New Technology and Protection of Personal Data

Leena van der Made

2021-01-28

ESA HQ, Paris

Overview

- **Data protection - ESA**
  - ESA activities: medical research; AI; technology; space, …
- **Personal data: why does it matter?**
- **New technologies, processing and risk**
- **What can we influence?**
- **Data Protection as an opportunity for innovation of technology + society**
- **Key principles as tools for change**
- Questions

ESA Protection of Personal Data Framework

The European Space Agency (ESA) is Europe's mission is to shape the development of Europe's space capability and ensure that investment in space continues to deliver benefits to the citizens of Europe and the world. ESA promotes for peaceful purposes, cooperation among European States in space research and technology and their space applications, with a view to their being used for scientific purposes and for operational space applications systems

The European Space Agency is subject to a Personal Data Protection framework composed of the following elements:

- The Principles of Personal Data Protection, as adopted by ESA Council Resolution (ESA/C/CCLXVIII/Res.2 (Final)) adopted on 13 June 2017
- The Rules of Procedure for the Data Protection Supervisory Authority, as adopted by ESA Council Resolution (ESA/C/CCLXVIII/Res.2 (Final)) adopted on 13 June 2017
- The Policy on Personal Data Protection adopted by Director General of ESA on 5 February 2018 (ADMIN/IPOL-LEGI(2018)01) and **effective since 1 March 2018**

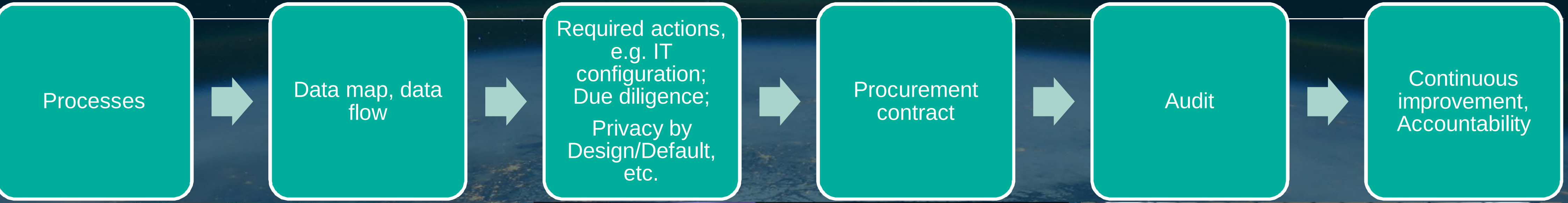
ESA PDP Framework is publicly available at:

http://www.esa.int/About_Us/Law_at_ESA/Highlights_of_ESA_rules_and_regulations

Governance

- Independent Supervisory Authority
- Data Protection Officer
- Data Protection Committee

ESA Protection of Personal Data Implementation



Processes

Data map, data flow

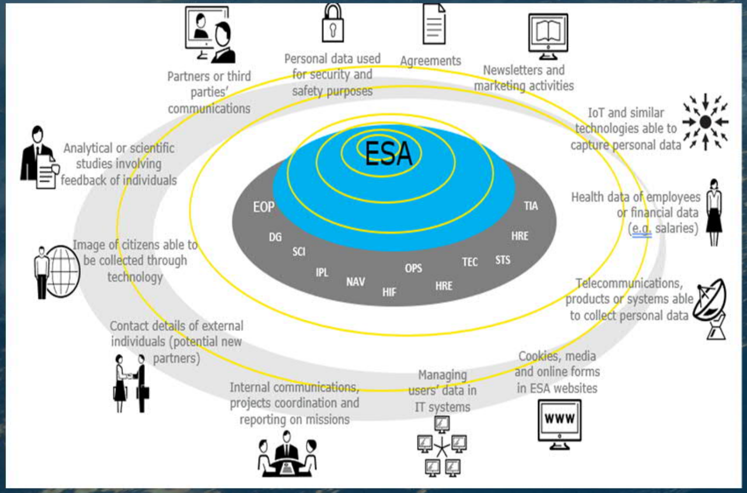
Required actions, e.g. IT configuration; Due diligence;

Privacy by Design/Default, etc.

Procurement contract

Audit

Continuous improvement, Accountability


Partners or third parties' communications
Personal data used for security and safety purposes
Agreements
Newsletters and marketing activities
IoT and similar technologies able to capture personal data
Analytical or scientific studies involving feedback of individuals
ESA
EOP
DG
SCI
IPL
NAV
HIF
OPS
HRE
TEC
STS
HRE
TIA
Health data of employees or financial data (e.g. salaries)
Image of citizens able to be collected through technology
Telecommunications, products or systems able to collect personal data
Contact details of external individuals (potential new partners)
Cookies, media and online forms in ESA websites
Internal communications, projects coordination and reporting on missions
Managing users' data in IT systems
www

Personal data: system logs, medical research data; physical image, location data, contact details, …

Why does it matter?

