FUJITSU

shaping tomorrow with you

Date : Wed 20th May 2020

What is PDPA & impact in summary?

Katsunori Azuma

JOC Project Support

Service Integration Group

Agenda

- What is Personal Data?
- Thailand's Personal Data Protection Act （PDPA）
- Business Impact
- Benefits
- What happen after the GDPR enforcement?
- Conclusion

What is Personal Data?

What is Personal Information?

EU – General Data Protection Regulation (GDPR)

Personal Data, or Personal Information (PI) – GDPR definition:

- any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular 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;

Reference: https://gdpr-info.eu/art-4-gdpr

TH – Personal Data Protection Act (PDPA) / พรบ. คุ้มครองข้อมูลส่วนบุคคล

"ข้อมูลส่วนบุคคล" หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

Reference: http://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0052.PDF

Example of personal data in PDPA

FUJITSU

- Name and surname;
- Home address;
- Email address such as name.surname@company.com;
- Identification card number; bank account number; social security number
- Location data (for example the location data function on a mobile phone);
- Internet Protocol (IP) address
- Cookie ID
- Biometric data
- Sensitive Data

Examples of data not considered personal data in PDPA

FUJITSU

- Company registration number;
- Email address such as info@company.com;
- Anonymous data
- Information of the deceased persons

Personal data risks

Social Engineering

Identity Theft

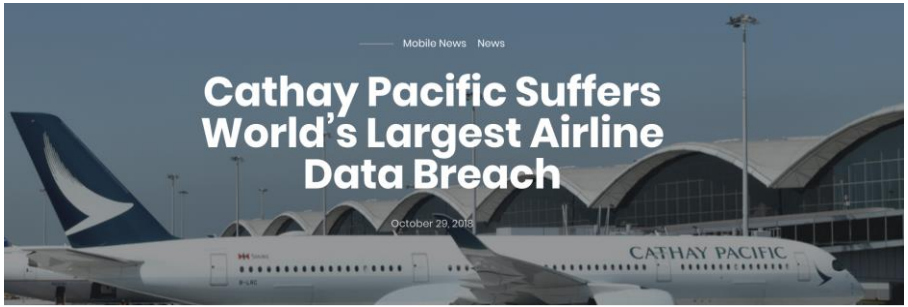
Tracking / Stalking

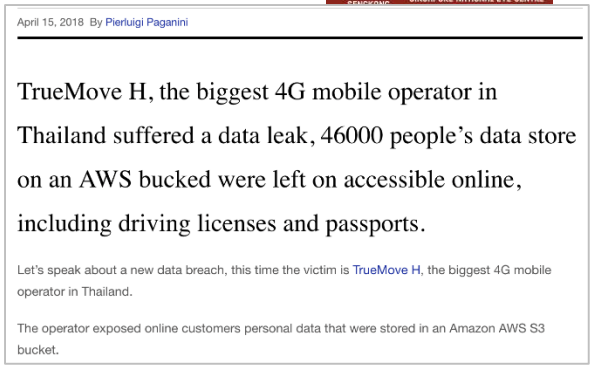
Misuse

RISK

Profiling

Data breach incidents





Data breach incidents

FUJITSU

Marriott to be fined nearly £100m over GDPR breach

ICO imposes fine after personal data of 339 million guests was stolen by hackers

£99.2m

BA faces £183m fine over passenger data breach

ICO says personal data of 500,000 customers was stolen from website and mobile app

£183m

Facebook to pay $5bn fine as regulator settles Cambridge Analytica complaint

Penalty by US government reflects scale of breach, first reported by the Observer

$5bn

Reference: https://www.theguardian.com

Thailand's Personal Data Protection Act (PDPA)

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

The gazette of PDPA

พระราชบัญญัติ
คุ้มครองข้อมูลส่วนบุคคล
พ.ศ. ๒๕๖๒

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ
พระวชิรเกล้าเจ้าอยู่หัว

ให้ไว้ ณ วันที่ ๒๔ พฤษภาคม พ.ศ. ๒๕๖๒
เป็นปีที่ ๔ ในรัชกาลปัจจุบัน

Reference: http://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0052.PDF

PDPA Summary

Personal Information

- Directly
- Indirectly

Including sensitive information

PDPA's Players

Data Subject

Data Controller & Data Processor

Committee

Applicability

Extraterritorial Applicability

Entities in and outside of Thailand

Legal Basis

Consent or
Other Legal Exceptions

Data Subject's Right

(30) Right to Access	(31) Right to data portability
(32) Right to object	(33) Right to be forgotten
(34) Right to restriction of processing	(35, 36) Right to rectification

Penalties

- Criminal
- Administrative
- Civil

500,000 – 5M Baht
and/or
Imprisonment

Imprisonment

มาตรา ๘๑ ในกรณีที่ผู้กระทาความผิดตามพระราชบัญญัตินี้เป็นนิติบุคคล ถ้าการกระทาความผิดของนิติบุคคลนั้นเกิดจากการสั่งการหรือการกระทาของกรรมการหรือผู้จัดการ หรือบุคคลใด ซึ่งรับผิดชอบในการดาเนินงานของนิติบุคคลนั้น หรือในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการหรือกระทาการและละเว้นไม่สั่งการหรือไม่กระทาการจนเป็นเหตุให้นิติบุคคลนั้นกระทาความผิด ผู้นั้นต้องรับโทษ ตามที่บัญญัติไว้สาหรับความผิดนั้น ๆ ด้วย

Section 81 In the case where the offender who commits the offense under this Act is a juristic person and the offense is conducted as a result of the instructions given by or the act of any director, manager or person, who shall be responsible for such act of the juristic person, or in the case where such person has a duty to instruct or perform any act, but omits to instruct or perform such act until the juristic person commits such offense, such person shall also be punished with the punishment as prescribed for such offense.

Reference: http://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0052.PDF

Data Controller & Data Processor Responsibilities

FUJITSU

Data Controller

- ✓ Provide appropriate security measures to prevent loss, access, use, change, correction or disclosure of personal data
- ✓ Provide an inspection system to detect personal data that has been kept for longer than necessary or is not relevant to the objective.
- ✓ Inform the Office of the Personal Data Protection Board of any violation of the personal data within 72 hours
- ✓ Prepare and maintain a list of the data processing activities
- ✓ Appoint data controller representative and Data Protection Officer (DPO)
- ✓ Respond to data owner's requests

Data Processor

- ✓ Strictly follow the instructions of the data controller
- ✓ Provide appropriate security measures to prevent loss, access, use, change, correction or disclosure of personal data
- ✓ Inform the data controller of any violation of the personal data that occurs.
- ✓ Prepare and maintain a list of the data processing activities

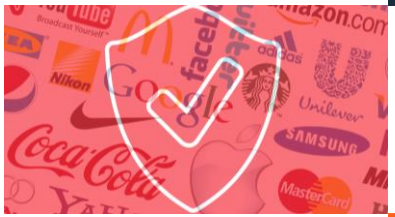
FUJITSU

Business Impact

Positive Impact (Example of the GDPR)

Improved Cybersecurity

Standardization of Data Security & Data Privacy



Brand Safety

Loyal Customer Following

Negative Impact (Example of the GDPR)

Non-Compliance Penalties

The Cost of Compliance

Overregulation Hampering Innovation

FUJITSU

Benefits

Personal (Example of the GDPR)

- Confident to use the products/services
- Reduce personal data violation and privacy infringement
- Have the rights of their own personal data
- File a complaint and Claim for damages

Business (Example of the GDPR)

- Customer Loyalty And Trust
- Better data security
- Reduced maintenance costs
- Better alignment with evolving technology
- Greater decision-making

FUJITSU

What happen after the GDPR enforcement?

