



Centre for
Information
Policy
Leadership
Hunton Andrews Kurth LLP



PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

Centre for Information Policy Leadership Workshop
in collaboration with the Singapore Personal Data Protection Commission

Implementing Accountability

26 July 2018, Singapore

- ❖ 8:30 Registration
- ❖ 9:00 **Introduction and the Importance of Organisational Accountability**
- ❖ 9:10 **Session I: Elements of Accountability — Data Protection Officer, Documentation, Demonstration**
- ❖ 10:40 Break
- ❖ 11:00 **Session II: Transparency, Legal Bases for Processing (Consent, Notification of Purpose and Legitimate Interest) & Data Protection Impact Assessments**
- ❖ 12:30 Lunch
- ❖ 13:30 **Session III: Data Protection by Design and Data Protection Impact Assessment Case Study**
- ❖ 15:05 Break
- ❖ 15:35 **Session IV: Regulator Perspectives on Accountability and How to Incentivise It**
- ❖ 17:20 End of Workshop



Centre for
Information
Policy
Leadership
Hunton Andrews Kurth LLP



PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

Introduction and the Importance of Organisational Accountability

Zee Kin Yeong, Deputy Commissioner, Singapore PDPC

Bojana Bellamy, President, CIPL

BRIDGING REGIONS
BRIDGING INDUSTRY & REGULATORS
BRIDGING PRIVACY AND DATA DRIVEN INNOVATION

ACTIVE GLOBAL REACH

60+
Member
Companies

We **INFORM** through
publications and events

We **NETWORK** with global
industry and government leaders

5+
Active
Projects &
Initiatives

We **SHAPE** privacy policy,
law and practice

We **CREATE** and
implement best practices

20+
Events
annually

ABOUT US

- The Centre for Information Policy Leadership (CIPL) is a global privacy and security think tank
- Based in Washington, DC, Brussels and London
- Founded in 2001 by leading companies and Hunton Andrews Kurth LLP
- CIPL works with industry leaders, regulatory authorities and policy makers to develop global solutions and best practices for data privacy and responsible use of data to enable the modern information age



Twitter.com/the_cipl



<https://www.linkedin.com/company/centre-for-information-policy-leadership>



www.informationpolicycentre.com



2200 Pennsylvania Ave NW
Washington, DC 20037

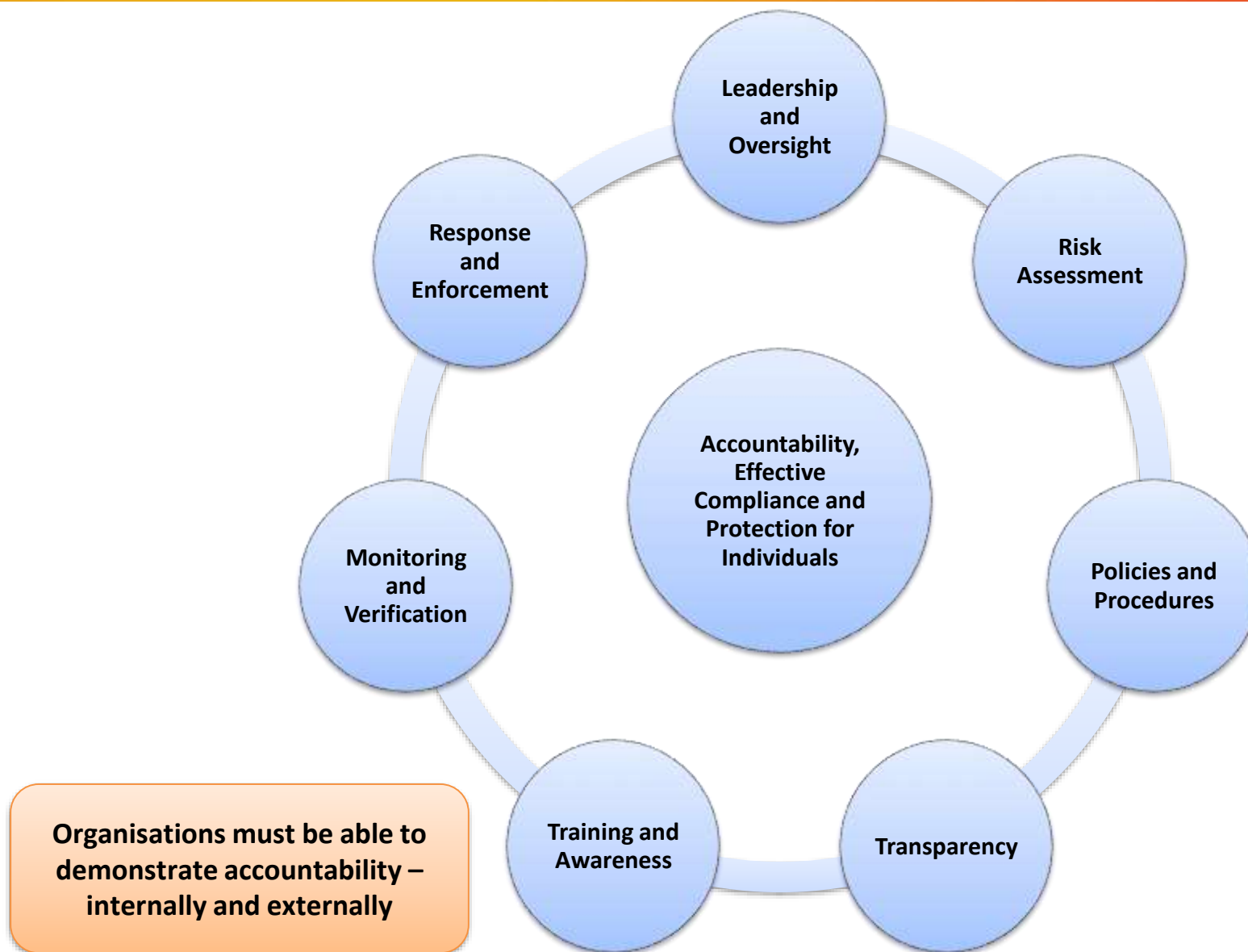


Park Atrium, Rue des Colonies 11
1000 Brussels, Belgium



30 St Mary Axe
London EC3A 8EP

Universal Elements of Accountability



Accountability – Examples of Content of Privacy Management Programmes

- Executive oversight
- Data privacy officer/office of oversight and reporting
- Data privacy governance
- Privacy engineers

Leadership & Oversight



- At program level
- At product or service level
- DPIA for high risk processing
- Risk to organisations
- Risk to individuals

Risk Assessment



- Internal privacy rules based on DP principles
- Information security
- Legal basis and fair processing
- Vendor/processor management
- Procedures for response to individual rights
- Other (e.g. Marketing rules, HR rules, M&A due diligence)
- Data transfers mechanisms
- Privacy by design
- Templates and tools for PIA
- Crisis management and incident response

Policies & Procedures



- Privacy policies and notices to individuals
- Innovative transparency – dashboards, integrated in products/apps, articulate value exchange and benefits, part of customer relationship
- Access to information portals
- Notification of data breaches

Transparency



- Mandatory corporate training
- Ad hoc and functional training
- Awareness raising campaigns and communication strategy

Training & Communication



- Documentation and evidence - consent, legitimate interest and other legal bases, notices, PIA, processing agreements, breach response
- Compliance monitoring as appropriate, such as verification, self-assessments and audits
- Seals and certifications

Monitoring & Verification



- Individual requests and complaints-handling
- Breach reporting, response and rectification procedures
- Managing breach notifications to individuals and regulators
- Implementing response plans to address audit reports
- Internal enforcement of non-compliance subject to local laws
- Engagement/Co-operation with DPAs

Response and Enforcement



Organisations must be able to demonstrate - internally and externally

Accountability – Self-Enlightened Interest of Organisations

**Proactive data management is a business issue;
accountability > legal compliance**

Enable new business models, digitalisation,
globalisation and data-driven innovation

Address increased expectations of individuals
for transparency, control and value exchange

Ensure data protection, sustainability and
digital trust

Address regulatory change, impact and
implementation

Mitigate legal, commercial and reputational
risks

Accountability – Benefits for DPAs and Individuals

DPAs

Reduces enforcement and oversight burden of DPAs

Promotes constructive engagement with accountable organisations

Enables leverage of peer pressure and “herd” mentality

Individuals

Effective protection and reduced risk/harm

Empowered, able to exercise rights and complaints

Trusting and ready to benefit and participate in digital society

How Can DPAs and Policymakers Incentivise Accountability

**A differentiating or
mitigating factor in
investigation or
enforcement**

**“Licence to operate” and
use data responsibly, based
on organisations' evidenced
commitment to data privacy**

**Publicly recognising best in
class organisations and
showcasing accountable
“best practices”**

**Supporting and guiding
organisations (particularly
small and emerging
companies) on a path
towards heightened
accountability**

**Co-funding between DPAs
and industry for research
into novel accountability
tools**

**Offer to play proactive
advisory role to
organisations seeking to
implement heightened
accountability**

**Using accountability as
evidence of due diligence in
business processes
(outsourcing, IT services etc)**

**Enable cross-border data
transfers within the
company group and to third
parties, based on formal
accountability schemes**

**Articulate proactively the
elements and levels of
accountability to be
expected**

New CIPL Papers on Accountability

The Central Role of Organisational Accountability in Data Protection

- **Paper 1 — The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society**
- **Paper 2 — Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability**

Available at informationpolicycentre.com



Centre for
Information
Policy
Leadership
Hunton Andrews Kurth LLP



PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

Session I

Elements of Accountability: Data Protection Officer, Documentation and Demonstration

- ❖ Hilary Wandall, General Counsel, Corporate Secretary and Chief Data Governance Officer, TrustArc
- ❖ Mark Jaffe, Senior Vice President Privacy and Data Protection for the Americas, Teleperformance
- ❖ Keith Enright, Legal Director, Privacy, Google
- ❖ Knut Mager, Head of Global Data Privacy, Novartis



Centre for
Information
Policy
Leadership
Hunton Andrews Kurth LLP



PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

Session II

Transparency, Legal Bases for Processing (Consent, Notification of Purpose and Legitimate Interest) and DPIA

- ❖ Alex Cebulsky, Senior Legal Counsel, Global Data Privacy, Accenture
- ❖ Derek Ho, Vice President, Senior Managing Counsel, Privacy and Data Protection, Mastercard
- ❖ Alison Howard, Assistant General Counsel, Microsoft
- ❖ Katherine Tassi, Deputy General Counsel, Privacy and Product, Snap

DATA PRIVACY



**ACCOUNTABILITY/
PRIVACY
ASSESSMENTS**

accenture

AGENDA

- Accountability
- Privacy Assessments

ACCOUNTABILITY

ACCENTURE'S BINDING CORPORATE RULES

What are BCRs

- ⑩ Under EU legislation, personal data cannot leave the EEA without being protected by adequate safeguards.
- ⑩ BCRs are a scheme designed by an organization to apply internally according to this organization's own specific security measures
- ⑩ It is vetted by a Data Protection Authority to validate such safeguards
- ⑩ The participating entities need to sign a binding InterCompany Agreement to enter the scheme and be recognized

Having BCRs means that:

- All our **group entities** which sign up to them must comply with the same internal set of rules – that there are appropriate and uniform data privacy safeguards in place across our organization
- **Individuals' rights** stay the same no matter where individuals' personal data are processed by Accenture
- **All Accenture entities and employees** bound by these BCRs, irrespective of geographic location, abide by the same rules for processing personal data as set out in the document



ACCENTURE BCRS:

- Explain Accenture's data privacy obligations and commitment
- Define Accenture employees' responsibilities and accountability for data privacy
- Describe individuals' rights under the BCRs
- Explain how Accenture handles complaints and/or queries
- Provide information on how to contact Accenture

ACCENTURE'S POLICY 90 AND DP STATEMENT

POLICY 90

- ⑩ Applicable to all the companies within Accenture
- ⑩ Sets the **minimum data privacy standard** across Accenture irrespective of geography
- ⑩ Sets out Accenture's **obligations and commitments** to comply with data privacy ethics and laws;
- ⑩ Defines **employees' responsibilities and accountability** for data privacy;
- ⑩ **Governs** how personal data will be managed;
- ⑩ Identifies **further resources** to help employees with this policy and local law requirements.




THE PURPOSE OF THE DATA PRIVACY STATEMENT:

The Global Data Privacy Statement ensures we meet the fair processing requirements within data privacy laws which require that we are transparent and open with our employees by informing them about how we collect and process their personal data and the purposes for which we use it. It is accessible to all employees before collection and processing of their personal data.

ACCENTURE'S DATA PRIVACY STATEMENT

PROTECTING ACCENTURE

[About IS](#) [Stay Secure](#) [Client Data Protection](#) [IS Advocate](#) [Infrastructure & Standards](#) [Report Security Incident](#)

[DATA SECURITY](#) > [GLOBAL DATA PRIVACY STATEMENT](#)

GLOBAL DATA PRIVACY STATEMENT

ACCENTURE

GLOBAL DATA PRIVACY STATEMENT

1. GENERAL INFORMATION

PRIVACY STATEMENT This global privacy statement explains how Accenture PLC and/or its affiliates ("Accenture") protect the personal data Accenture processes and controls relating to you ("your personal data"), why Accenture processes your personal data, who has access to your personal data and how you can exercise your rights in relation to the processing of your personal data.

Further information on Accenture (and, if relevant, its representative) can be found [here](#). Any Accenture entity located outside the European Union will for the purposes of compliance with data privacy laws be represented by Accenture PLC.

This global privacy statement provides an overview of Accenture's most common processing activities of your personal data. Please note that certain specific processing activities may be subject to a separate and tailored privacy statement.

ACCENTURE'S POLICY 90 – EXAMPLE

Policy 90 describes expected behaviour of employees:

4.2. Be **lawful**: Define purposes and limit use of personal data to those purposes

Personal data can only be processed for specified and **lawful purposes** as defined in data privacy laws. For example, processing is lawful if it is necessary to comply with a legal obligation, for the performance of a contract with the individual or with clear consent. These purposes must be **clearly explained to individuals** when using their data. For example, if you use personal data obtained from external sources (social media, external web sites and data brokers/list providers) you must check with Data Privacy that you have a lawful basis for processing that data prior to use. More information on the definitions for lawful processing can be found [here](#).



4.3. Be **transparent**: Provide notice, consent and choice

You must provide individuals with information (for example in a data privacy notice) which clearly explains how their data will be processed by Accenture. Notices should be in written in accordance with Accenture guidance, using plain language to inform individuals why we are collecting and using their personal data, for how long and any other relevant information. In some cases, their consent may be required and we may need to provide them with a choice (also known as opt-ins/opt-outs) for purposes such as marketing. Guidance and templates for meeting these requirements are available on the Data Privacy Site. Accenture's data privacy notice about how it generally uses employee personal data is available [here](#).