Personal data protection is:

- key to **European** ethics
- a fundamental human right based in the EU Charter of Fundamental Rights
- key to human dignity, value, respect and autonomy

Ongoing scandals on the misuse of personal data:

- collected without informing individuals or sold and combined with other personal data
- the loss of control raises concerns. A loss of trust damages business.
- Personal data drives business and income: further exploitation of the individual. New technologies are likely to result in a high risk for individuals if not **governed**

Is this what we want?

What can I do about it?

Technology should benefit and serve mankind

New Technologies: smart tools, AI and Blockchain, IoT, 5 G, analytics, …

Crew Interactive MObile Companion 2 (CIMON)

CIMON travels with astronauts on the International Space Station (ISS)

Features:

- A tone analyser to detect emotions during conversation: excited, frustrated, impolite, polite, sad, satisfied, sympathetic, incl. machine learning
- Voice controlled, explains information, lab assistant to experiments
- Performs video documentation
- Formal work personality and casual conversation mode
- Autonomous and flies throughout the ISS
- AI powered
- Aims to reduce stress by helping, e.g. isolation during Covid or space flights
- Understands context, content and intent behind questions

Inbuilt privacy controls: astronauts control the tone analyser

- CIMONs eyes are closed and it sleeps when in offline mode
- Data belongs to the customer: the customer decides whether data is used to improve algorithms or not

Does the technology feed on personal data, serve us?

Cloud solutions

Social media networks

Fingerprint recognition

Wi-Fi/Bluetooth/RFID tracking

wearables

Machine learning and deep learning

Smart technologies

smartphones

IoT applications

hardware/software monitoring

Online tracking by third parties

Data aggregation/data aggregation platforms, re-use of publically available data

Tracking: data processing at the: workplace, home, remote working, processing

Few and powerful market players

Could imply:
less competition,
less service quality,
less innovation,
less protection,
excessive collection,
exploitation,
loss of benefits +
trust,
invasive surveillance,
large scale detailed
profiles of individuals
shared/sold

High risk: innovative technology I

High risks may arise from:

- **Unknown personal/social consequences of new technology:**
- innovative use
- or new organisational solutions
- or new application of existing technologies or combined technologies

Sensitive data or data of very personal nature:

- **biometric data:**
- **facial recognition technology**
- **genetic data:** biomedical science services
- **political opinions** of individuals: or synthetic media
- **criminal convictions** or offences

- The **more personal data and increasing amount of people involved**, the higher the risk

High risk processing and technology (II)

- Processing operations aiming at preventing individuals from exercising a right / using a service contract
- Automated decision-making
- Artificial intelligence (AI) machine learning and deep learning
- Internet of things applications
- Connected and autonomous vehicles, intelligent transport systems
- Smart technologies (including wearables)
- Evaluation or scoring

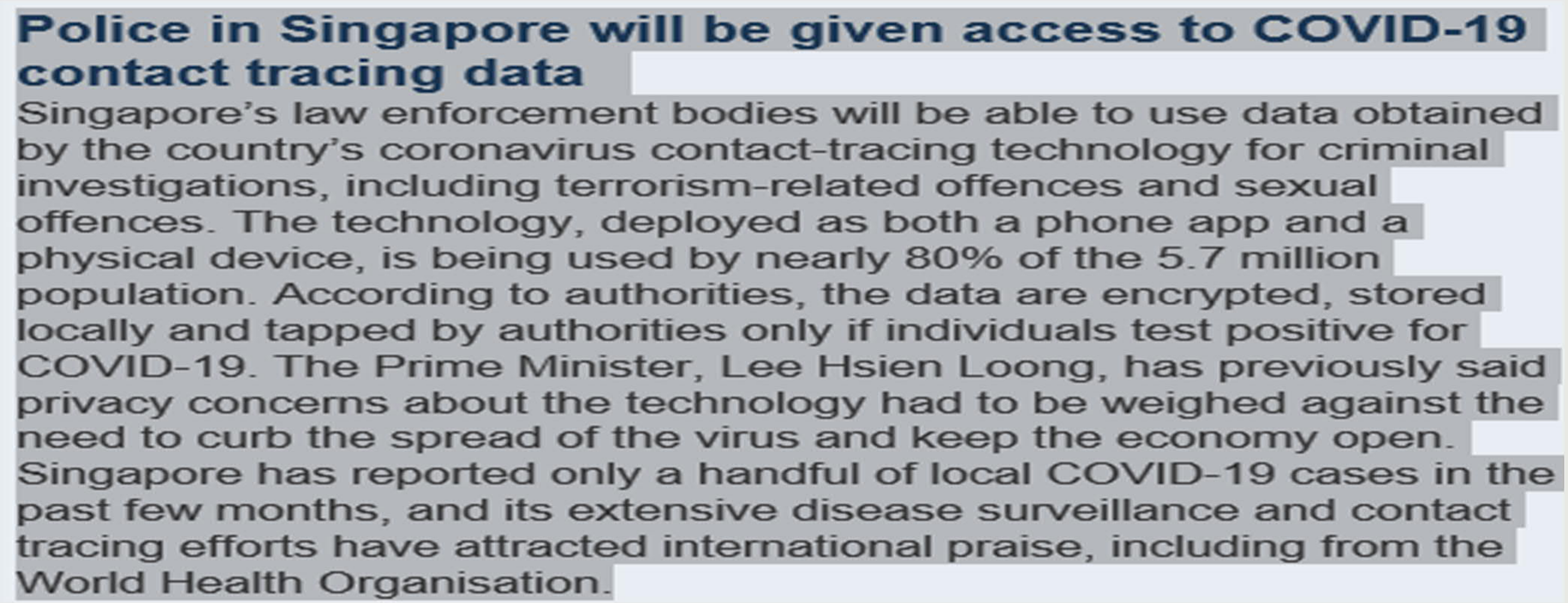
High risk processing and technology (III)