What happen after the GDPR enforcement?

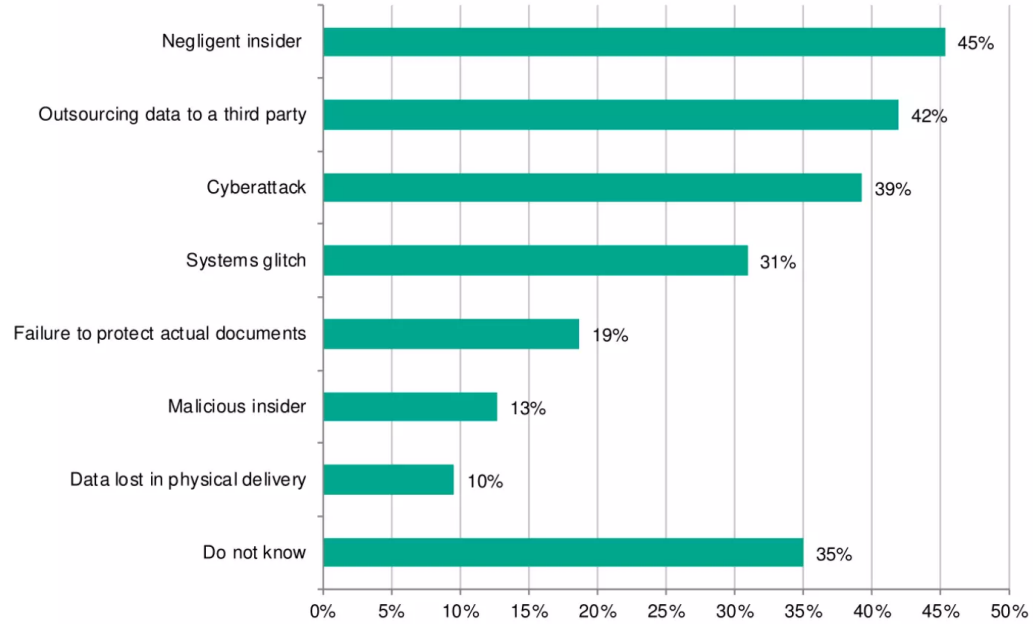
- 18 percent of respondents, said they had a high degree of confidence in their ability to communicate a data breach to the correct EU regulators within 72 hours of becoming aware of it.
- 54 percent – said GDPR implementation took longer than it expected
- 45 percent - said they had an average of two reportable data breaches since GDPR came into effect.

Reference: https://digitalguardian.com/blog/survey-gdpr-compliance-still-lagging

The biggest causes of the breaches

Figure 3. What were the root causes of these data breaches?

More than one response permitted



Reference: https://digitalguardian.com/blog/survey-gdpr-compliance-still-lagging

FUJITSU

Conclusion

Conclusion

- This law was issued to protect personal information both IT and non-IT.
- Any organization that ignores or does not comply with this law is likely to be punished by law.
- Every organization who collect, use, process transfer and disclose personal data need to comply with this law.

FUJITSU

shaping tomorrow with you

Date : Wed 27th May 2020

Step by step to go on track with PDPA's solution by Fujitsu

Katsunori Azuma

JOC Project Support

Service Integration Group

PDPA Summary

Personal Information

- Directly
- Indirectly

Including sensitive information

PDPA's Players

Data Subject

Data Controller & Data Processor

Committee

Applicability

Extraterritorial Applicability

Entities in and outside of Thailand

Legal Basis

Consent or
Other Legal Exceptions

Data Subject's Right

(30) Right to Access	(31) Right to data portability
(32) Right to object	(33) Right to be forgotten
(34) Right to restriction of processing	(35, 36) Right to rectification

Penalties

- Criminal
- Administrative
- Civil

500,000 – 5M Baht
and/or
Imprisonment

10 Steps to Preparing for PDPA

Teaming up!

FUJITSU

In most organizations, enterprise architects & IT department do not have final responsibility for ensuring regulatory compliance.

This responsibility may lie with ...

- Legal department
- Risk Management
- Compliance
- Information Security
- Data Protection Officer
- HR, Marketing etc.

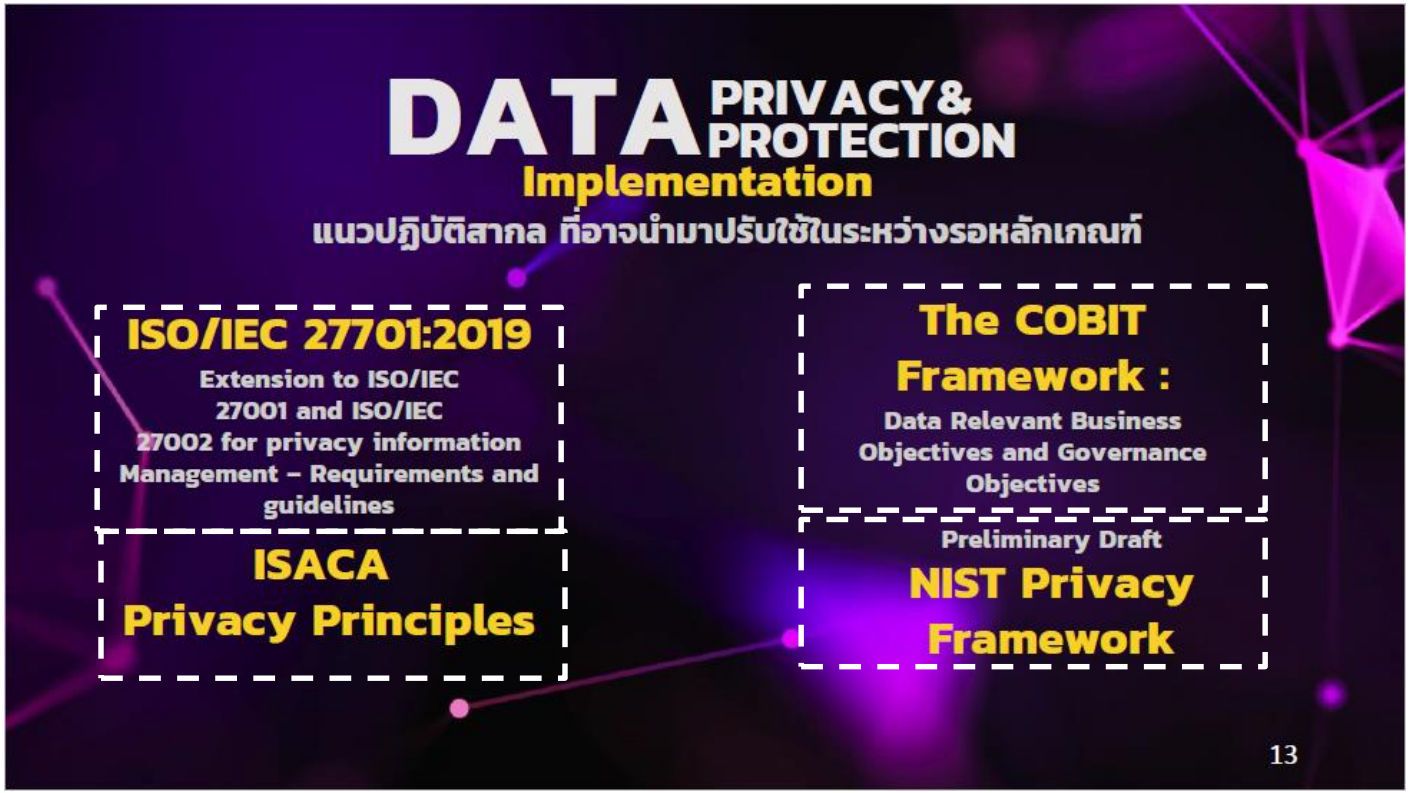
Reference: https://www.rsaconference.com/industry-topics/webcast/7-gdpr-without-the-hype