GDPR IMPACTED CHANGES

To address GDPR requirements impacting Accenture's internal operations globally, they include but are not limited to:



PRIVACY CONTROLS

- New controls added to existing Information Security Management System (ISMS) and ISO27001 Certification Framework
- Enhanced Data Privacy Impact Assessments (DIPA)



INCIDENT RESPONSE

- Updated our Cyber Incident Response Team (CIRT) Incident Response process



DATA PROTECTION OFFICER

- Appointed a global Data Protection Officer (DPO) and network of Geographic Privacy & Security Leads



INDIVIDUAL RIGHTS REQUESTS

- New process to address individuals rights to access, view, correct, and request the deletion of personal data



SUPPLIER DUE DILIGENCE & ASSESSMENT

- Data privacy questions added to supplier due diligence & assessment process
- Increased supplier assessments



EMPLOYEE TRAINING & COMMUNICATIONS

- Enhanced training, communications, and security behavior change to include GDPR awareness
- GDPR content in FY18 required training

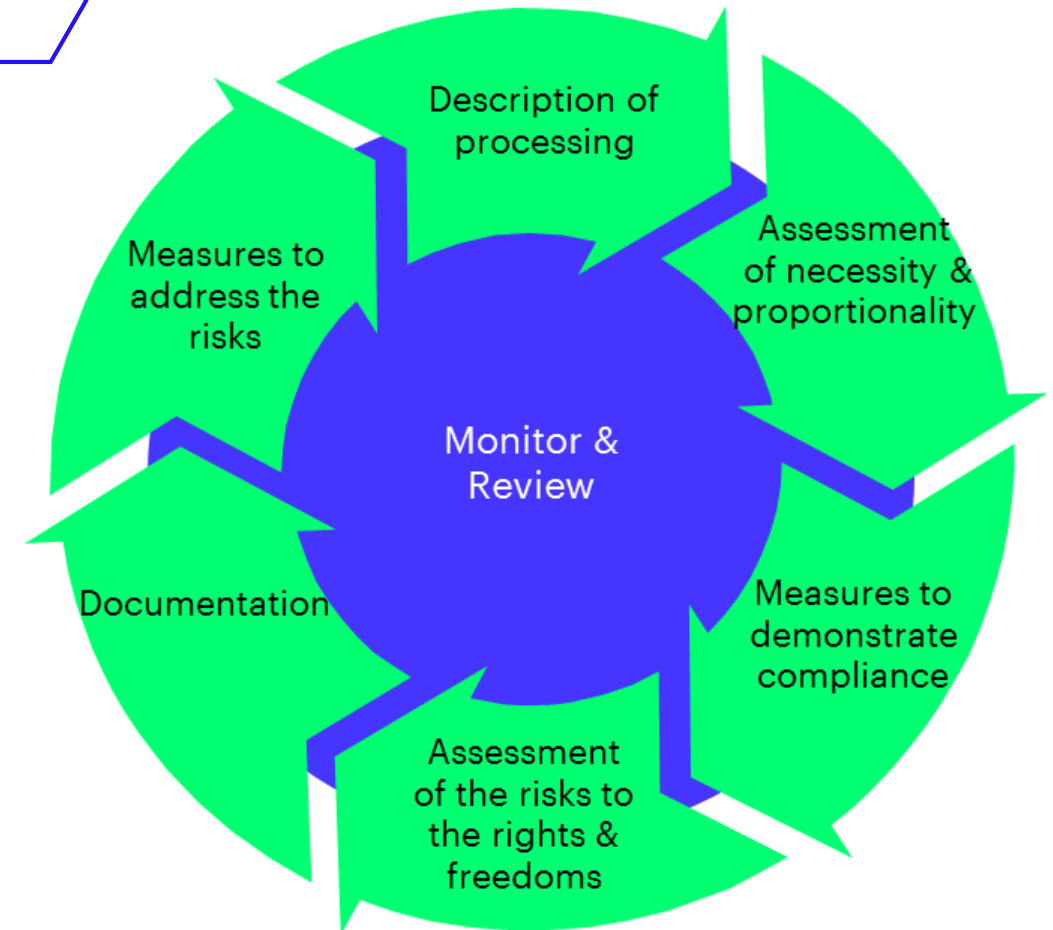
DOCUMENTING OUR COMPLIANCE

PRIVACY REVIEWS AND DPIA_s

WHAT IS A PRIVACY REVIEW?

What is a Privacy Review ?

- A Privacy Review (PR) is a data privacy specific assessment of any planned processing of personal data within Accenture
- Accenture must undertake privacy reviews of its personal data processing operations, either for its own internal processing activities related to Accenture employees and third parties or where Accenture processes personal data as part of Accenture's business offerings
- The Process Owner must undertake a privacy review of new or modified personal data processing operations prior to any implementation

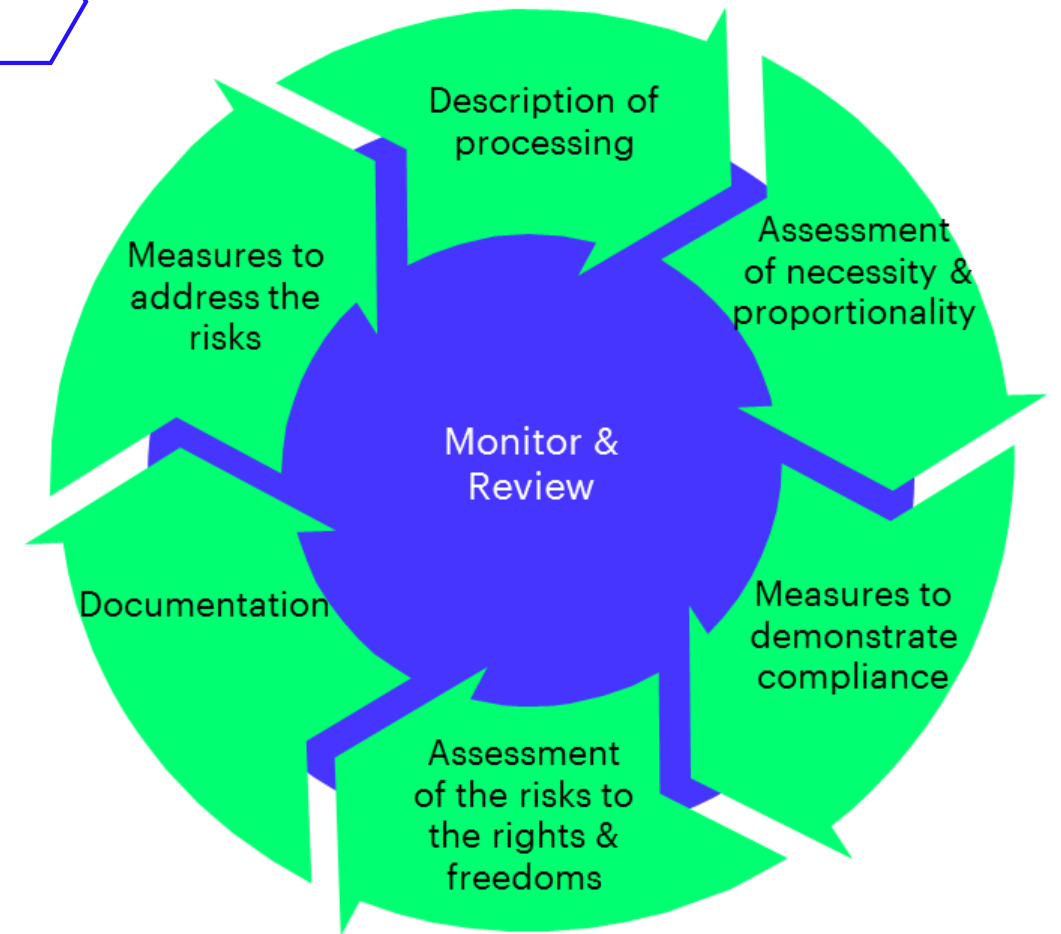


WHAT IS A DPIA?

What is a DPIA?

Data Protection Impact Assessments (DPIAs) evaluate processing activities to determine the likelihood and severity of **potential risk to individuals**, and help determine appropriate mitigating measures.

DPIAs are not a new concept but are now formalized under the General Data Protection Regulation (GDPR).



WHEN IS A DPIA REQUIRED?

PRE-ASSESSMENT – POTENTIAL HIGH RISK ?

If either one or more **MUST DO** criteria or two or more **MAY DO** criteria apply, a **DPIA** must be conducted

MUST DO

Scenarios always deemed to likely result into a high risk (Art. 35.3 GDPR):

1. Decision taken based on
 - **Systematic** and **extensive** evaluation of personal aspects and
 - Based on **automated processing** (incl. profiling) and
 - Has a **legal/significant affect** on individual
2. Processing **sensitive data** or data relating to criminal conviction and offences at large scale
3. Systematic monitoring of publicly accessible area at large scale

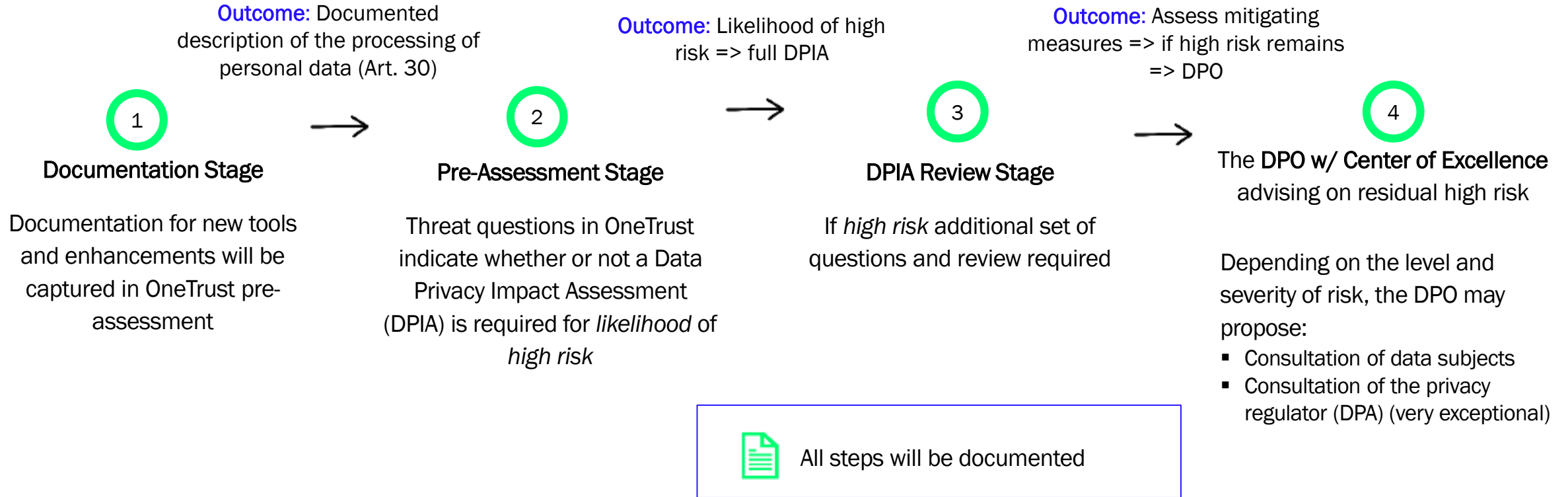
MAY DO

More than one of risk triggers as of A29 WP guidance:

1. Evaluation or **scoring** of individuals
2. Observing, **monitoring** or controlling individuals
3. Processing **sensitive data** or data of a highly personal nature
4. Processing data on a **large scale**
 - Number of individuals
 - Volumes and different types of data
 - Duration of processing
 - Geographical extent of the processing
5. Matching or combining datasets from **different sources**
6. Processing data related to **vulnerable individuals** (incl. employees)
7. Processing data in an **innovative manner** or using **new technology**
8. Processing activity could **prevent exercising a right**

DPIA APPROACH

HIGH LEVEL VIEW



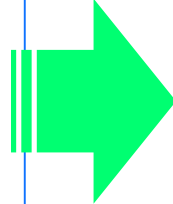
Regular monitoring

EXAMPLE OF DPIA QUESTION:

LEGAL BASIS/LEGITIMATE INTEREST

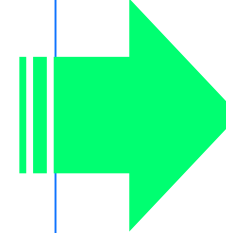
IDENTIFY LEGAL BASES :

1. Processing necessary for the performance of a contract ?
2. Processing necessary for Accenture's compliance with legal obligations?
3. Processing is necessary based on Accenture's legitimate interest ?
4. Processing is based on consent?



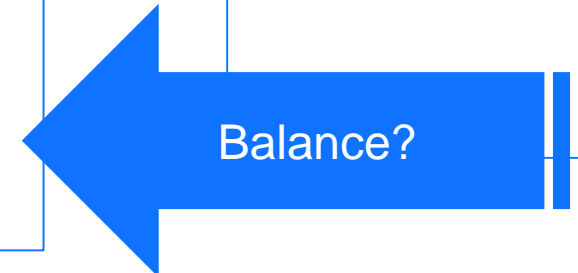
DEFINE LEGITIMATE INTEREST:

- ensuring and verifying that Accenture complies with laws and policies.
- protecting Accenture's reputation.
- managing disputes.
- managing potential corporate transactions.
- ensuring proper communication.
- ensuring handling of emergency situations within Accenture.
- combatting bribery and fraud.
- ensuring security.
- managing its workforce (including by evaluating performance).
- performing projects for clients.
- Other (free text field)



IMPACT TO INDIVIDUAL:

- Describe necessity and proportionality
- Describe the technical and organizational measures
- Transfer of data
- Rights of the individual
- Risk to the individual
- Stakeholder involvement



DPIA QUESTIONS APPROACH

BASED ON EXISTING DOCUMENTATION

Section 1: Documentation (Article 30)

(29 questions)

1. Identity of the data controller
2. Description of processing activity

Section 2: Pre-Assessment (16 questions)

Threshold Questions

- a. Similar processing activity in place?
- b. Mandatory scenarios (5)
 - Automated decision making
 - Sensitive data at large scale
 - Systematic monitoring at large scale
- c. Risk factors whether a DPIA is mandatory (8)
(at least two to apply)



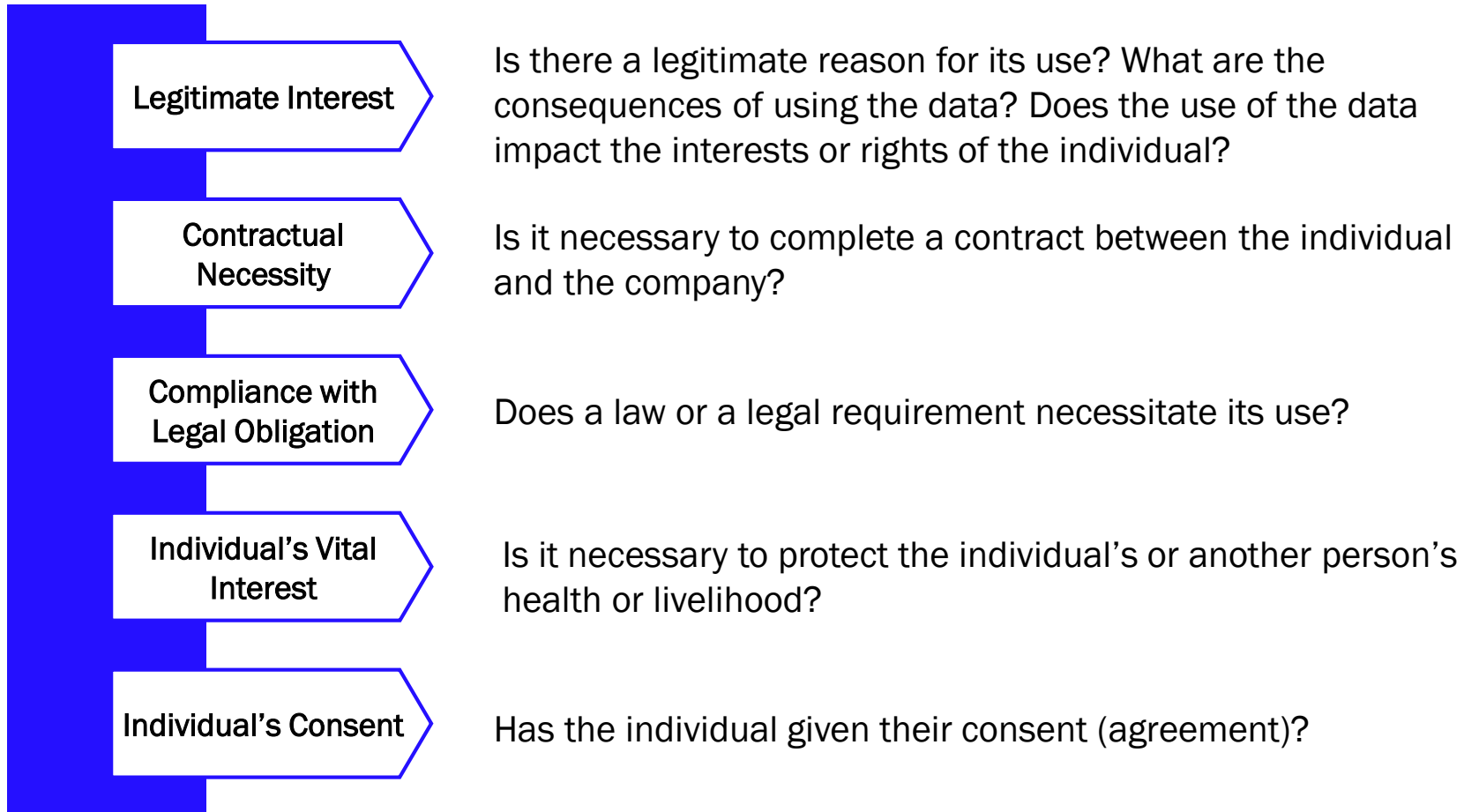
Section 3: Full DPIA

(28 main questions)

