documents
How To Join APCERT
Related Sites
Supporting the Internet Security in ASIA PACIFIC
APCERT ANNUAL REPORT 2021
TSUBAME

APCERT cooperates with CERTs (Computer Emergency Response Teams) and CSIRTs (Computer Security Incident Response Teams) to ensure Internet security in the Asia Pacific region, based around genuine information sharing, trust and cooperation. ▸ More about APCERT

What's NEW ▸ Back Number

26 April 2022	**APCERT Annual Report 2021 Released**
01 October 2021	**Results of the APCERT Steering Committee (SC) Election 2021** - Chair: CyberSecurity Malaysia (2021-2022) - Deputy Chair: CNCERT/CC (2021-2022) - SC: CyberSecurity Malaysia, JPCERT/CC, and Sri Lanka CERT|CC (2021-2023) (ACSC, CNCERT/CC, KrCERT/CC, and TWNCERT remain until 2022.)
25 August 2021	**APCERT Drill 2021 – Supply Chain Attack Through Spear-Phishing - Beware of Working from Home** updated
27 April 2021	**APCERT Annual Report 2020 Released**
01 Feb 2021	**FIRST joins APCERT Strategic Partner** Forum of Incident Response and Security Teams (FIRST)'s Strategic Partnership application has been accepted.
06 Jan 2021	**OIC-CERT joins APCERT Strategic Partner** OIC-CERT (Organisation of The Islamic Cooperation – Computer Emergency Response Teams)'s Strategic Partnership application has

▸ **APCERT Annual Report 2021**

APCERT Annual Report introduces activity updates of APCERT, APCERT Members and Partners.

▸ read more

▸ **Event Calendar**

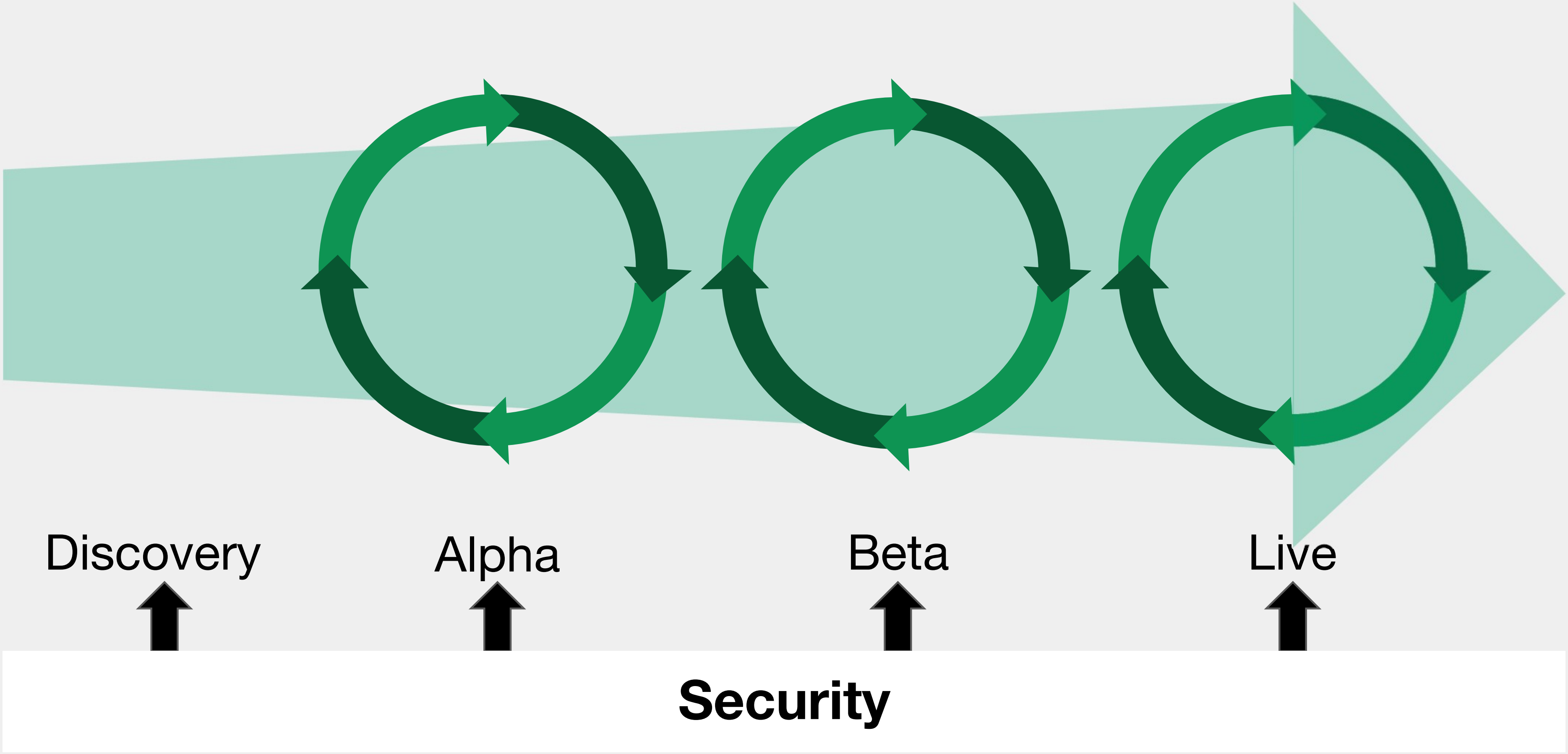
International Information Security Event Calendar

▸ **TSUBAME WG**

A technical WG to exchange analytical information of TSUBAME, the packet traffic monitoring system to observe suspicious scanning activities in the Asia Pacific region

It is difficult to add security in **after** a digital service is built.

Security by design



What can you do concretely?

- Set up multi-disciplinary digital teams
- Implement service standards
- Involve information security experts in procurement
- Test regularly

⏱ 15-min group discussion

1. What are the biggest challenges that you foresee in building trust in digital services in your context?
2. What are the quick wins and the next steps that you can take to make digital services more secure?

Takeaways

- Digital government can help build people’s trust through increased transparency, enhanced citizen participation and responsive, effective and inclusive digital services.
- The dimensions of a trustworthy digital service are user experience, ethics, privacy, security and transparency.
- Data categorisation helps to assess the level of protection required for different types of data.

Takeaways

- Data privacy is a fundamental human right which all digital services should respect and protect.
- Governments have an important role to play in improving cybersecurity by increasing awareness, designing human-centred security policies and building incident response capability.
- Security is not an afterthought and must be included in all stages of the service development lifecycle.

Next module:

Data: uses, opportunities and risks

ASIA AND THE PACIFIC

Regional Innovation Centre

public digital

This presentation has been designed using resources from Flaticon.com and Unsplash.com.