1. Create governance framework

Step 1

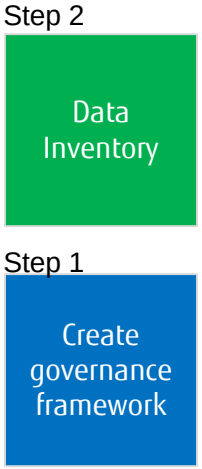
Create governance framework

Reference:
Data Privacy & Protection Implementation Guideline



https://www.etda.or.th/content/personal-data-protection-by-etda

2. Data inventory



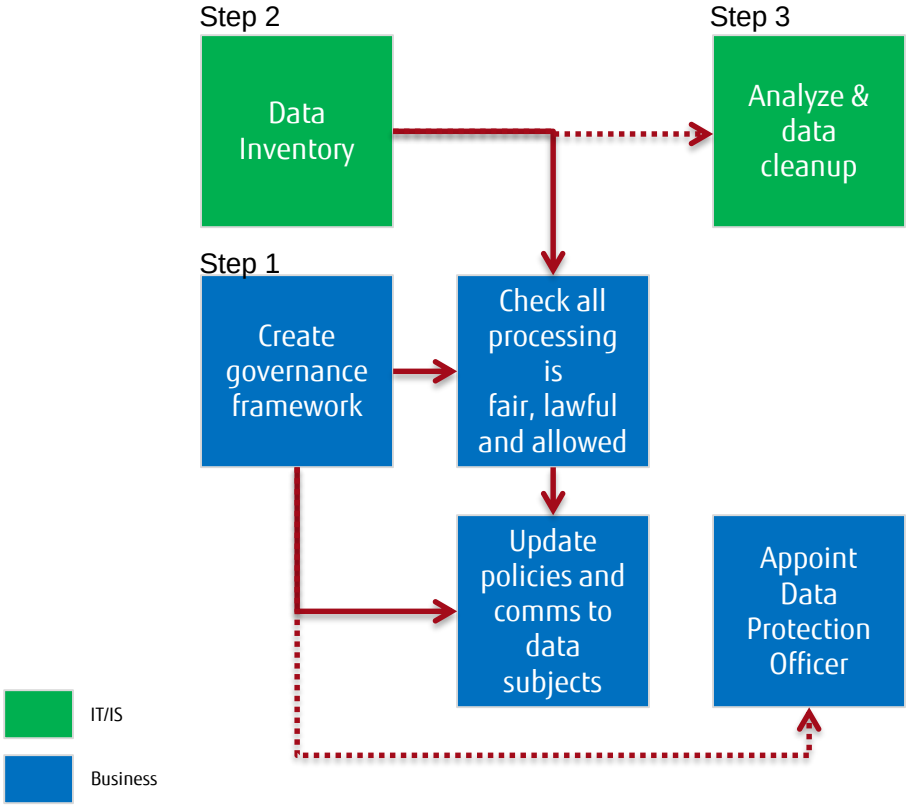
IT/IS

Business

2. Data inventory

- Identify all data that counts as ‘personal’ according to the PDPA.
- Data Discovery: Logical and physical
- What do you store:
  - How old is it
  - How much is there
- Classification
- What third parties?

3. Analyze & data cleanup

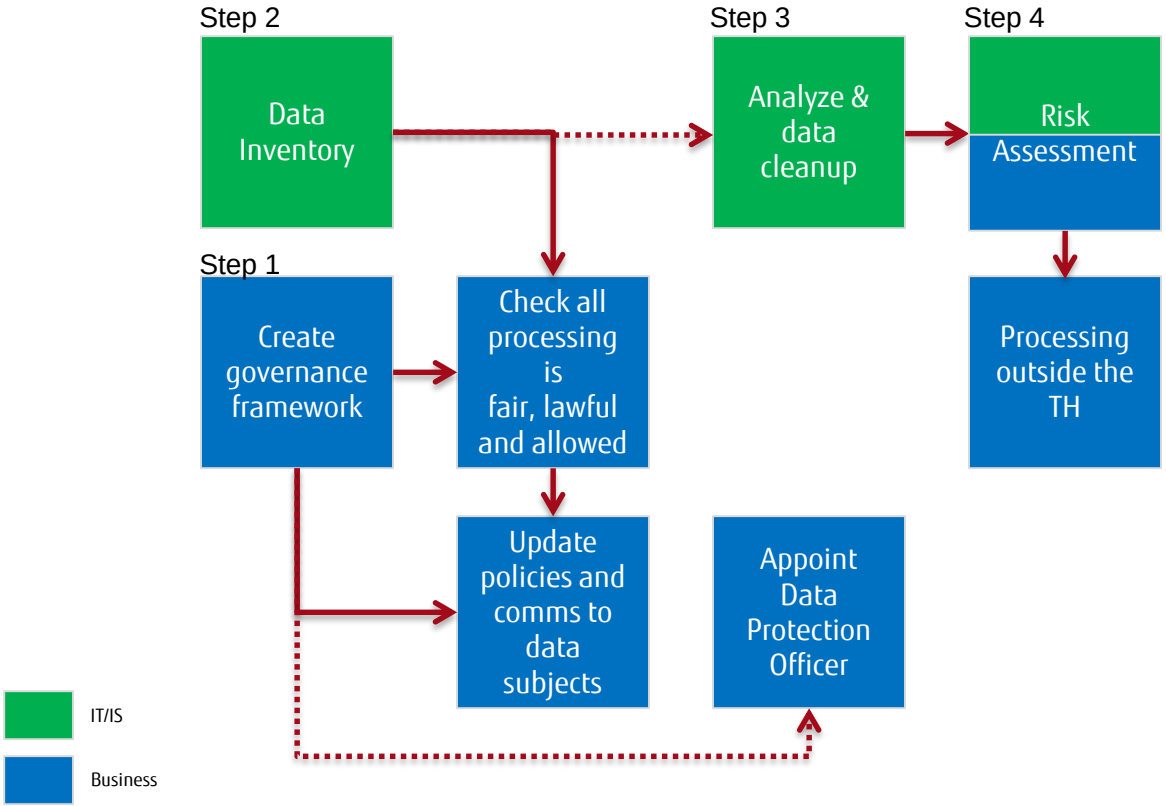


3. Analyze & data cleanup

FUJITSU

- Map data flows
- Be selective – work from high risk – low risk
- Delete all the data you don't need
  - Duplicate copies
  - "Just-in-case" backups
  - Excess fields in systems
  - Records the business has decided is no longer required