1. Purpose
2. Systems/Tools
3. Legal basis
4. Necessity and proportionality
5. Recipients
6. Technical and organizational security of personal data
7. Rights of the individuals
8. Risk identification towards rights
9. Consultation of stakeholders

LEGAL BASIS

5 mechanisms of legal basis for processing personal data:



EXAMPLE OF DPIA QUESTIONS:

LEGAL BASIS

<p>This question should be repeated for each purpose selected in question 1.</p> <p>What is the legal basis for the processing of (non-sensitive) personal data?</p>	<p>Drop down menu with the following options:</p> <ul style="list-style-type: none"> the processing is necessary for the performance of a contract between Accenture and the individual. the processing is necessary for Accenture's compliance with a legal obligation. the processing is necessary for the purposes of Accenture's legitimate interests. the processing is justified based on the consent of the individual. 	<p>Describe for each purpose the legal basis on which Accenture justifies the processing of (non-sensitive) personal data.</p> <p>There are 4 common legal bases on which Accenture can rely for the processing of (non-sensitive) personal data. A brief explanation of when you should select each legal basis is set out below:</p> <ul style="list-style-type: none"> the processing is necessary for the performance of a contract between Accenture and the individual. <p>You should select this legal basis where Accenture needs to process the personal data to perform its obligations under a contract with an employee, supplier or customer.</p> <p>For instance:</p> <ul style="list-style-type: none"> Accenture may use the bank account details of an employee to pay such employee the monthly wage agreed in his/her employment contract. for purposes of managing a customer project, Accenture may use the contact details of the customer employee that is listed in the customer contract as the project manager. the processing is necessary for Accenture's compliance with a legal obligation. <p>You should select this legal basis where Accenture needs to process the personal data to fulfil the requirements of under social security laws or other legal obligations.</p> <p>For instance, Accenture may disclose personal data of an employee to a social security institution where it is required to do so under social security laws.</p> the processing is necessary for the purposes of Accenture's legitimate interests. <p>You should select this legal basis where Accenture has a legitimate interest to process the personal data, unless such legitimate interest is overridden by the interests or rights and freedoms of the individuals.</p> <p>For instance, in the context of monitoring of personnel, Accenture has a legitimate interest to review whether its employees complied with the relevant policies (and, if the monitoring is limited to professional documents, the interests or rights and freedoms of the employee are unlikely to be more important than Accenture's legitimate interest).</p> the processing is justified based on the consent of the individual. <p>You should select this legal basis only very exceptionally. Accenture's policy on using consent as a legal basis is as follows:</p> <ul style="list-style-type: none"> you may use consent as the legal basis if you are taking automated decisions based on the profiling of individuals (see numbers 6 and 7). Note that, even with consent, you still have to put in place certain safeguards, such as the right to obtain human intervention. individuals you should not use consent as the legal basis for any other processing of (non-sensitive) personal data. Therefore, to the extent that the other legal bases do not apply, Accenture recommends not undertaking the processing. If you believe that exceptional circumstances justify the use of consent as a legal basis, contact dataprivacy@accenture.com. <p>Note that for consent to be valid, it must be freely given, specific and informed. The individual can also at any time revoke its consent.</p>
--	--	--

EXAMPLE OF DPIA QUESTIONS:

LEGAL BASIS/LEGITIMATE INTEREST

<p>Only display if the answer in question 9 is “the processing is necessary for the purposes of Accenture's legitimate interests”</p> <p>Describe Accenture's legitimate interests.</p>	<p>Drop down menu with the following options:</p> <ul style="list-style-type: none"> ensuring and verifying that Accenture complies with laws and policies. protecting Accenture's reputation. managing disputes. managing potential corporate transactions. ensuring proper communication. ensuring handling of emergency situations within Accenture. combatting bribery and fraud. ensuring security. managing its workforce (including by evaluating performance). performing projects for clients. other. <p>If “other” is selected, free text field.</p>	<p>Describe precisely what legitimate interests Accenture is pursuing.</p> <p>For instance:</p> <ul style="list-style-type: none"> if Accenture reviews its employees' compliance with internal Accenture policies, Accenture's legitimate interest could be described as follows: “monitoring employees so as to verify compliance with the relevant policies”. if Accenture includes contact data of an employee in an organization chart, Accenture's legitimate interest could be described as follows: “creating and maintaining an organization chart with contact data of the relevant employees, so as to facilitate internal communications”. <p>if Accenture retains a database with contact data of its main contact persons with suppliers, Accenture's legitimate interest could be described as follows: “creating and maintaining a database with contact data of the relevant contact persons with suppliers of Accenture, to facilitate communications between Accenture and such suppliers”.</p> <p>List the legal basis on which Accenture can rely for the processing of sensitive personal data. The legal bases for processing sensitive personal data are more limited than those for non-sensitive personal data.</p>
<p>Only display if the answer to question 4 is “yes”.</p> <p>What is the legal basis for the processing of sensitive personal data?</p>	<p>Drop down menu with the following options:</p> <ul style="list-style-type: none"> (for sensitive data other than data relating to criminal convictions and offences) the processing is necessary for Accenture's compliance with a legal obligation under employment or social security laws. (for sensitive data other than data relating to criminal convictions and offences) the processing is justified based on the consent of the individual. (for sensitive data other than data relating to criminal convictions and offences) the processing is necessary to protect the vital interests of the individual. (only for data relating to criminal convictions and offences) the processing is authorised by European law or by the law of the relevant EU country. 	<p>For sensitive personal data (other than data relating to criminal convictions and offences), there are 3 legal bases on which Accenture can rely for the processing of sensitive personal data. A brief explanation of when you should select each legal basis is set out below:</p> <ul style="list-style-type: none"> the processing is <u>necessary for Accenture's compliance with a legal obligation under employment or social security laws</u>. You should select this legal basis where, in an employment context, Accenture must process sensitive personal data to comply with its obligations under employment or social security laws. the processing is justified based on the <u>consent of the individual</u>. You should be careful in selecting this legal basis. Accenture's preference is to use other legal bases than consent for the processing of sensitive personal data. However, to the extent that processing sensitive personal data would be required for Accenture's legitimate business needs, and this processing cannot be justified on any other legal basis, you may select consent as the legal basis for the transfer. <p>Note that for consent to be valid, it must be explicit, freely given, specific and informed. The individual can also at any time revoke its consent.</p> <ul style="list-style-type: none"> the processing is necessary to <u>protect the vital interests of the individual</u>. You should select this basis only where you could not protect a vital interest of an individual without using the sensitive data. This is for instance the case where you use health information to provide first aid services to an employee. <p>For sensitive personal data relating to criminal convictions and offences, the legal bases are even more limited. Such data may only be processed where authorised by European law or by the law of the relevant EU country. If there is no law that authorises the processing of such data, Accenture may not undertake such processing.</p>



Centre for
Information
Policy
Leadership
Hunton Andrews Kurth LLP



PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

Session II

Transparency, Legal Bases for Processing (Consent, Notification of Purpose and Legitimate Interest) and DPIA

- ❖ Alex Cebulsky, Senior Legal Counsel, Global Data Privacy, Accenture
- ❖ Derek Ho, Vice President, Senior Managing Counsel, Privacy and Data Protection, Mastercard
- ❖ Alison Howard, Assistant General Counsel, Microsoft
- ❖ Katherine Tassi, Deputy General Counsel, Privacy and Product, Snap

Implementing Accountability

Centre for Information Policy Leadership (CIPL) Workshop in collaboration with the Singapore Personal Data Protection Commission (PDPC)

Derek Ho, Assistant General Counsel



Mastercard's Privacy & Data Protection Program

Mastercard's program has been built to ensure compliance, enable innovation and be responsive to the evolving regulatory landscape

Compliance



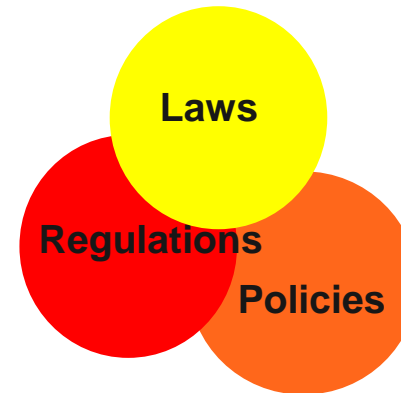
- Legal Inventories
- Policies, Standards, Procedures
- Regulatory Requirements
- Data Transfer solutions
- Breach notification
- Audits/Reviews

Privacy By Design



- Ensures privacy/data protection requirements are addressed as part of product design
- Work as a key business advisor
- Ensure accurate system and process implementation

Regulatory



- Monitor new and pending laws and regulations
- Proactive incorporation into product design thinking
- Regulatory outreach to explain business implications of new law

Training & Development



- Provide training
- Understand privacy requirements in all business areas
- Create key business partnerships and drive controls

Priceless



a meal | or curated
Cantonese cuisine

Choose Mastercard®. Choose Priceless.

Book a meal at Hong Kong's Lai Bun Fu with
Mastercard and access priority reservations
and 50% off a special tasting menu.
Book now at priceless.hk



mastercard.

Privacy by Design:
Priceless


Transparency is embedded through providing clear language during the registration process. Specific choices are presented for marketing communications opt-ins

Program specific opt-in marketing consent

General Mastercard product and services opt-in marketing consent

Clear / easy to understand information about providing and withdrawing consent

Things to do Locations Log in



Priceless Cities

Connect to Priceless Cities

Email

Create Password*

Password must be at least 8 characters and contain two of the following: upper case, lower case, numbers and special characters

Confirm Password*


☐ I agree that Mastercard International Inc. and its affiliates may use my contact details and interactions with Priceless Cities to send me personalized marketing communications about all Priceless programs.

☐ I agree that Mastercard International Inc. and its affiliates may use my contact details to send me email marketing communications about all products and services.

Your consent to receiving marketing communications is voluntary. You are free to withdraw your consent at any time, free of charge. More information on Mastercard's privacy practices and on your rights including withdrawing consent is available in the [Priceless Cities Privacy Notice](#).

By clicking Sign Up or Sign Up with Facebook, I confirm that I have read and agree to the [Terms of Use](#) for Priceless Cities.

Sign up

 SIGN UP WITH FACEBOOK

[Already have an account? Log in here](#)

Privacy by Design:
Priceless

*Transparency and choice is embedded through layered
program specific notices and clear opt-outs*

Priceless Cities

Interests

Things to do

Locations

Log in

Sign up

English

Priceless Cities Global Privacy Notice

Effective Date: 4/4/18

Mastercard International Inc., Mastercard Europe SA, and their affiliates and other entities within Mastercard's group of companies (collectively, "Mastercard", "we", "us", or "our") respect your privacy.

This Privacy Notice applies to our privacy practices pertaining to Personal Information collected in the context of Priceless Cities. This Privacy Notice does not cover the collection and use of your Personal Information by Mastercard in the context of other programmes, by third parties on other Mastercard branded websites, by your Mastercard Card issuers (e.g., your bank), or any other information or communications that may reference Mastercard outside of Priceless Cities.

This Privacy Notice describes the types of Personal Information we collect in connection with Priceless Cities, the purposes for which we collect that Personal Information, the other parties with whom we may share it, and the measures we take to protect the security of the data. It also tells you about your rights and choices with respect to your Personal Information, and how you can reach us to update your contact information or get answers to questions you may have about our privacy practices.

Your visit to the Priceless Cities website and your participation in the programme is subject to this Privacy Notice and to our [Terms of Use](#). Children and minors (under the age of 18) are not eligible to use Priceless Cities. For more general information about Mastercard's privacy practices, please visit Mastercard's Global Privacy Notice at <https://www.mastercard.com.sg/en-sg/about-mastercard/what-we-do/privacy.html>.

1. Personal Information We May Collect

2. How We May Use Your Personal Information

3. How We Share Your Personal Information

4. Your Rights and Choices

5. How We Protect Your Personal Information

6. Data Transfers

7. Features and Links to Other Websites

8. Updates to This Privacy Notice

9. How to Contact Us

1. Personal Information We May Collect

We May Collect the following Personal Information:

• Registration information and contact details.

• Your credit or debit card number (the 16 digit payment card number).

• Information related to your use of Priceless Cities collected via cookies and other similar technologies.

Learn more

Top of Page

Home | About Mastercard | Careers | Newsroom | Investor Relations

mastercard

About Mastercard

Who We Are

What We Do

Being a Responsible Company

Careers

English

Effective Date: 4/4/2018

Mastercard International Incorporated and its affiliates (collectively, "Mastercard") respect your privacy.

• Personal Information We May Collect

• How We May Use Your Personal Information

• How We Share Your Personal Information

• Your Rights and Choices

• Data Transfers

• How We Protect Your Personal Information

• Features and Links to Other Websites

• Updates to This Global Privacy Notice

• How to Contact Us

This Global Privacy Notice describes the types of Personal Information we collect, the purposes for which we collect that Personal Information, the other parties with whom we may share it and the measures we take to protect the security of the data. It also tells you about your rights and choices with respect to your Personal Information, and how you can contact us about our privacy practices.

Our privacy practices may vary among the countries in which we operate to reflect local practices and legal requirements. Specific privacy notices may apply to some of our products and services. Please visit the webpage of the specific product or service to learn more about our privacy and information practices in relation to that product or service.