- **Data matching**
- **Processing on a large scale**
- **Invisible processing:** processing personal data not obtained directly from the individual
- **Tracking**
  - **BigData**
    - **A health insurance data company seeks a patent application for data scraping software to draw healthcare info from Facebook and Twitter**

High risk processing and technology (IV)

Systematic monitoring: personal data may be collected without individuals being aware of who is collecting their data and how it will be used, e.g. processing in public spaces, processing used to: observe, monitor, control data subjects, including data collected through networks

- **Would contact-tracing apps and bigdata, used to fight COVID-19, be used by governments for tracking individuals for other purposes?**
- **Contact-tracing apps and face-recognition camera data can reveal the individuals' location/s, type of transportation, purchases, interaction with social networks, attitudes, personal preferences, body temperatures (face recognition cameras in public spaces)**

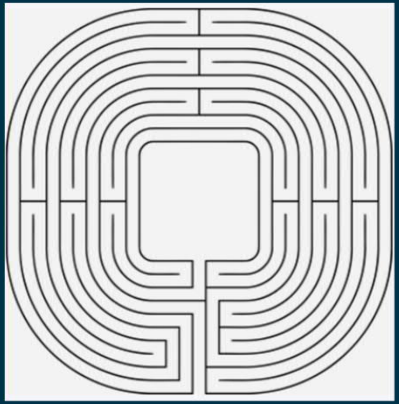


Police in Singapore will be given access to COVID-19 contact tracing data

Singapore's law enforcement bodies will be able to use data obtained by the country's coronavirus contact-tracing technology for criminal investigations, including terrorism-related offences and sexual offences. The technology, deployed as both a phone app and a physical device, is being used by nearly 80% of the 5.7 million population. According to authorities, the data are encrypted, stored locally and tapped by authorities only if individuals test positive for COVID-19. The Prime Minister, Lee Hsien Loong, has previously said privacy concerns about the technology had to be weighed against the need to curb the spread of the virus and keep the economy open. Singapore has reported only a handful of local COVID-19 cases in the past few months, and its extensive disease surveillance and contact tracing efforts have attracted international praise, including from the World Health Organisation.

What can we influence?

What is the benefit to society? Can we make a difference?



Legislation leads change: Schrems II

promote the beneficial for society
protect human rights
promote digital trust
Use technology for good

Data Protection as an *opportunity* for innovation: technology + society

Governance:

change

people

processes

technologies

Technology should benefit and serve mankind

Governance:

- Implant enforcement mechanisms: independent data protection authorities
- International agreements
- Set standards for harmonization, e.g. IGOs standards
- Due diligence: ensure technology and terms of service conform to data protection standards, determine the purposes and the means of the processing, issue instructions to the processor
- Implement data protection policies, keep records of processing activities, data map/flow
- Increase user control: offer means for users to understand make it easy to withdraw consent
- Protect: implement appropriate security measures, manage incidents, breaches. Risk based approach: identify threats to IT systems and assess whether security measures in place provide an adequate level of protection. Monitor systems in operation

➢ **Improve technology to improve service value, innovation, benefits to our lives**

➢ **Demand technology leaders to protect personal data and human rights, make it a contractual condition**

Key principles, tools for change

Proportionality of the data use: weigh advantages against risks created for data subjects. Are the advantages justified, also ethically?

Transparency: informed consent, protection, respect, build trust

Purpose Limitation: personal data shall not be used for further purposes that are incompatible with the original purpose (without a valid legal basis);

Lawfulness: legal basis and specific purpose limitation

Data Accuracy

Disclosure control

Data subjects' rights, human rights: consider: ethics, responsibility, transparency and accountability, data protection legislation

Protect personal data: prevent companies from exploiting data, reduce risk by data minimization and prevent threats to the individual, the organisation, the political structure. Risk mitigation (DPIA)

Accountability

Data minimization

Fairness: is your data use fair? Should providers pay individuals if their data is used? Can the data be used to violate your rights? Can the Internet remain an ungoverned space? Data protection demands "respect for the individual". Social media platforms use boosts the collection of personal data for commercial purposes, how to change the trend?

Ethics: use of personal data: how does the organisation's use of personal data reflect its public image, corporate social responsibility, level of compliance and trust?

Privacy by design: decentralized data storage, identification and authentication, encrypted communications , data minimization

Define how to support the use of new technologies so as to respect human rights, privacy, sustainability and corporate social responsibility.

Ask industry for compliant, secure and ethical technology: consider the impact on society

Questions?