4. Risk Assessment



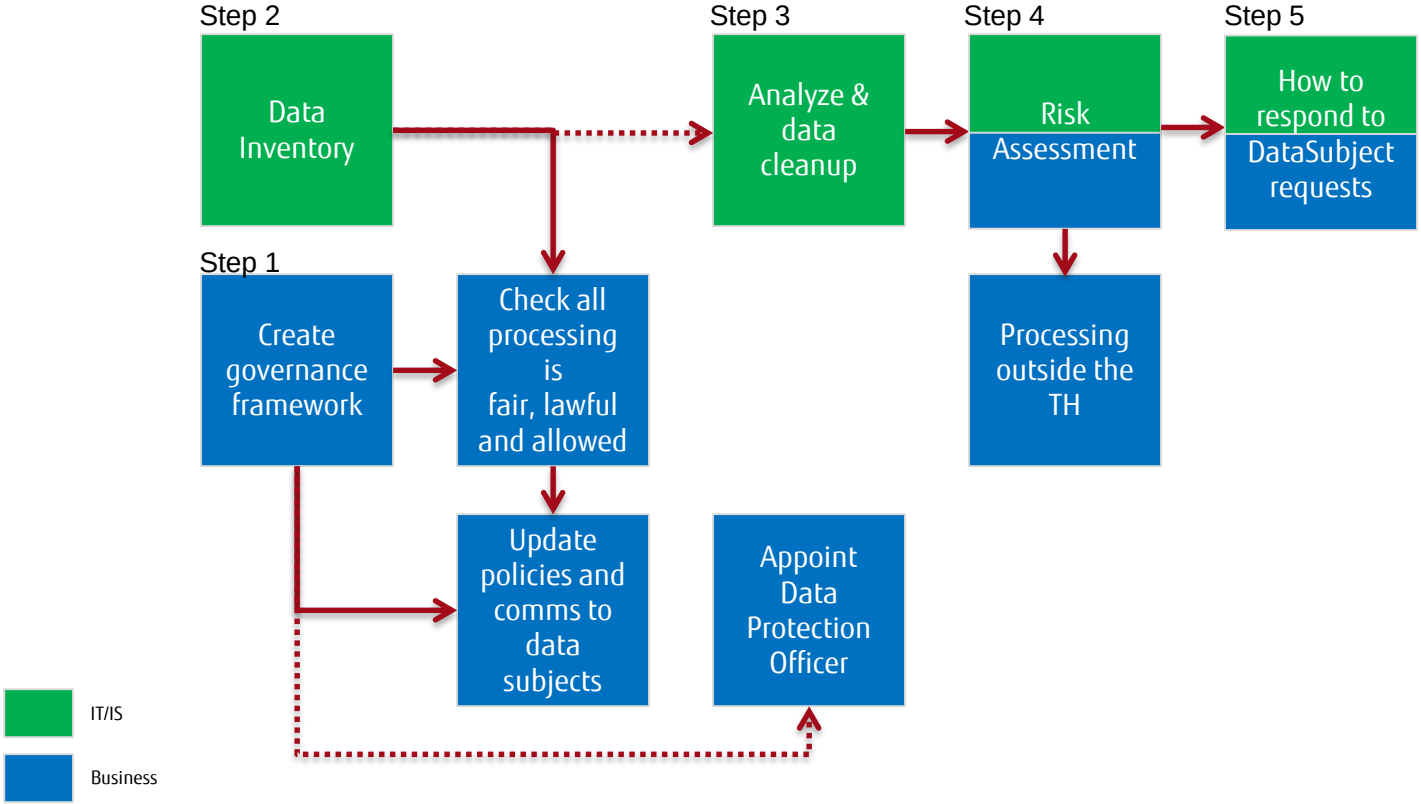
4. Risk Assessment

- Privacy risk assessment
- Conduct security risk assessment
  - Effects of breach of CIA and R on data subject rights

    C : Confidentiality I : Integrity A : Availability + R : Reliability

- Third party risks

5. Understand technically how to respond to ...



5. Understand technically how to respond to ...

FUJITSU

... Right to Access

(Article 30)

... Right to data portability

(Article 31)

... Right to object

(Article 32)

... Right to be forgotten

(Article 33)

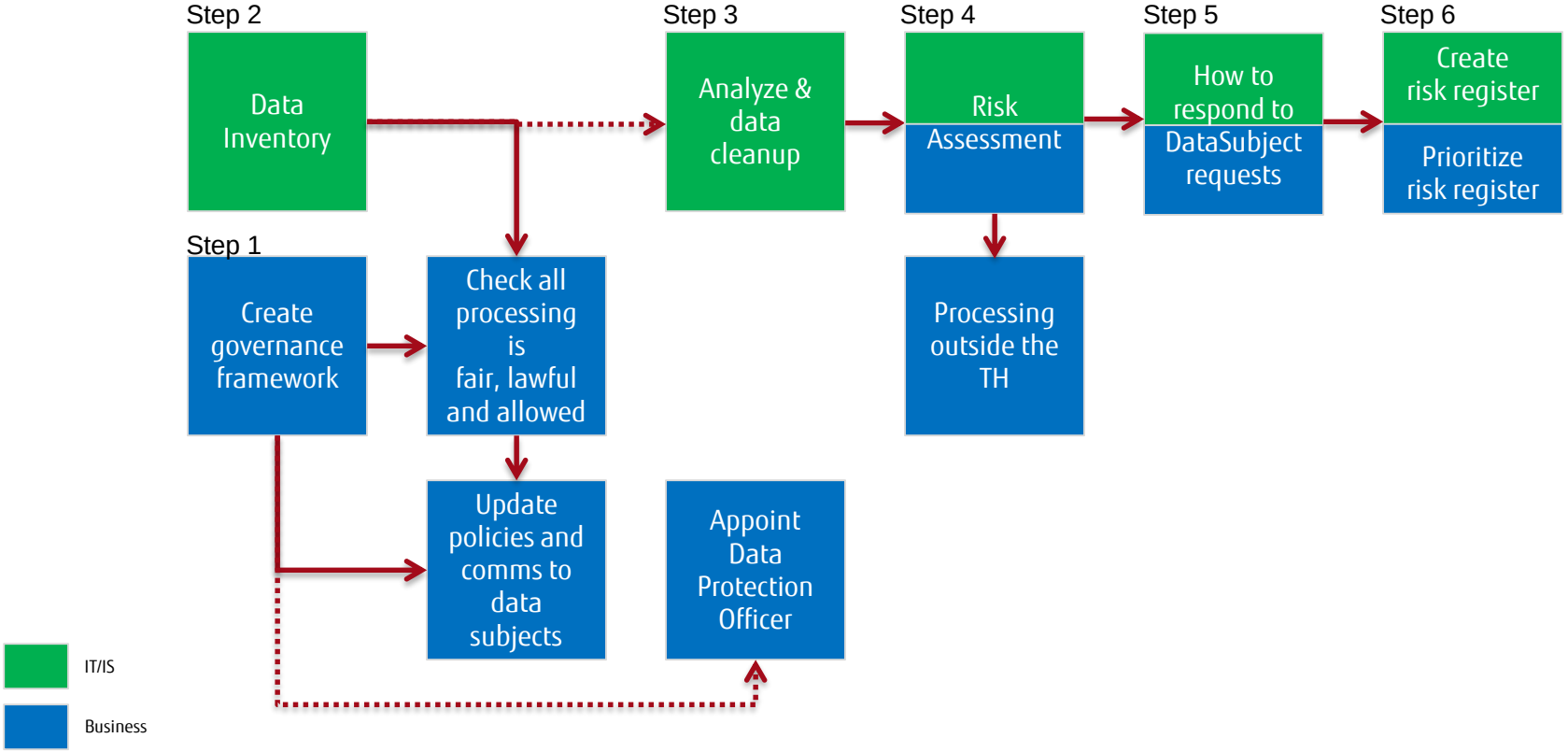
... Right to restriction of processing

(Article 34)