Data Analytics Opt Out

Web Analytics Opt Out

Marketing Email Opt Out

My Data

Mastercard Concierge App Privacy Notice

Program specific layered privacy notice

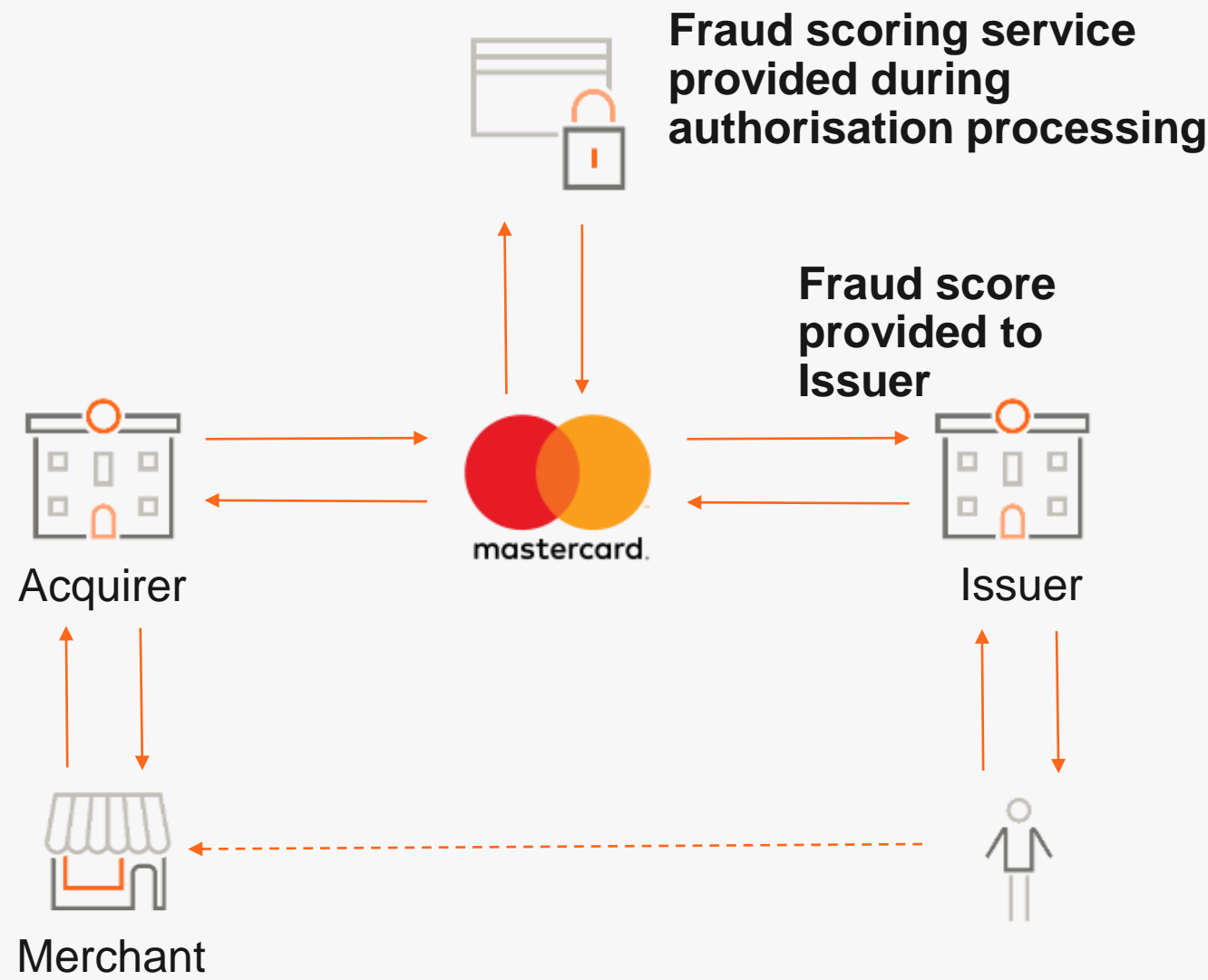
Easily accessible opt-out choices located prominently within the global privacy notice

mastercard

©2018 Mastercard. Proprietary and Confidential.

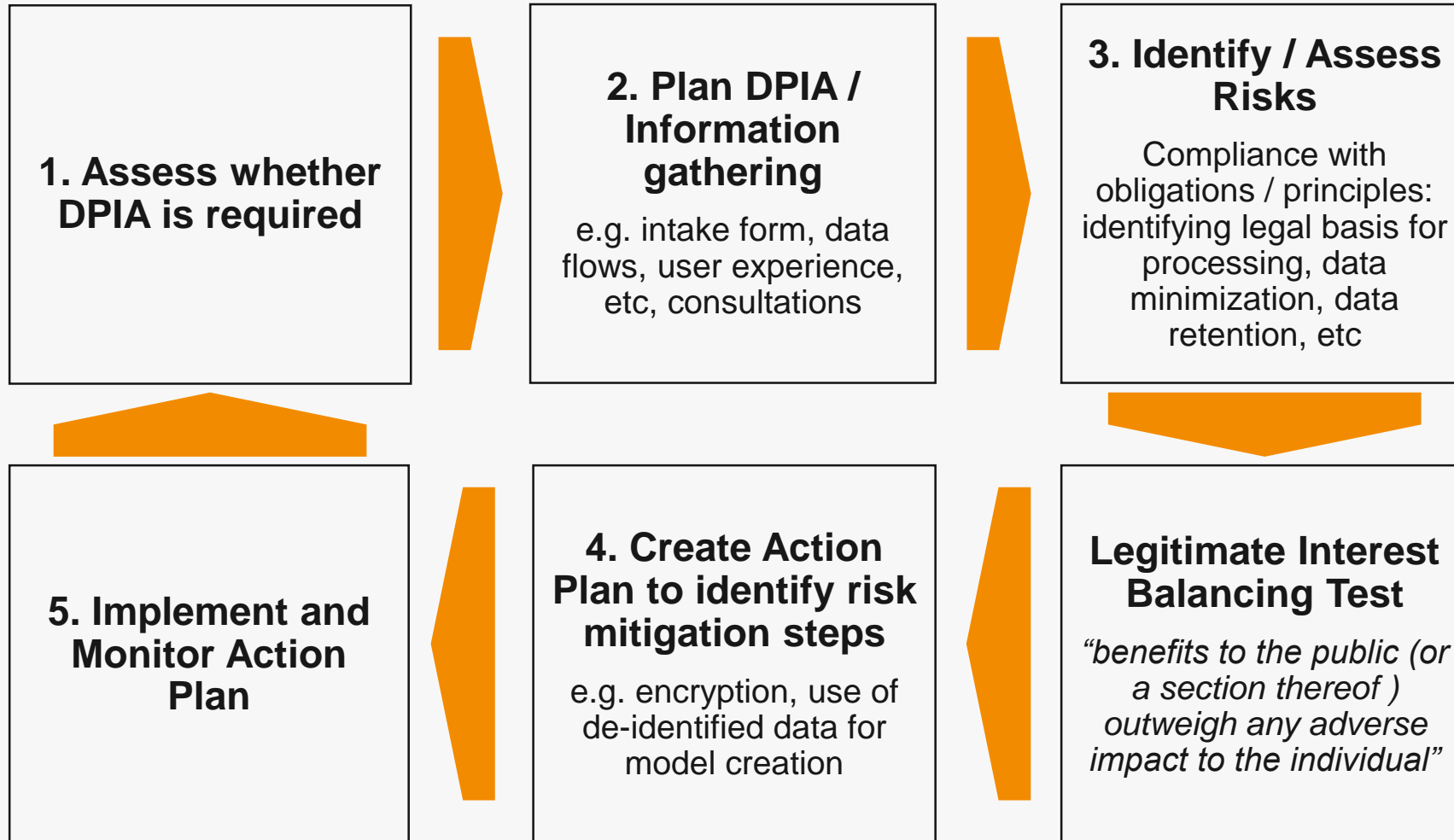
Fraud Prevention

Legitimate interest would be relied on as the basis for fraud prevention processing activities



Data Protection Impact Assessment (using the PDPC Guide to DPIAs)

Conducting a risk assessment and documenting a legitimate interest balancing test in the context of fraud prevention





Centre for
Information
Policy
Leadership
Hunton Andrews Kurth LLP



PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

Session II

Transparency, Legal Bases for Processing (Consent, Notification of Purpose and Legitimate Interest) and DPIA

- ❖ Alex Cebulsky, Senior Legal Counsel, Global Data Privacy, Accenture
- ❖ Derek Ho, Vice President, Senior Managing Counsel, Privacy and Data Protection, Mastercard
- ❖ Alison Howard, Assistant General Counsel, Microsoft
- ❖ Katherine Tassi, Deputy General Counsel, Privacy and Product, Snap

Layered Approach to Transparency

- Microsoft Privacy Statement
- Privacy Dashboard for consumers
- Service Trust Portal for commercial customers
- In-product notices

GDPR update in May

<https://privacy.microsoft.com/en-us/privacystatement>

Microsoft Privacy Statement

Last Updated: May 2018 [What's new?](#)

Your privacy is important to us. This privacy statement explains the personal data Microsoft processes, how Microsoft processes it, and for what purposes.

Microsoft offers a wide range of products, including server products used to help operate enterprises worldwide, devices you use in your home, software students use at school, and services developers use to create and host what's next. References to Microsoft products in this statement include Microsoft services, websites, apps, software, servers, and devices.

Please read the product-specific details in this privacy statement, which provide additional relevant information. This statement applies to Microsoft's interactions with you and the Microsoft products listed below, as well as other Microsoft products that display this statement.

Personal Data We Collect

How We Use Personal Data

Reasons We Share Personal Data

How to Access & Control Your Personal Data

Cookies & Similar Technologies

Products Provided by Your Organization—Notice to End Users

Microsoft account

Other Important Privacy Information 

Product-specific details:

Enterprise & Developer Products 

Productivity & Communications Products 

Search & Artificial Intelligence 

Windows 

Entertainment and Related Services 

Microsoft Health Services 

Cookies

Most Microsoft sites use cookies, small text files placed on your device which web servers in the domain that placed the cookie can retrieve later. We use cookies to store your preferences and settings, help with sign-in, provide targeted ads, and analyze site operations. [Click here to learn more.](#)

EU-U.S. & Swiss-U.S. Privacy Shield

Microsoft adheres to the principles of the EU-U.S. and Swiss-U.S. Privacy Shield frameworks. To learn more, [click here](#).

Personal Data We Collect

Microsoft collects data from you, through our interactions with you and through our products. You provide some of this data directly, and we get some of it by collecting data about your interactions, use and experiences with our products. The data we collect depends on the context of your interactions with Microsoft and the choices you make, including your privacy settings and the products and features you use. We also obtain data about you from third parties.

If you represent an organization, such as a business or school, that utilizes Microsoft's Enterprise and Developer Products, please see the [Enterprise](#) and [Developer](#) section of this statement to learn how we process your data.

You have choices when it comes to the technology you use and the data you share. When we ask you to provide personal data, you can decline. Many of our products require some personal data to provide you with a service. If you choose not to provide data necessary to provide you with a product or feature, you cannot use that product or feature. Likewise, where we need to collect personal data by law or to enter into or carry out a contract with you, and you do not provide the data, we will not be able to enter into the contract; or if this relates to an existing product you're using, we may have to suspend or cancel it. We will notify you if this is the case at the time. Where providing the data is optional, and you choose not to share personal data, features like personalization that use such data will not work for you.

[Learn More](#)

[Top of page](#) 

How We Use Personal Data

Microsoft uses the data we collect to provide you rich, interactive experiences. In particular, we use data to:

- Provide our products, which includes updating, securing, and troubleshooting, as well as providing support. It also includes sharing data, when it is required to provide the service or carry out the transactions you request;
- Improve and develop our products;
- Personalize our products and make recommendations; and
- Advertise and market to you, which includes sending promotional communications, targeting advertising, and presenting you relevant offers.

GDPR update in May

<https://privacy.microsoft.com/en-us/Updates>

Change History for Microsoft Privacy Statement

[Back to the privacy statement](#)

May 2018

- We made edits throughout the privacy statement intended to improve transparency and readability. For example, we:
 - added new categories of personal data we collect, such as voice data, content consumption data, and browse history;
 - added new uses of personal data;
 - simplified text and eliminated duplicative text and qualifiers such as "we may";
 - added navigation cues, like bullet points, to highlight key points and reduce reader fatigue; and
 - improved consistency in the language used to describe similar concepts.
- We added language required by the EU General Data Protection Regulation (GDPR). For example, we now:
 - describe individuals' rights to access their data, which applies regardless of location;
 - describe the legal bases for Microsoft's data processing, including under the GDPR's legitimate interests provisions, and the purposes of our processing of personal data; and
 - specify the choices individuals have with respect to sharing personal data with Microsoft, along with the consequences of sharing and Microsoft's data processing.
- In the **Personal Data We Collect** section, we:
 - added language to direct customers to the appropriate sections of the privacy statement;
 - added new examples of third-party sources of personal data; and
 - updated the descriptions of types of personal data we collect.
- In the **How We Use Personal Data** section, we:
 - clarified how Microsoft uses data generally, using concepts from the data taxonomy framework in the ISO 19944 international standard;
 - clarified our policies around storing unauthenticated data and authenticated data; and
 - updated specific descriptions of how Microsoft uses personal data. For example, we added text to describe how we use personal data for promotional communications and legal compliance, and we provided information about where Microsoft uses automated systems to process personal data. Additionally, we moved some details about our advertising practices to a separate section under **Other Important Information**.
- In the **How to Access & Control Your Personal Data** section, we described how customers can access their personal data and made the text applicable to all customers, regardless of their location.
- In the **Cookies and Similar Technologies** section, we updated the description of the cookies Microsoft uses.
- In the **Notice to End Users** section, we clarified cases when organizations, like an employer or school, have access to an individual's personal data.
- In the **Microsoft Account** section, we clarified the differences between the three types of Microsoft accounts.
- In the **Other Important Privacy Information** section, we:
 - moved the contents of the **European Privacy Rights** subsection to the **How to Access & Control Your Personal Data** and **How to Contact Us** sections;
 - added a section called **Advertising**, using text from the original **How We Use Personal Data** section, to describe Microsoft's advertising practices and commitments;
 - updated information on how Microsoft processes children's personal data;
 - clarified how and when Microsoft makes changes to the privacy statement;
 - identified which Microsoft entities are data controllers under the GDPR, how to contact us, and how to lodge a complaint.
- In the **Enterprise and Developer Products** section, we:
 - described how basic, aggregated account information related to Enterprise Online Services may be shared with authorized partners in certain circumstances;
 - identified that Microsoft is a data processor under the GDPR when providing the **Enterprise Online Services**.
- In the **Office** and **Skype** sections we described new features and updated how existing features and functionality process personal data. For example, we explain how Cortana works in Skype.
- In **Search and Artificial Intelligence**, we described our most current features and functionality. For example, in the **Cortana** subsection, we described the personal data Microsoft collects from users who are signed in and signed out of the service.
- In the **Windows** section, we removed text about a service, Wi-Fi Connecting to suggest open hotspots, that is no longer available. Under **Web Browsers**, we described the type of browser data that syncs across devices.
- In the **Entertainment and Related Services** section, we updated how existing features and functionality process personal data and provided new information on Xbox, Xbox Live, and Mixer.
- We added a hyper link to access the privacy policy of our subsidiary **LinkedIn**.

Consumer Privacy Dashboard

Browsing history



If browsing history in Cortana is turned on, your Microsoft Edge browsing history is sent to Microsoft so that Microsoft features and services may use this data to provide you with timely and intelligent answers, proactive personalized suggestions, or to complete tasks for you.

In addition to the browsing history saved here, Microsoft Edge also saves your browsing history on your device. To clear that data, on your device, go to **Microsoft Edge > More > Settings**.

When you use InPrivate tabs or windows, your browsing data (like your history, temporary internet files, and cookies) isn't saved on your device once you're done. [Learn more about InPrivate Browsing](#)

[VIEW AND CLEAR BROWSING HISTORY >](#)

Search history



Like other search engines, Bing uses your search history to give you better results, including personalization and autosuggest. Cortana also uses that data to give you timely, intelligent answers, personalized suggestions, and complete other tasks for you.

[View and change your search settings](#)

[Learn more about InPrivate Browsing](#)

[VIEW AND CLEAR SEARCH HISTORY >](#)

Location activity



To give you directions to the places you want to go, and show you data relevant to where you are, we use locations that you provide or that we've detected using technologies like GPS.

[Learn more about changing the location settings on your Windows device](#)

[VIEW AND CLEAR LOCATION ACTIVITY >](#)

Voice activity



When you use voice commands with Windows, Cortana, and other cloud-based, voice-enabled products and services from Microsoft, we will collect and store your audio recordings so that we can enhance your experience with better speech recognition and other personalized speech experiences. Microsoft uses your voice command data to improve the ability of its products and services to correctly recognize your pronunciation and speech patterns.

[VIEW AND CLEAR VOICE ACTIVITY >](#)

<https://account.microsoft.com/privacy/>

Media activity



When you watch movies or TV on a Microsoft app or service, we collect data about your media activity so that we can provide you with more relevant recommendations for entertainment and content.

[VIEW AND CLEAR MEDIA ACTIVITY >](#)

Product and service activity



When you use a Microsoft product or service, we may save data about your activity to your Microsoft account – such as info about which apps or services you use and how you use them. This info helps improve our products and make them work better for you.

[VIEW AND CLEAR APPS AND SERVICES ACTIVITY >](#)

Product and service performance



When you use a Microsoft product or service, we collect reliability and performance data to measure the quality of your experience. This data tells us about the health of these products and services and helps us fix and improve them.

[CLEAR PRODUCT AND SERVICE PERFORMANCE DATA >](#)

Cortana's Notebook



To help you avoid traffic, remember anniversaries, text the right "Jennifer" in your contact list, and in general do more, Cortana needs to know what you're interested in, what's on your calendar, and who you might want to do things with. The Notebook is where Cortana keeps track of your interests to give you a personalized experience. When you don't want to reach for a keyboard, Cortana can use your speech and to help translate what you say or write into documents and text messages. On the dashboard, you can manage some of your Cortana preferences in the cloud, please visit the Cortana Notebook available within your Cortana App to view more information.

[EDIT CORTANA DATA >](#)

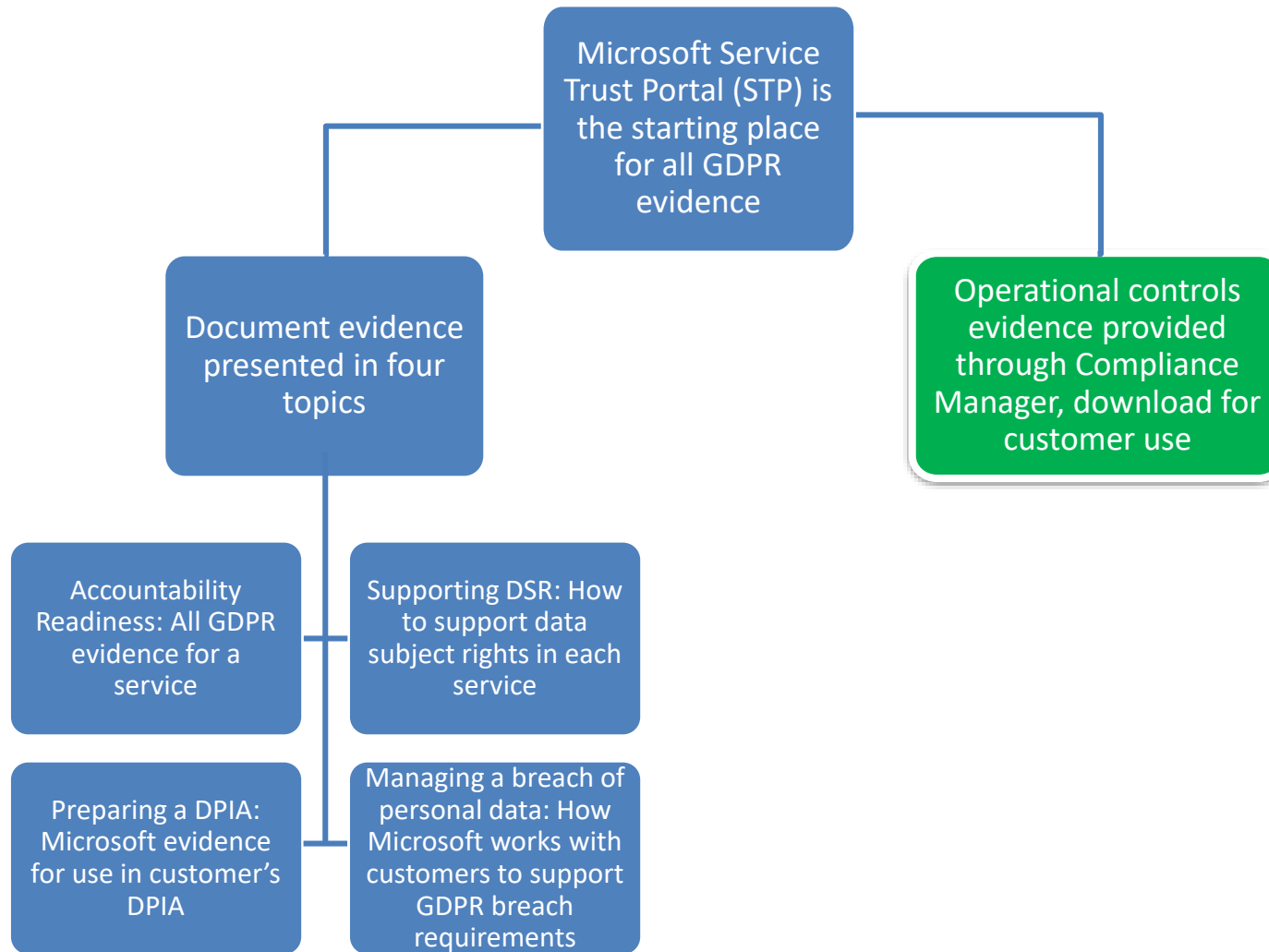
LinkedIn



When you connect your Microsoft and LinkedIn accounts, Microsoft shares some of your account data with LinkedIn, such as calendar and contact data. Likewise, LinkedIn shares some of your account data with Microsoft, such as profile and connections data. [Find out how to connect and disconnect Microsoft and LinkedIn accounts and manage shared data.](#)

[VIEW LINKEDIN CONNECTION SETTINGS >](#)

Service Trust Portal: How the documentation is presented



How customers can use the info

Incorporate the evidence into their accountability information

- Demonstrate they have met their controller obligations per Article 28
- Use Microsoft-provided evidence to supplement their DPIA as appropriate
- Implement their record keeping using information from Microsoft services

Support Data Subject Rights

- Incorporate evidence into the information they provide to data subjects
- Build their DSR-response system on the capabilities described in the documentation

Integrate the Microsoft operational controls into their privacy information management system



GDPR

Get Started: Support for GDPR Accountability

Our commitment to support your GDPR compliance starts right here

What is the GDPR?

On May 25, 2018, a European privacy law, the General Data Protection Regulation (GDPR), will take effect. The GDPR imposes new rules on companies, government agencies, non-profits, and other organizations that offer goods and services to people in the European Union (EU), or that collect and analyze data tied to EU residents.

This site is designed to provide you information about the capabilities in Microsoft services that you can use to address specific requirements of the GDPR. Access the documentation helpful to your GDPR accountability, and to your understanding of the technical and organizational measures Microsoft has taken to support the GDPR. Documentation for Data Protection Impact Assessments, Data Subject Requests (DSRs), and Data Breach Notification is provided to incorporate into your own accountability program in support of the GDPR.

Select a topic below to get started:



Data Protection Impact Assessments

How Microsoft helps organizations
meet their own DPIA obligations

[LEARN MORE >](#)



Data Subject Requests

How Microsoft Helps Controllers
Address Data Subject Requests
Under the GDPR

[LEARN MORE >](#)



Data Breach Notification

How Microsoft detects and responds
to a breach of personal data and
notifies controllers under the GDPR

[LEARN MORE >](#)



Accountability Readiness Checklist

A convenient way to access the
information you may need to
support GDPR when using Microsoft
services.

[LEARN MORE >](#)

Data Protection Impact Assessments

Filter by title

[Microsoft 365 Enterprise documentation and resources](#)

> Deploy Microsoft 365 Enterprise

Services and concepts

> Identity and device access configurations

▼ Compliance solutions

▼ GDPR

> Accountability readiness checklists

Information protection

> Data subject requests

> Breach notification

▼ Data protection impact assessments

Office 365

Azure

Dynamics

Microsoft Support and Professional Services

Microsoft's data protection officer

Data Protection Impact Assessments: Guidance for Data Controllers Using Dynamics 365

05/18/2018 • 10 minutes to read • Contributors

Under the General Data Protection Regulation (GDPR), data controllers are required to prepare a Data Protection Impact Assessment (DPIA) for processing operations that are "likely to result in a high risk to the rights and freedoms of natural persons." There is nothing inherent in Dynamics 365 that would necessarily require the creation of a DPIA by a Data Controller using it. Rather, whether a DPIA is required will be dependent on the details and context of *how* the data controller deploys, configures, and uses Dynamics 365.

The purpose of this document is to provide data controllers with information about Dynamics 365 that will help them to determine whether a DPIA is needed and, if so, what details to include.

Part 1 – Determining Whether A DPIA is Needed

Article 35 of the GDPR requires a data controller to create a Data Protection Impact Assessment "[w]here a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons." It further sets out particular factors that would indicate such a high risk, which are discussed in the following table. In determining whether a DPIA is needed, a data controller should consider these factors, along with any other relevant factors, in light of the controller's specific implementation(s) and use(s) of Dynamics 365.

Table 1 - High risk factors in Dynamics 365

Risk Factor	Relevant Information about Dynamics 365
A systematic and extensive evaluation of personal aspects relating to natural persons which is based on	Dynamics 365 does perform certain automated processing of data, such as lead or opportunity scoring (e.g. predicting how

Accountability Readiness Checklist

Records related to processing PII (7.2.7)

Customer consideration

The customer should maintain all necessary and required records related to processing personal data (e.g. purpose, security measures, etc.). Where some of these records must be provided by a sub-processor, the customer should ensure that they can obtain such records.

Supporting Microsoft Documentation:

The tools provided by Microsoft services to help you maintain the records necessary demonstrate compliance and support for accountability under the GDPR. See the Azure Security Documentation [2] for activity and diagnostic logging and logging of processing of personal data.

Addresses GDPR Article(s)

(5)(2), (24)(1), (30)(1)(a), (30)(1)(b), (30)(1)(c), (30)(1)(d), (30)(1)(g), (30)(1)(f), (30)(3), (30)(4), (30)(5)

Records related to processing (7.2.7): Azure



Logging and auditing

OMS provides extensive logging of system and user activity, as well as system health. The OMS [Log Analytics](#) solution collects and analyzes data generated by resources in Azure and on-premises environments.

- **Activity logs:** [Activity logs](#) provide insight into operations performed on resources in a subscription. Activity logs can help determine an operation's initiator, time of occurrence, and status.
- **Diagnostic logs:** [Diagnostic logs](#) include all logs emitted by every resource. These logs include Windows event system logs, Azure Storage logs, Key Vault audit logs, and Application Gateway access and firewall logs.
- **Log archiving:** All diagnostic logs write to a centralized and encrypted Azure storage account for archival. The retention is user-configurable, up to 730 days, to meet organization-specific retention requirements. These logs connect to Azure Log Analytics for processing, storing, and dashboard reporting.

Additionally, the following OMS solutions are included as a part of this architecture:

- **AD Assessment:** The Active Directory Health Check solution assesses the risk and health of server environments on a regular interval and provides a prioritized list of recommendations specific to the deployed server infrastructure.
- **Antimalware Assessment:** The Antimalware solution reports on malware, threats, and protection status.
- **Azure Automation:** The Azure Automation solution stores, runs, and manages runbooks.
- **Security and Audit:** The Security and Audit dashboard provides a high-level insight into the security state of resources by providing metrics on security domains, notable issues, detections, threat intelligence, and common security queries.
- **SQL Assessment:** The SQL Health Check solution assesses the risk and health of server environments on a regular interval and provides customers with a prioritized list of recommendations specific to the deployed server infrastructure.
- **Update Management:** The Update Management solution allows customer management of operating system security updates, including a status of available updates and the process of installing required updates.
- **Agent Health:** The Agent Health solution reports how many agents are deployed and their geographic distribution, as well as how many agents which are unresponsive and the number of agents which are submitting operational data.
- **Azure Activity Logs:** The Activity Log Analytics solution assists with analysis of the Azure activity logs across all Azure subscriptions for a customer.
- **Change Tracking:** The Change Tracking solution allows customers to easily identify changes in the environment.

DPIA approach

DPIAs are at a higher level of group processing than privacy reviews, generally that of a service (e.g., Windows) or business process (e.g., email marketing)

- Privacy reviews will continue to occur at a granular level. Each DPIA will have many privacy reviews that “ladder” up to it.
- The scope of a particular DPIA is determined by identifying common types of data processing, the common sets of risk mitigations or logical product or service groupings.
- Discrete components of services may warrant their own DPIA, if the processing or risks are unique.

DPIAs introduce an opportunity for better consistency and quality across Microsoft

The European DPO has significant input to the DPIAs



DPIA Template

DPIA FOR <PRODUCT/SERVICES/BUSINESS OPERATION NAME>

Contents

PART I: For Privacy Managers	2
1.0 Record of Review.....	2
1.1 – Contact Information.....	2
1.2 – History of Review.....	2
1.3 – Review and Document Change Log.....	2
2.0 Baseline Review.....	3
2.1 – Description of the Processing.....	3
2.2 – Data Inventory.....	4
2.3 – Data Location and Data Flows.....	5
2.4 – Measures contributing to the Rights of Data Subjects & Other Privacy Considerations.....	5
Part II: For Frontline Attorneys	10
3.0 Initial Evaluation of Processing / Risk Rating.....	10
3.1 Bases of Processing.....	10
3.2 Legitimate Interests.....	11
3.3 Evaluation of High Risks.....	12
3.4 Evaluation of Other Risks.....	13
4.0 Risk Mitigations and Findings.....	13
4.1 Risk Mitigations.....	13
4.2 Residual Risk.....	13
PART III: For the Data Protection Officer	14
5.0 Data Protection Officer Findings.....	14
5.1 DPO Recommendations.....	14
5.2 Prior Consultation.....	14
PART IV: For Corporate, External, & Legal Affairs	14
6.0 Final Determination.....	14
7.0 Document Change Log.....	15
Appendix A: Data Inventory	16
Appendix B: Data Flow Diagrams	17



Centre for
Information
Policy
Leadership
Hunton Andrews Kurth LLP



PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

Session II

Transparency, Legal Bases for Processing (Consent, Notification of Purpose and Legitimate Interest) and DPIA

- ❖ Alex Cebulsky, Senior Legal Counsel, Global Data Privacy, Accenture
- ❖ Derek Ho, Vice President, Senior Managing Counsel, Privacy and Data Protection, Mastercard
- ❖ Alison Howard, Assistant General Counsel, Microsoft
- ❖ Katherine Tassi, Deputy General Counsel, Privacy and Product, Snap

Transparency in different contexts

Factors to consider:

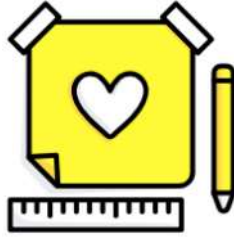
- Audience/customer (organization's audience and regulators)
- Types of data
- Types of processing
- Purposes of processing
- Product(s)

Note: Transparency requirement in GDPR (prescriptive sections, but general requirement tied to accountability)



We communicate honestly and openly

When you use Snap products, you share information with us – it's our responsibility to help you understand how that information is used. Our [Privacy Policy](#) explains how we collect, use, and share information – you can read the highlights [here](#). If you're curious about how a certain feature uses your data, [Our Approach to Privacy](#) breaks things down a bit more. We also explain how features use data right inside of our apps, and throughout our [Support Center](#). Of course, if you still can't find what you need, [you can always ask!](#)



We design with privacy in mind

New features go through an intense privacy review process – we talk about things, we debate them, and we work hard to build products we're proud of and that we'll want to use. After all, we use these products every day, both at work and in our personal lives. We handle your information with the same care that we use for ourselves, our company, our family, and our friends.