... Right to rectification

(Article 35, 36)

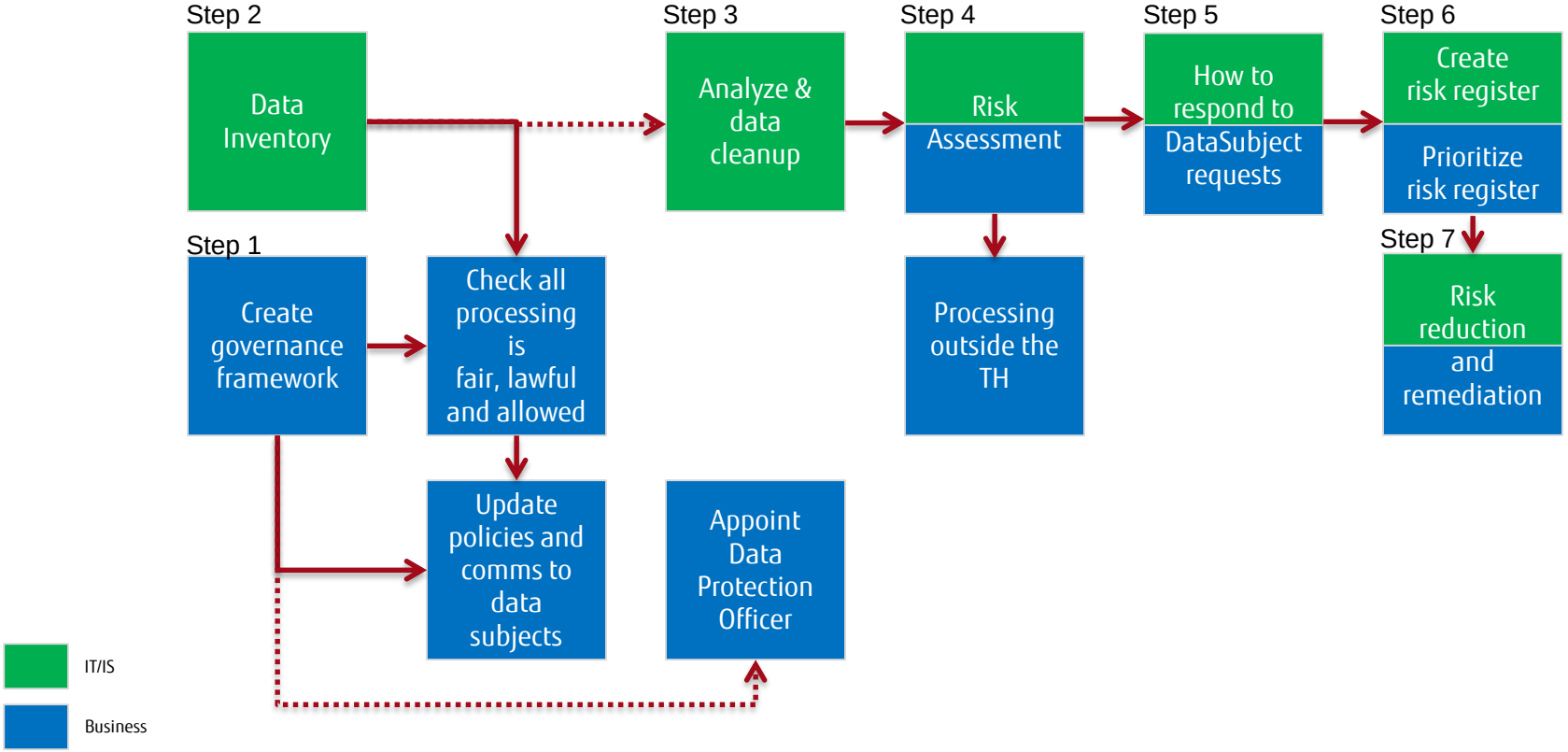
6. Prioritize risks



6. Prioritize risks

- List risks to Data Subjects
  - Prioritized
- List regulatory risks
  - Prioritized

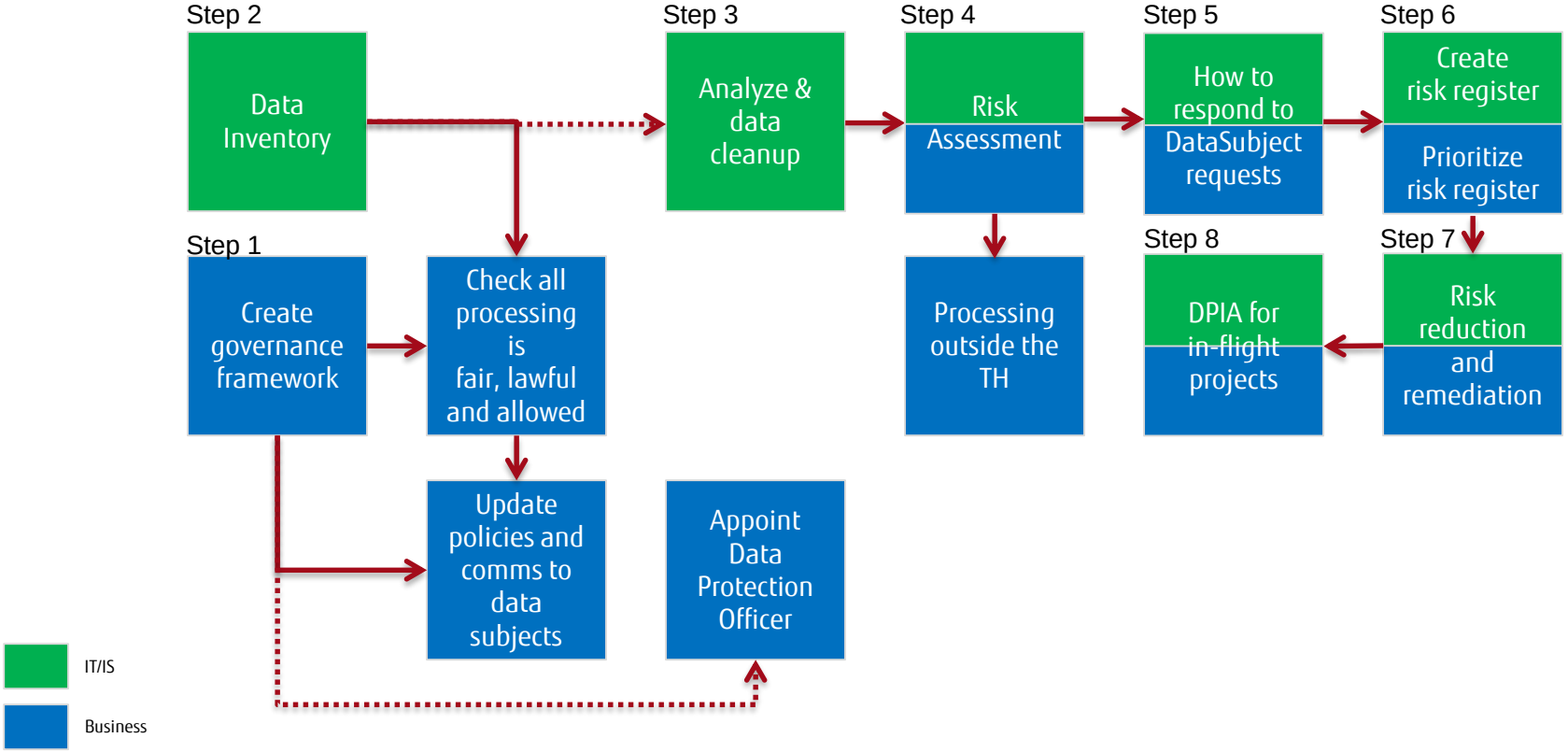
7. Risk reduction and remediation



7. Risk reduction and remediation

- Do we need to do this with that data?
- Confidentiality
  - Pseudonymization
  - Encryption
- Access control – does everyone need access?
- What security posture based on data subject risk
  - Will you create different security zones?