Deletion is our default

Snapchat aims to capture the feeling of hanging out with friends in person – that’s why Snaps and Chats are deleted from our servers once they’re opened or expired. After a Snap is deleted, we’ll mainly be able to see the basic details – like when it was sent and who it was sent to. [Learn more.](#)

It’s important to keep in mind that other Snapchatters can always take a screenshot, or save things using a third-party app. At the end of the day, it’s best to only share the need-to-know stuff with the people you really trust – just like you would in real life!

Notification of Purposes of Processing

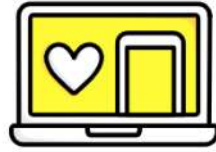
Factors to consider:

- Audience/customer (organization's audience and regulators)
- Impact of processing on individual
- Is there any action that can follow from notice



Keep Our Services Safe & Secure

It's important to us that you're as safe and secure as possible when you're using our services, so we use some of your information to enhance these aspects of our products too! For example, we provide two-factor authentication to secure your account and can send you an email if we notice any suspicious activity. We also scan URLs sent on Snapchat to see if that webpage is potentially harmful, and can give you a warning about it.



Develop New Features & Improve Existing Ones

First stop: development. Our teams work closely together to develop fun, imaginative new features. You actually help out our development team every day, just by using our products!

For example, we look at the Filters and Lenses that Snapchatters use the most to decide which ones we should create next. We develop a lot of our features with the same approach, so we can stay on top of our game and build new things you love!

We're always looking for ways to improve our services too. Sometimes, we'll change how a feature works or how the app looks. Your information can help us decide what kind of improvements we should make. For example, Snapchat can guess who your best friends are, based on who you talk with the most – so the app can place them right at the top of your Send To screen to make Snapping with them that much easier. Studying data from a lot of Snapchatters can help us see trends in the ways that people use the app. This helps inspire us to improve Snapchat in big ways, on a larger scale!



Provide Relevant Ads

We think ads are best when they're relevant—advertisers prefer them and we think you'll like them more too. So, we use some of the information we learn about you to try and select the right ads at the right time. For example, if you've clicked on a bunch of ads for video games, we might keep those ads coming! But we also use your information to avoid showing you ads you probably won't like. For example, if a ticketing site tells us you've already bought tickets for a movie – or if you bought them through Snapchat – we can stop showing you ads for it. [Learn more.](#)



Snapchat Support

Discover tips and tricks, find answers to common questions, and get help!

What can we help you with?



< Privacy

Privacy Settings

Remove or Block a Friend

Access My Snapchat Data

Advertising & Interest Preferences

Learn About Our Service Providers

When does Snapchat delete Snaps and Chats?

I have a privacy question

🔔 What's New

Advertising & Interest Preferences

We want the ads you see on Snapchat to be fun, interesting, and relevant to you! To help do that, we let advertisers show you ads based on information collected outside of Snapchat and our other services. If you would prefer not to have ads shown to you based on this information, you can read more about your different options below!

Note: You'll still see ads if you disable these advertising features, but those ads may be less relevant to you. You may also continue to see ads based on the information you provide us and inferences we make based on your activity on Snapchat and our other services, like which Discover channels you watch.

Audience-Based Ads

Audience-Based Ads help advertisers show relevant ads to their desired audience.

Disclosure of legal bases for processing

Factors to consider:

- Audience/customer (organization's audience, e.g., customers/users vs. regulators)
- Complexity of analysis

Bases for using your information

Your country only allows us to use your personal information when certain conditions apply. These conditions are called “legal bases” and, at Snap, we typically rely on one of four:

- **Contract.** One reason we might use your information is because you’ve entered into an agreement with us. For example, when you buy an On-Demand Geofilter and accepted our Custom Creative Tools Terms, we need to use some of your information to collect payment and make sure we show your Geofilter to the right people at the right place and time.
- **Legitimate interest.** Another reason we might use your information is because we have—or a third party has—a legitimate interest in doing so. For example, we need to use your information to provide and improve our services, including protecting your account, delivering your Snaps, providing customer support, and helping you find friends and content we think you’ll like. Because most of our services are free, we also use some information about you to try and show you ads you’ll find interesting. An important point to understand about legitimate interest is that our interests don’t outweigh your right to privacy, so we only rely on legitimate interest when we think the way we are using your data doesn’t significantly impact your privacy or would be expected by you, or there is a compelling reason to do so. We explain our legitimate business reasons for using your information in more detail [here](#).
- **Consent.** In some cases we’ll ask for consent to use your information for specific purposes. If we do, we’ll make sure you can revoke your consent in our services or through your device permissions. Even if we’re not relying on consent to use your information, we may ask you for permission to access data like contacts and location.

- **Legitimate interest.** Another reason we might use your information is because we have—or a third party has—a legitimate interest in doing so. For example, we need to use your information to provide and improve our services, including protecting your account, delivering your Snaps, providing customer support, and helping you find friends and content we think you'll like. Because most of our services are free, we also use some information about you to try and show you ads you'll find interesting. An important point to understand about legitimate interest is that our interests don't outweigh your right to privacy, so we only rely on legitimate interest when we think the way we are using your data doesn't significantly impact your privacy or would be expected by you, or there is a compelling reason to do so. We explain our legitimate business reasons for using your information in more detail [here](#).

Determining legal basis for processing

Factors to consider:

- Data subjects, e.g., age of data subjects
- Sensitivity of data
- Purposes of processing

User Spec Template [v3]

Instructions: Parts of this document are underlined or indented. The indented text explains key privacy concepts that you should consider when designing your feature. Addressing these concepts in your designs will ease the product review process. Underlines are reserved for instructions about how to use this Quip. If you've read these instructions and still need help, contact [your product counsel](#).

Feature Overview

This is a one or two sentence description of the feature. If you can't describe this feature in two sentences, consider splitting the feature into more specs.

Feature Goals

1. [Goal 1]

a. Justification:

Summary

***Privacy Consideration:** Will people understand how this feature collects and uses their data? If not, can additional transparency be provided in the user flow, in our [privacy center](#), or elsewhere? Consider including just-in-time notices and iconography as you develop User Stories to aid understanding.*

This is an optional paragraph long description of what the user can do. It's different than the feature overview in that it's a bit more descriptive and does not talk about any business implications. It's useful for long user stories.

[ADD FLOW DIAGRAM]

Privacy Considerations:

- 1) Will people understand who can view the information they share?*
- 2) If user consent is required to process data for this feature, consider excluding this processing for children (ages 13-15).*
- 3) If this feature collects location data or information from the user's contact book, you must ensure we have asked the user for consent.*

What user data is needed for this product or feature?	How will the data be used?	How long is the retention period?	Will the data be deleted, de-identified, or aggregated after the retention period elapses?	Where will the data be stored?	Will this data be shared outside of Snap?
▼		▼	▼	▼	▼
▼		▼	▼	▼	▼
▼		▼	▼	▼	▼
▼		▼	▼	▼	▼

Will the user be able to view this data? With few exceptions, individuals have a right to access the data we have stored about them. Typically, this data should be available in the app (e.g. in settings) or via [Download My Data](#). If this data can't be made available to individuals, work with your product counsel to see if an exception applies. If new data will be added to Download My Data, the Design or Engineering Owner must contact dmd-request@snap.com as soon as possible to begin the integration process.

Will the user be able to edit or delete this data? As a general rule, individuals have the right to correct or request we delete their data. When possible, you should provide users with the ability to edit or delete data in the app and, in most cases, ensure that the data is deleted when the user account is deleted.

Privacy Review

Security and Legal must complete this section before any feature is released. Once completed, any changes to the feature will require additional review. If Legal believes a Privacy Impact Assessment (PIA) or Legitimate Interest Assessment (LIA) is required for this feature, please [submit a request](#) as soon as possible.

Reviewer	Date	Status	PIA required?	LIA required?	DMD?	Notes
Legal Reviewer		▼	▼	▼	▼	
Eng Reviewer		▼	n/a	n/a	n/a	

PIAs are required for high risk data processing activities. Processing of high risk data categories (e.g. biometric data and children's data) and long retention periods are indicators that a PIA may be required.

LIAs are required if we rely on legitimate interest as a ground for processing and the processing does not fall within existing processing activities.

Legitimate Interest Assessment

Outline

Processing Activity

Data

Purpose

Necessity

Balancing Considerations

Status

Legitimate Interest Assessment Questionnaire

← BACK

Processing Activity

***Required** One-sentence description of the processing activity under review:

Outline

Processing Activity

Data

Purpose

Necessity

Balancing Considerations

Status

***Required Detailed description of the processing activity:**

Data

***Required Data used for this processing activity:**

***Required Will data about children under the age of 16 be processed?**

☒ Yes

☐ No

Warning — possible high-risk issue

The GDPR requires Snap to give particular weight to protecting children's data. This is particularly true when data will be used for the purposes of marketing or creating user profiles.

Identify any risks particular to children and describe any extra measures or safeguards developed to mitigate potential harm to children.

***Required** Will sensitive data be processed?

☒ Yes

☐ No

Warning — possible critical-risk issue

Snap likely cannot rely on legitimate interest as the basis for processing sensitive data.

***Required** Would the individual reasonably expect their data to be processed in this way?

☐ Yes

☒ No

Warning — possible critical-risk issue

If the individual would not reasonably expect this processing activity, their interests are more likely to override Snap's legitimate interests.



Centre for
Information
Policy
Leadership
Hunton Andrews Kurth LLP



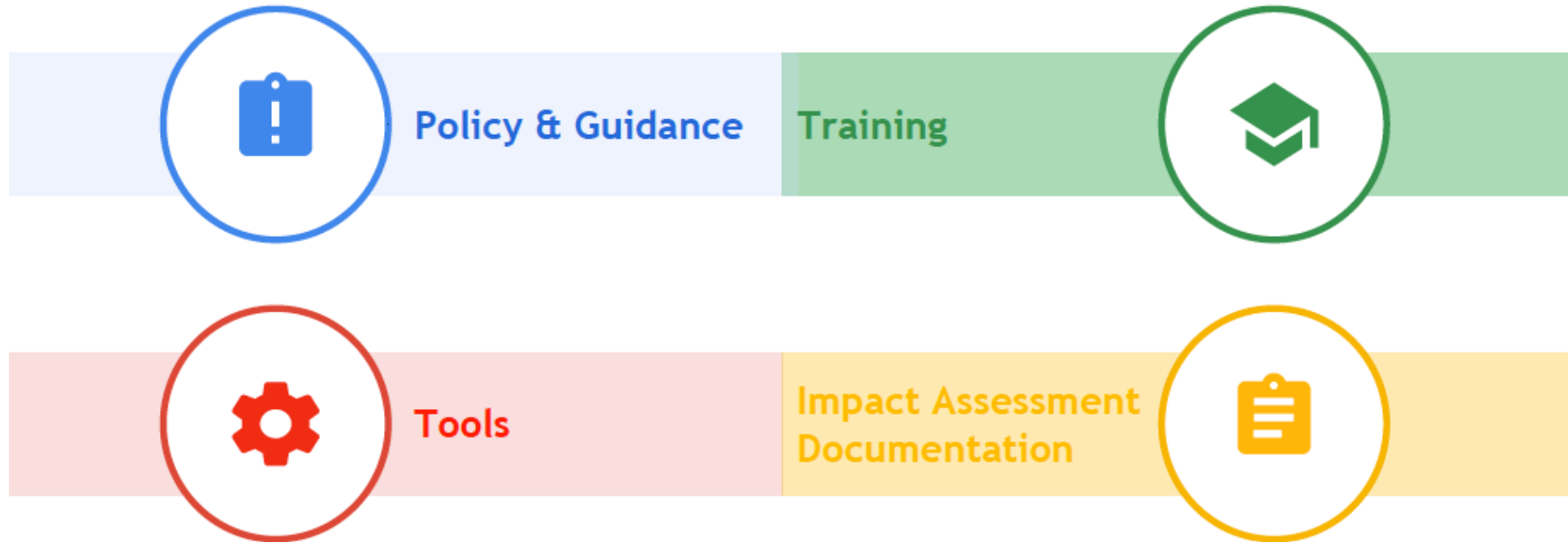
PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

Session III

Data Protection by Design and Data Protection Impact Assessment Case Study

- ❖ Huey Tan, Senior Privacy Counsel, Apple
- ❖ Keith Enright, Legal Director, Privacy, Google

Overview - Privacy by design





Part A: Privacy @ Google



Privacy Training

Content is tailored to job ladders — product designers and engineers get custom content

Our training is optimized to have the biggest possible impact across the company, ensuring that best practices are taught and reinforced year after year.

Engineers and product managers get special, in-depth training during on-boarding

More than half of our employees are enrolled in this special, in-depth training within three months of hire.



Privacy Reviews

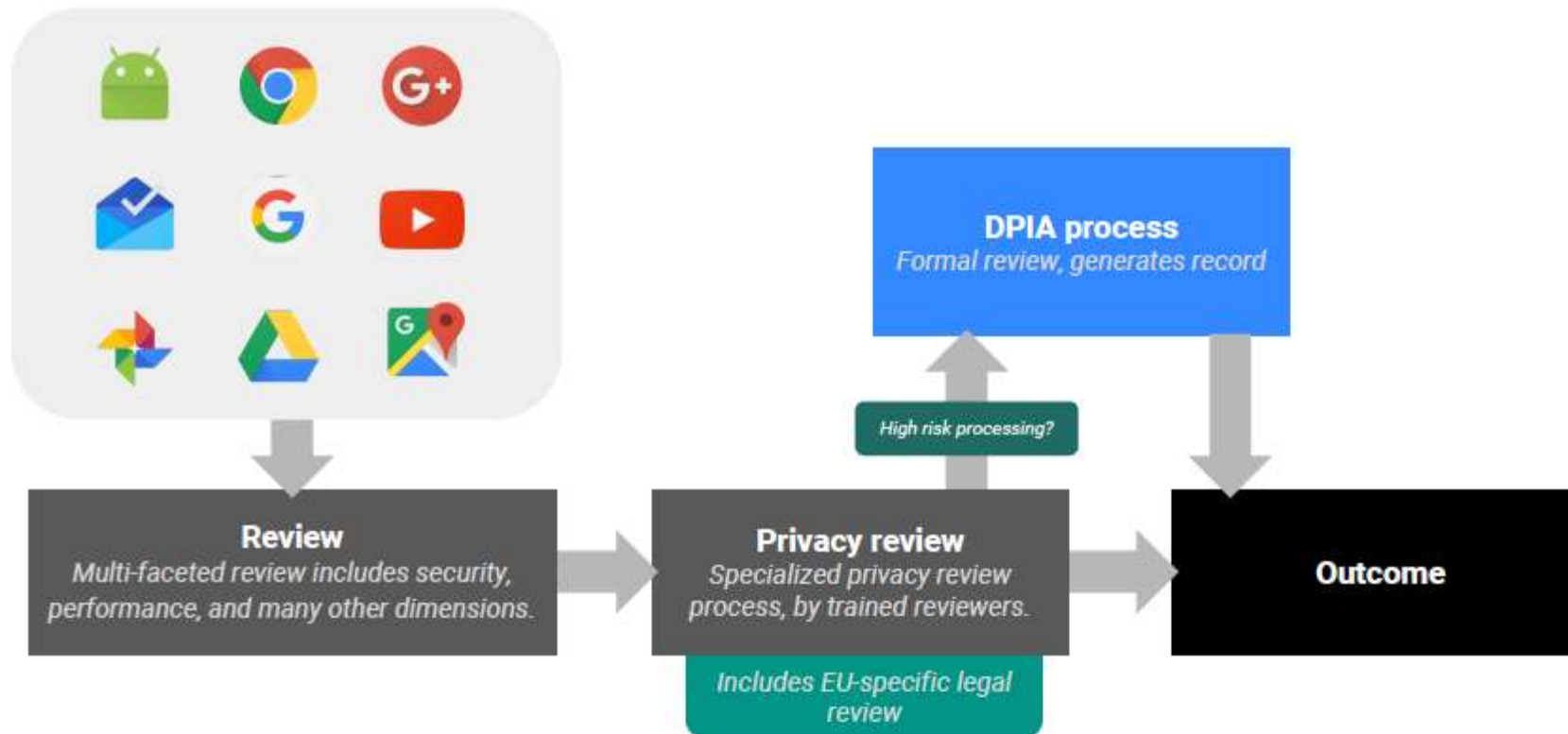
Privacy Working Groups (PWGs) partner with engineering teams throughout product development and conduct final launch reviews.