8. DPIA for in-flight projects

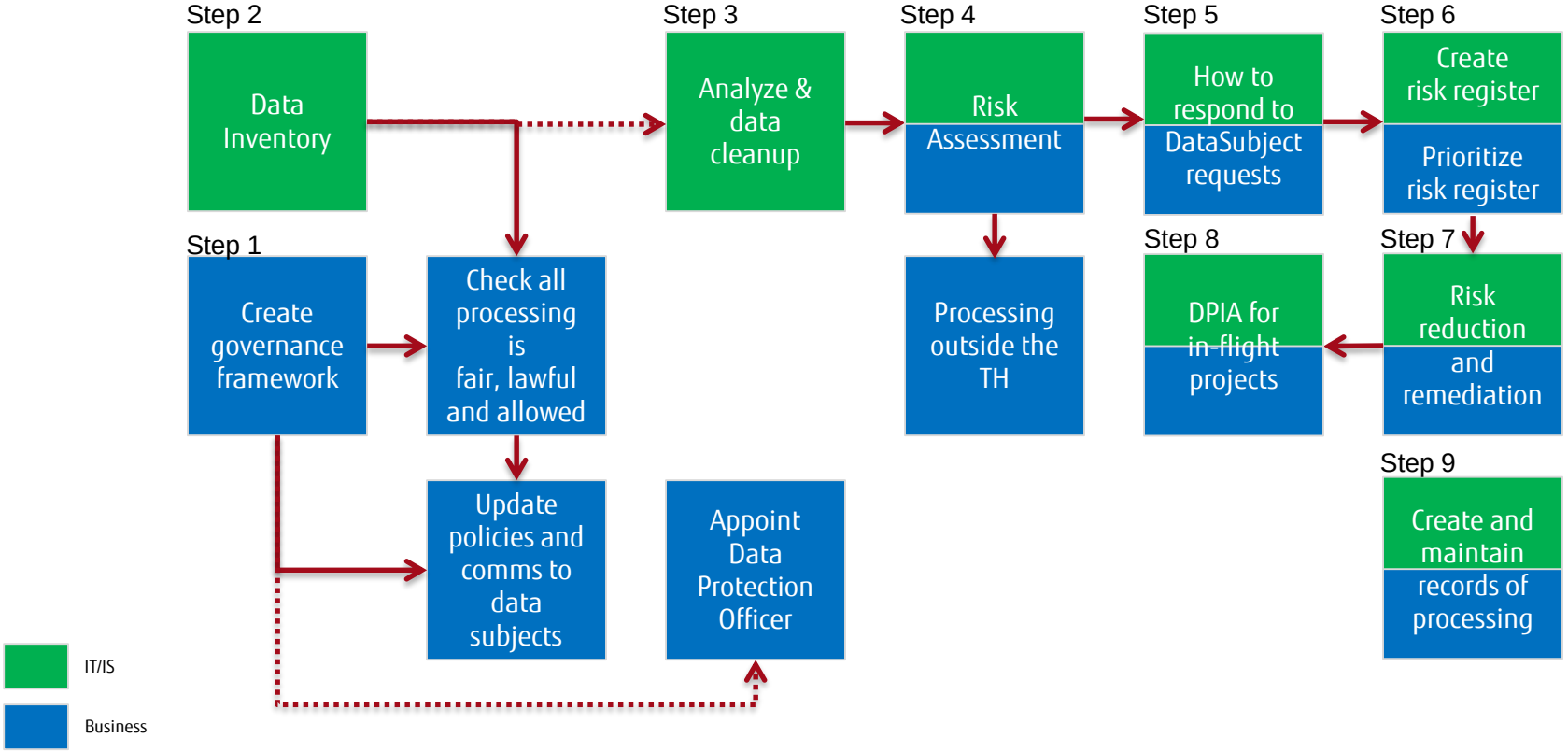


8. DPIA for in-flight projects

FUJITSU

- DPIAs required for ‘high risk’ processing and in specified circumstances
- Needs to contain:
  - Systematic description and basis of processing
  - Assessment of necessity and proportionality
  - Risks to Data Subjects
  - Risk reduction