Each PWG team focuses on a product area (e.g. Chrome or Maps) or a horizontal privacy theme (e.g. biometrics or aggregation). **PWG members are experts in their specific domains, and they get specialized legal support.**

30

Privacy Working Groups
focused on product areas and
privacy concepts.

Privacy review model: DPIA process



Data Protection Impact Assessments

We're launching a DPIA template that will be a key deliverable of the review process for High Risk processing.

DPIAs will be reviewed by privacy engineering, legal counsel, product leadership, and the DPO as **appropriate** — building upon similar reviews we do today.



Description of the processing

High risk criteria

Risk analysis and mitigation

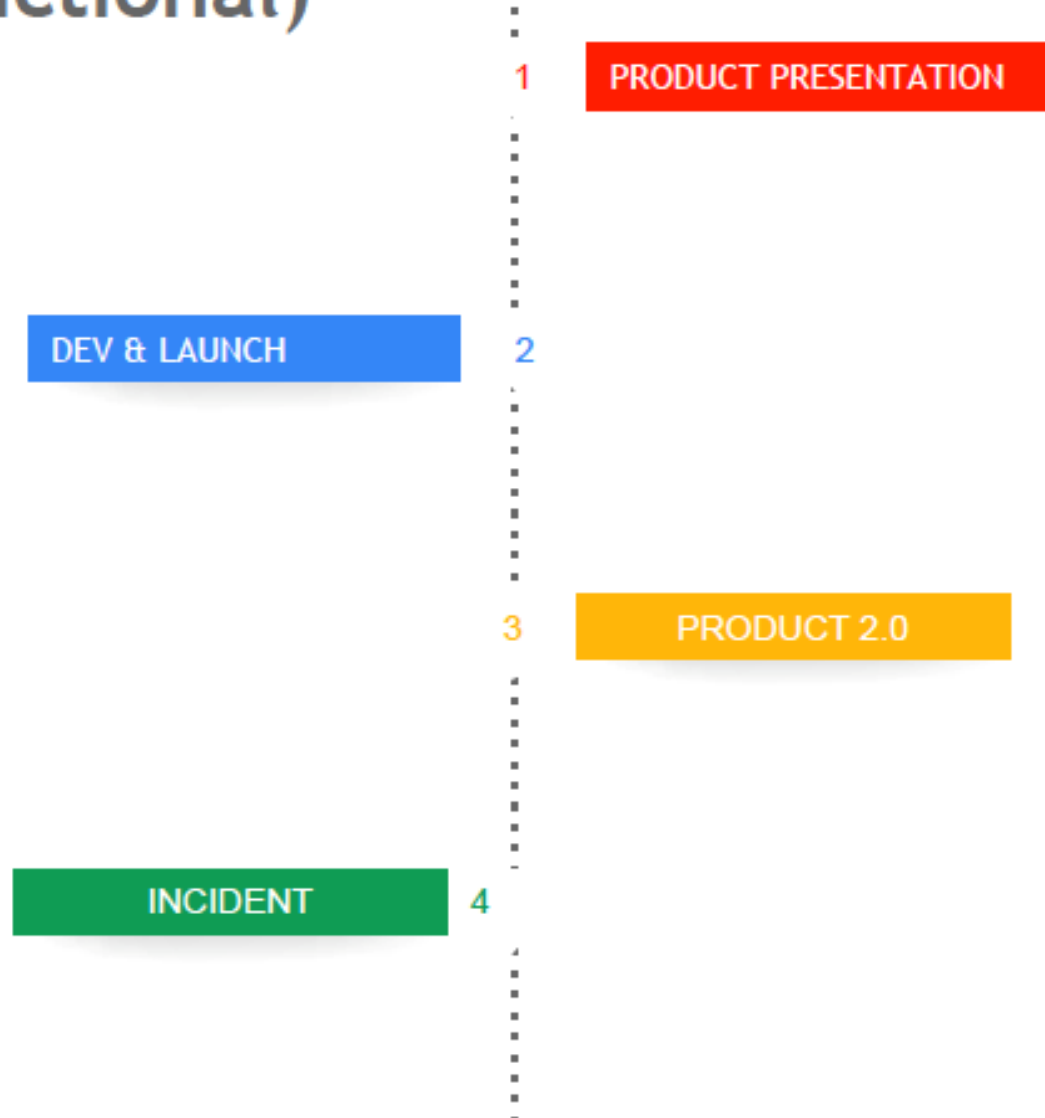
Stakeholder signoff



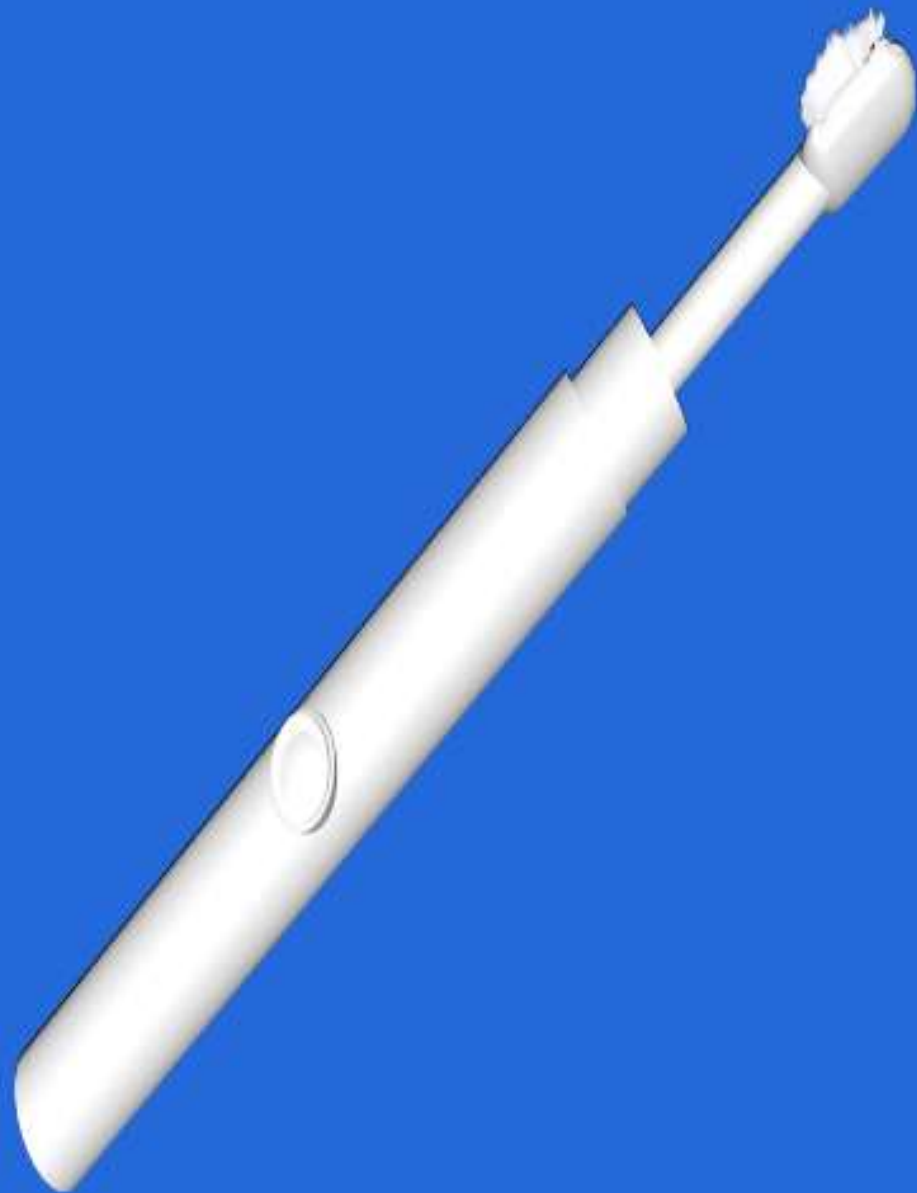
Part B: Fictional Case Study



Case study (fictional)



BRUSH.ly
(fictional)