9. Records of processing

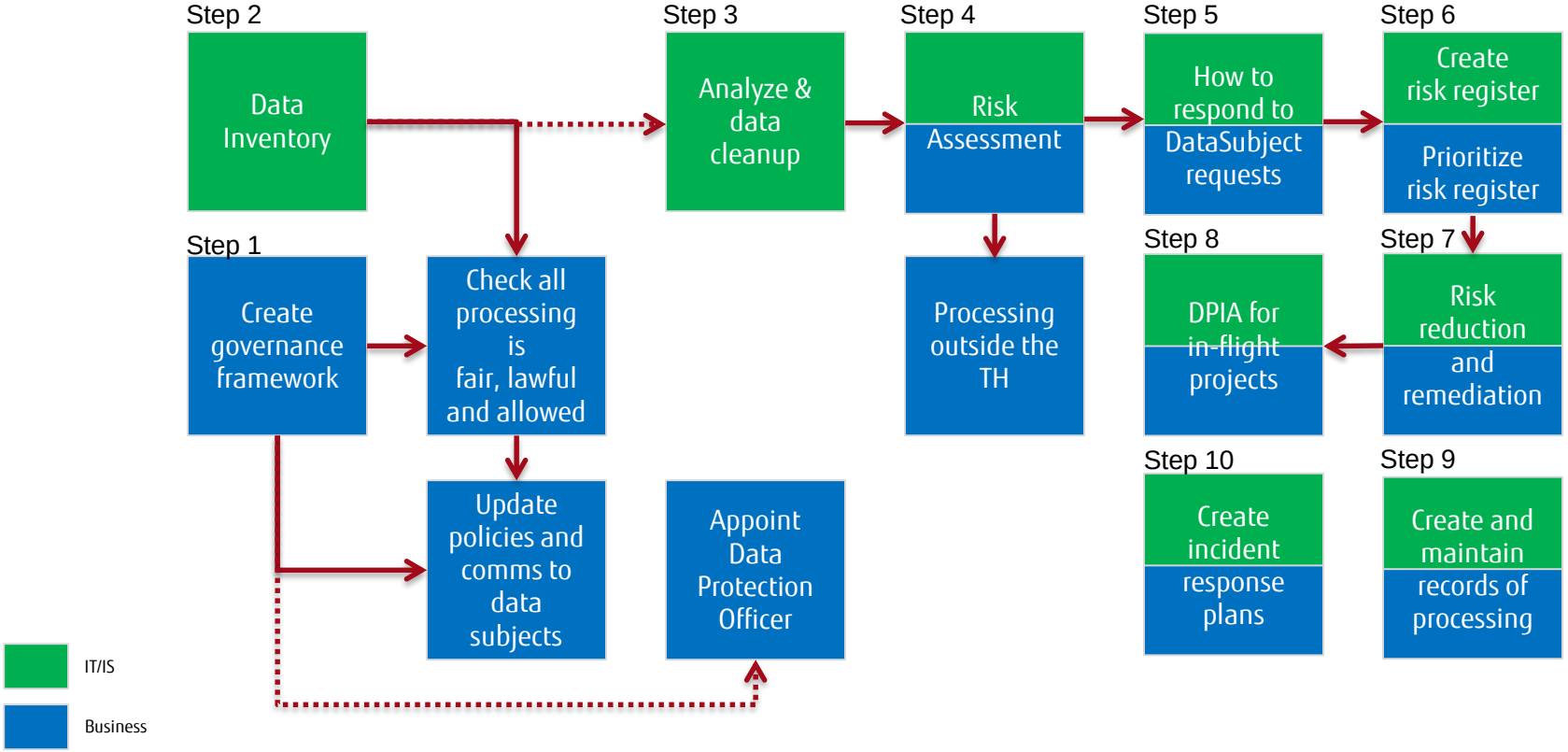


9. Records of processing

FUJITSU

- Essential for accountability principle (Article 39)
  - the collected Personal Data
  - the purpose of the collection of the Personal Data in each category
  - details of the Data Controller
  - the retention period of the Personal Data
  - rights and methods for access to the Personal Data
  - the use or disclosure
  - the rejection of request or objection
  - explanation of the appropriate security measures

10. Incident response



10. Incident response

What's a personal data breach?

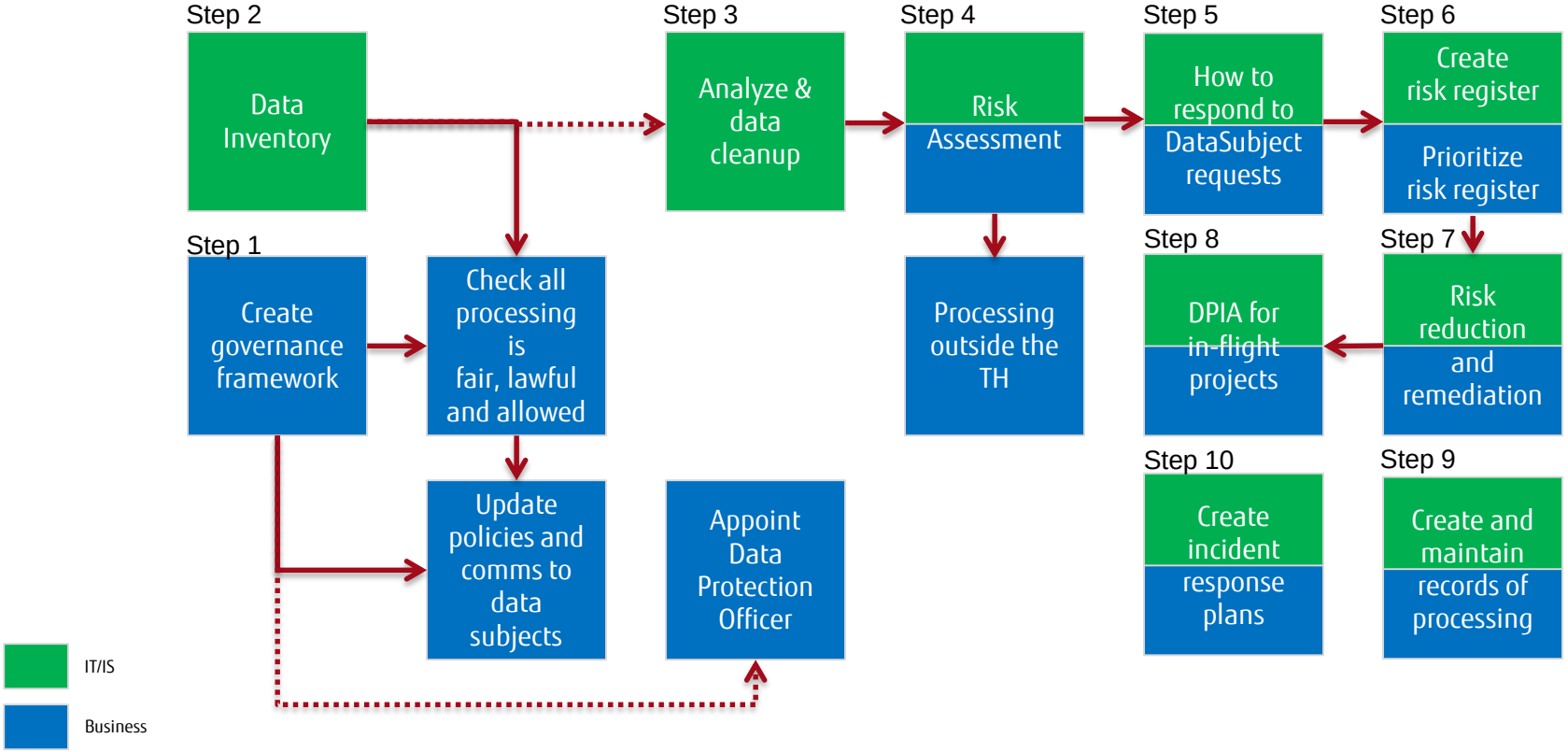
'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;

10. Incident response (Article 37 (4))

FUJITSU

- Notification of a breach to supervisory authority within 72 hours
- Notification to Data Subject
- Plan, test the plan
- Make sure legal are involved (because they will want to handle the notification)

Summary

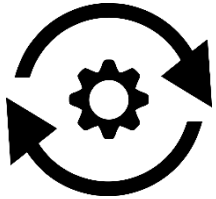


How Fujitsu Thailand can help you?

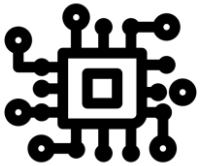
How Fujitsu Thailand can help you?

People

Policy



Processes



Technology

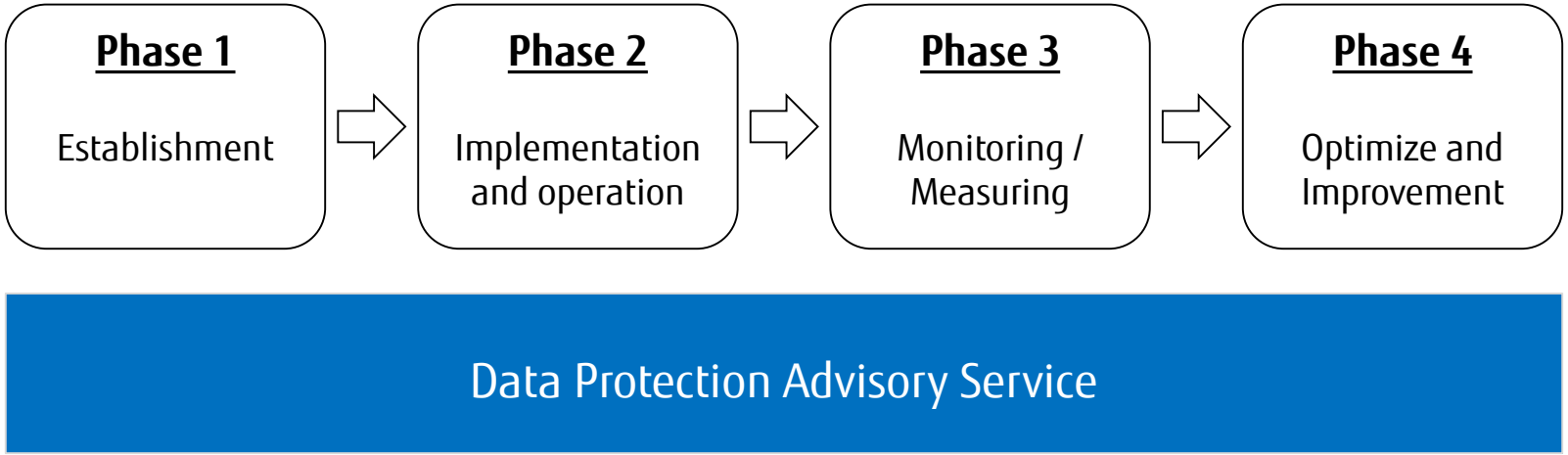
Data Protection Advisory Service

Privacy & Cybersecurity Solutions

IT/IS

Business

Consulting Service



Data Protection Advisory Service

FUJITSU

Phase 1

Establishment

- ✓ Top Management commitment
- ✓ Appoint Data Privacy committee
- ✓ Appoint Data Privacy Officer (DPO)
- ✓ Consist Manager, Working group
- ✓ Establish Data Privacy Policy and The Objective Define framework for protecting PII
- ✓ Increase employee awareness by training and communication scheme

Data Protection Advisory Service

FUJITSU

Phase 2

Implementation and operation

- ✓ Collect consent, implement single contact point for supporting "Individual Right" management
- ✓ PII Inventory
- ✓ Perform DPIA Risk Assessment / Treatment
- ✓ Define procedure / work instruction / standard process as risk level
- ✓ Monitoring and evaluate the result of risk treatment plan
- ✓ Make sure report major incident (with Resolution plan) to DPA in 72 Hrs.

Data Protection Advisory Service

FUJITSU

Phase 3

Monitoring / Measuring

- ✓ Process audit / Internal audit
- ✓ Check an Update regulation of DPA Thailand
- ✓ Cyber security assessment (VA, Penetration test)
- ✓ Regularly report the level of compliance to top management

Data Protection Advisory Service

FUJITSU

Phase 4

Optimize and Improvement

- ✓ Tuning standard process for fully compliance
- ✓ Improve process by IT and Cyber Security enhancement
- ✓ Looking for International Standard such as ISO 27001 for systematic approach framework

IT solutions supported Fujitsu

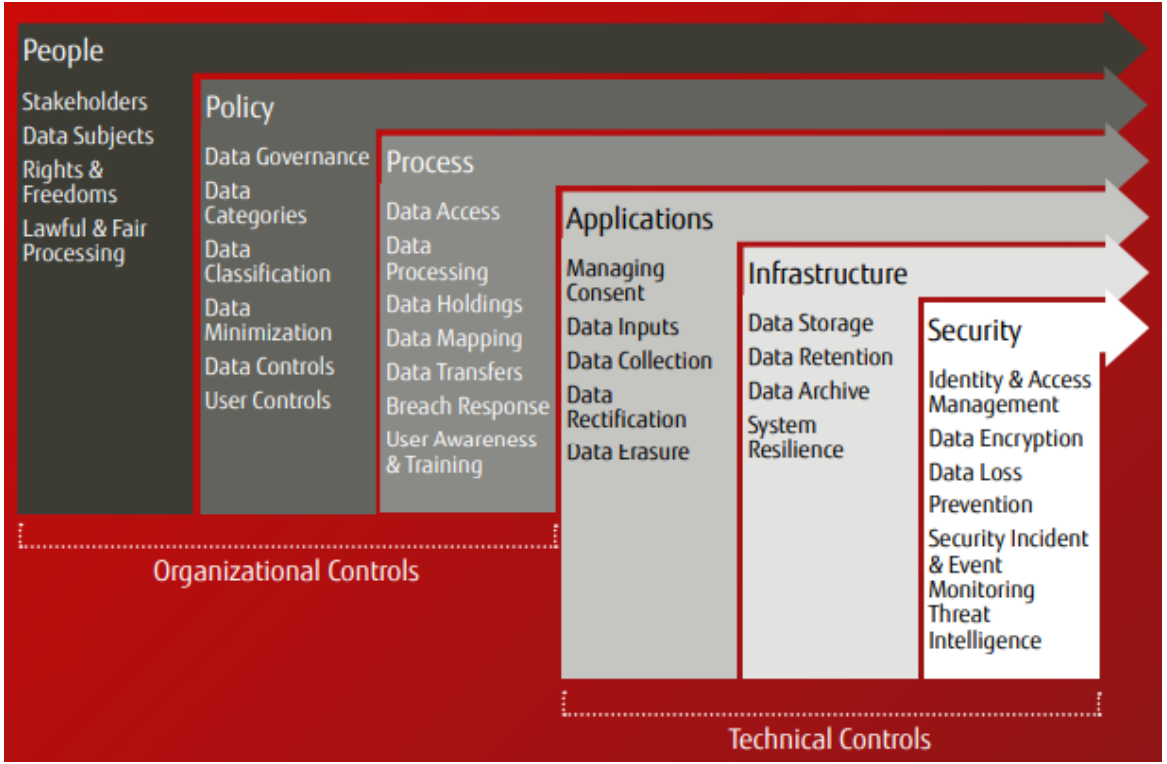
Solution		PDPA
Data Protection	Provides solutions to protect data from various risks such as failures, disasters, and cyber attacks.	PDPA article 37 [1] article 40 [2]
Access Control	Control that only authorized people can use it. In addition, security at the time of authentication is enhanced to prevent impersonation of.	
Monitoring Data	Provides integrity monitoring of file and database data content. Check for unauthorized changes.	
Incident Response	Monitor event and log data to quickly detect when a security incident occurs.Necessary log data can be collected, investigated and analyzed.	PDPA article37 [4]
Log Management	Establish security controls to prevent, detect, and respond to vulnerabilities and data breaches	PDPA article 39 article 40 [3]

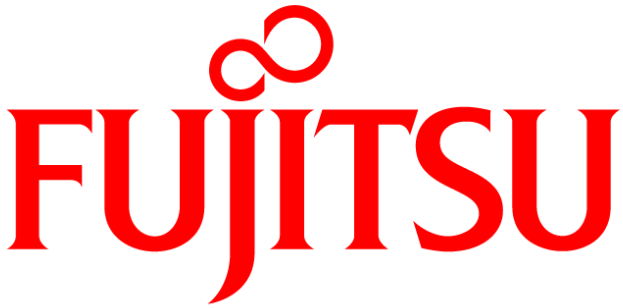
IT solutions supported Fujitsu (2)

Solution	
Data Protection	- Data Loss Prevention or Data Leakage Prevention (Endpoint Security) - Data Encryption - Backup & Recovery
Access Control	- Next Generation Firewall , Network Access Control - SSL VPN - Multi-Factor Authentication
Monitoring Data	- File Integrity Monitoring
Incident Response	- Security Information and Event Management (SIEM) - Endpoint Detection and Response (EDR)
Log Management	

How Fujitsu Thailand can help you?

People, policy and processes and technology that deliver 'privacy by nature'





shaping tomorrow with you