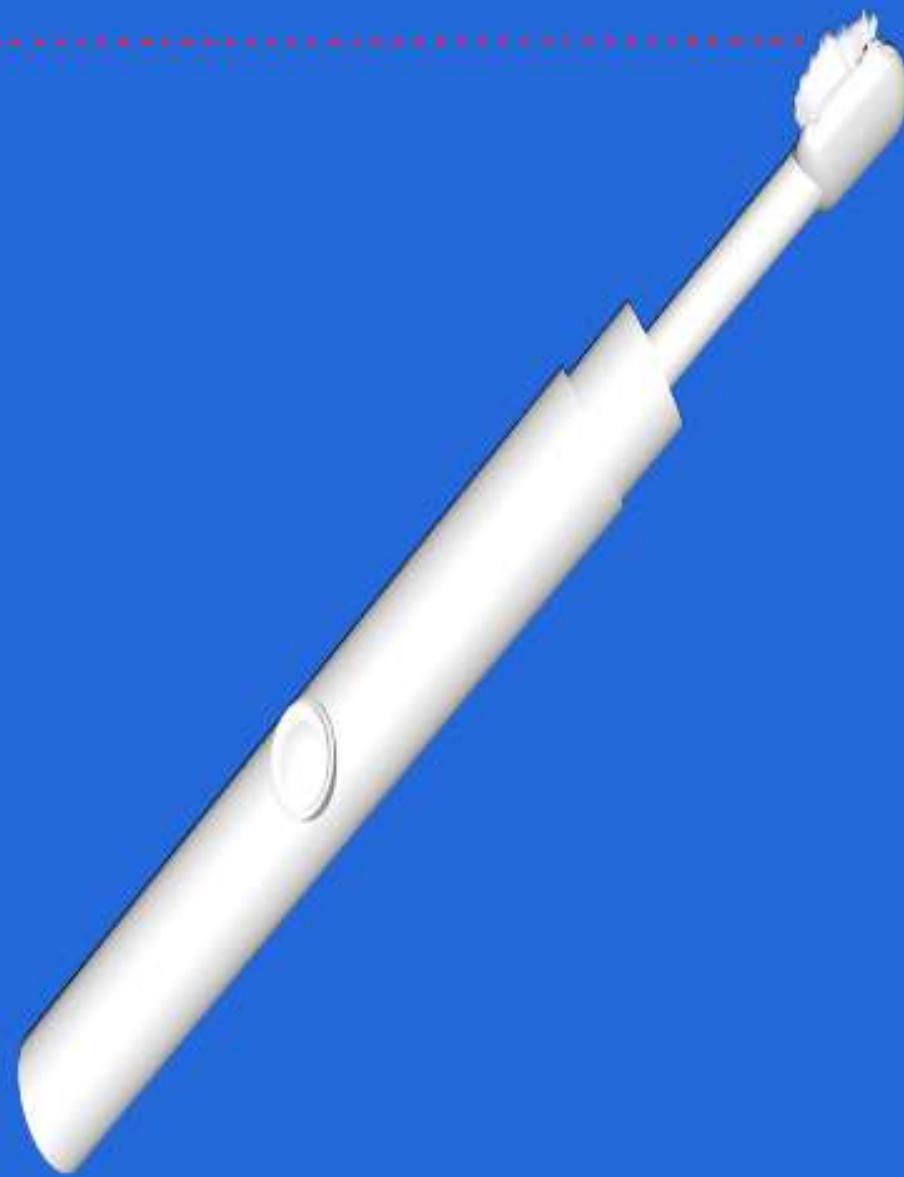


WiFi and Bluetooth enabled
to connect to phones



1

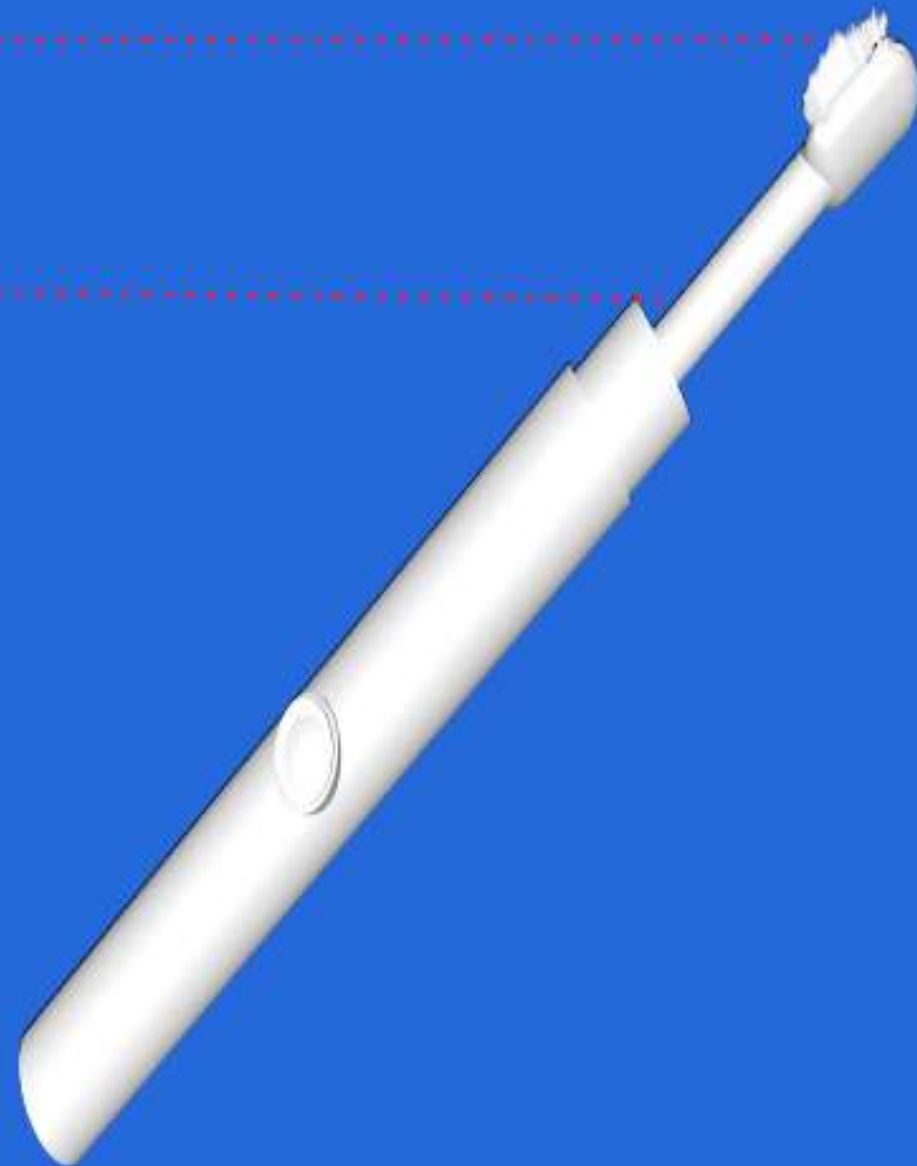
PRODUCT PRESENTATION



WiFi and Bluetooth enabled
to connect to phones



Companion mobile app to sync
with Brush.ly Account



WiFi and Bluetooth enabled
to connect to phones

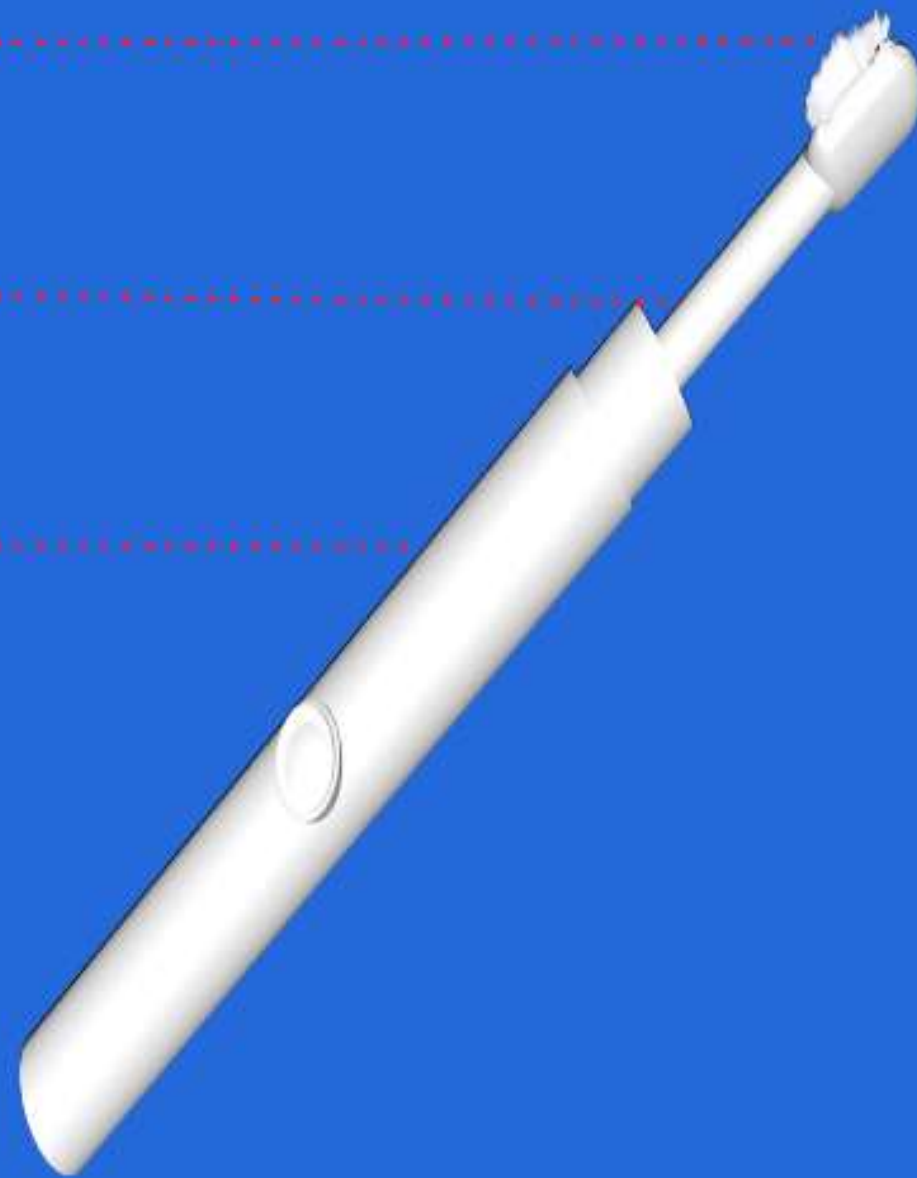


Companion mobile app to sync
with Brush.ly Account



Keeps detailed data in local storage
about:

- Brush position
- Accelerometer and gyro readings
of detailed movements
- Brushing time



WiFi and Bluetooth enabled
to connect to phones



Companion mobile app to sync
with Brush.ly Account

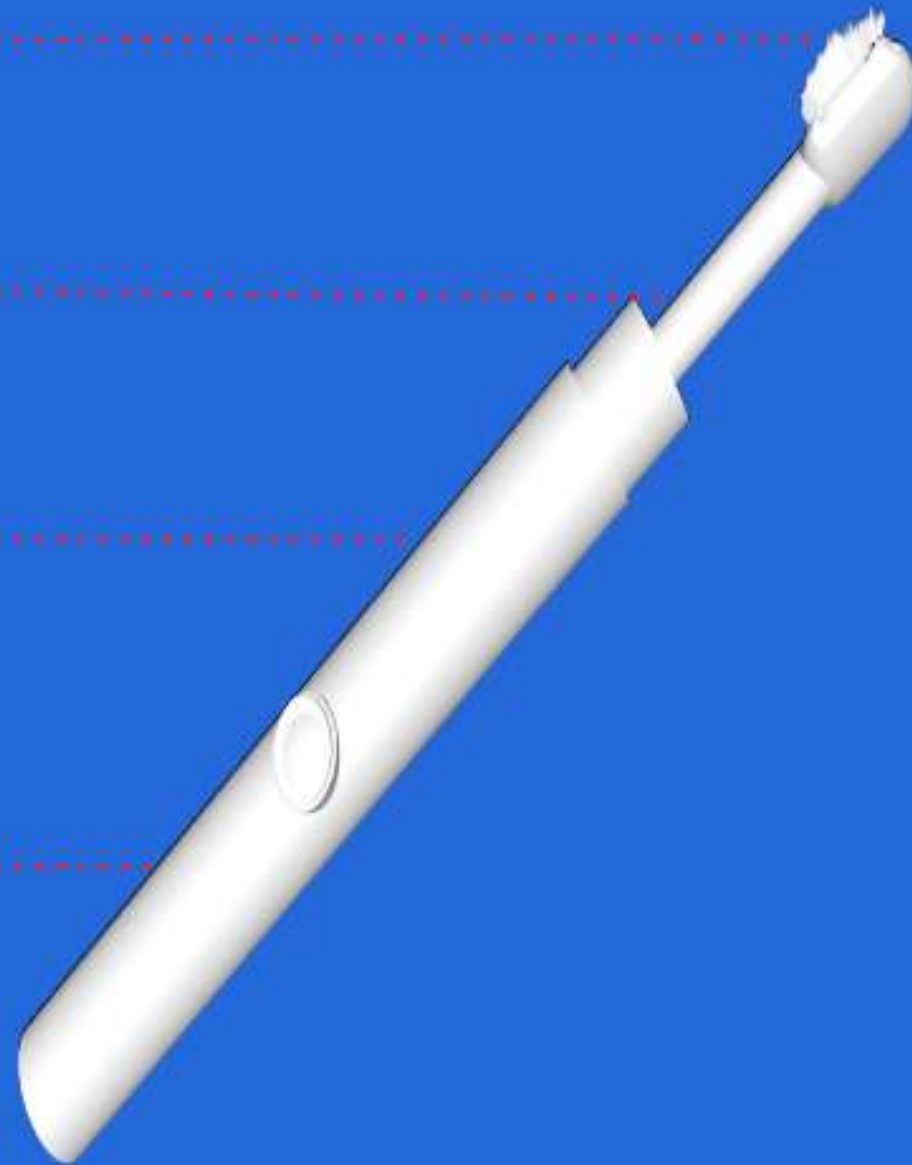


Keeps detailed data in local storage
about:

- Brush position
- Accelerometer and gyro readings
of detailed movements
- Brushing time



Small screen displays brushing
statistics



WiFi and Bluetooth enabled
to connect to phones



Companion mobile app to sync
with Brush.ly Account



Keeps detailed data in local storage
about:

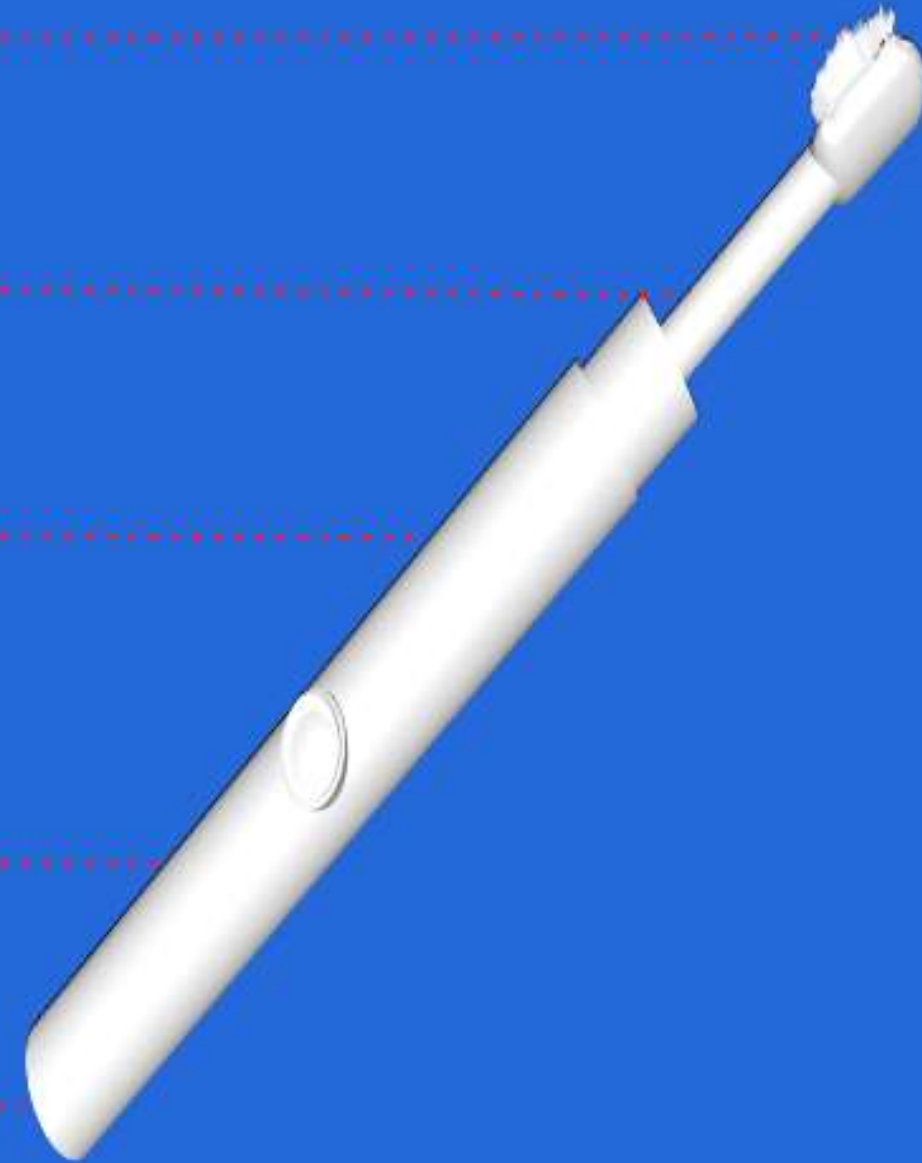
- Brush position
- Accelerometer and gyro readings
of detailed movements
- Brushing time



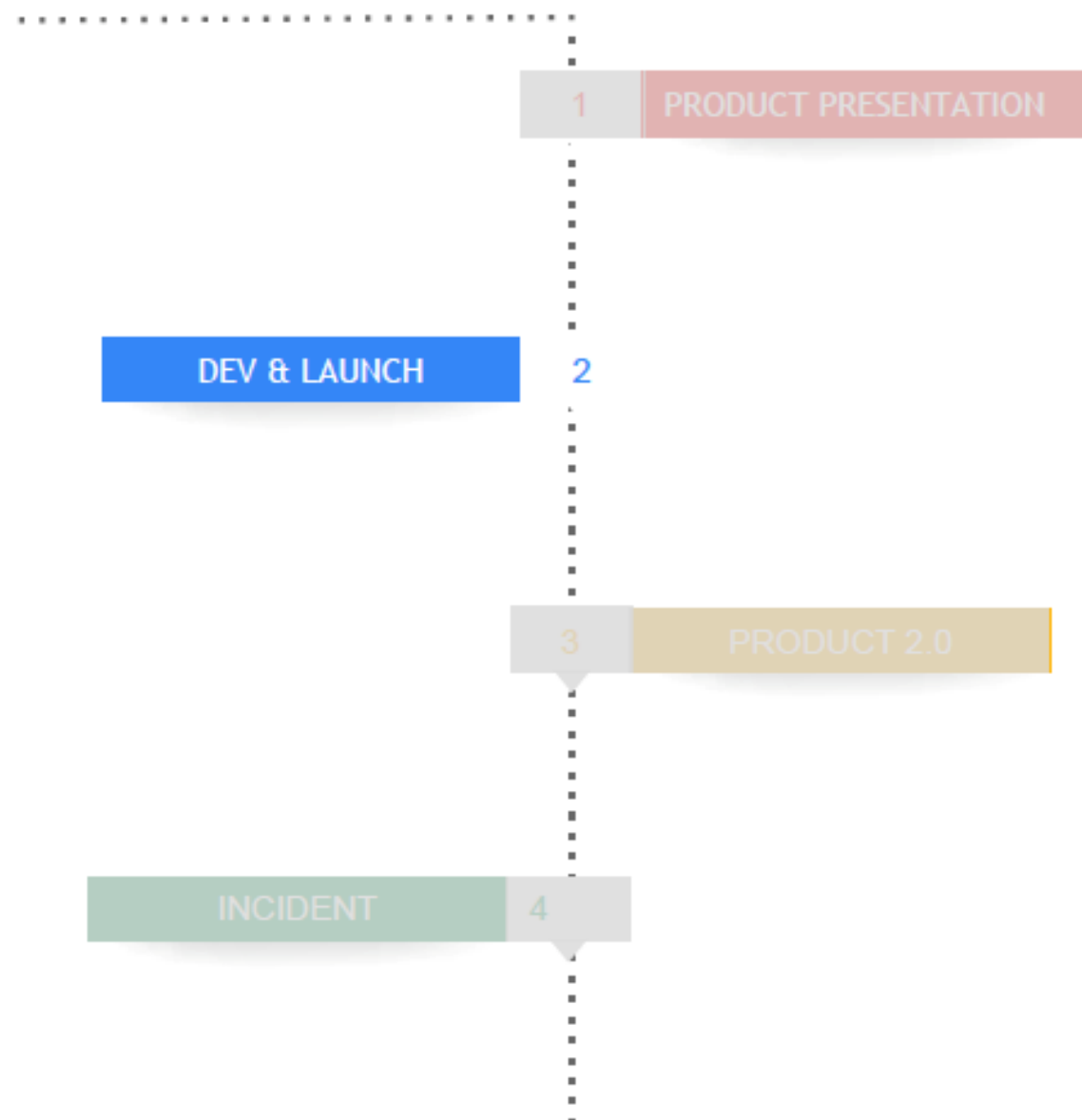
Small screen displays brushing
statistics



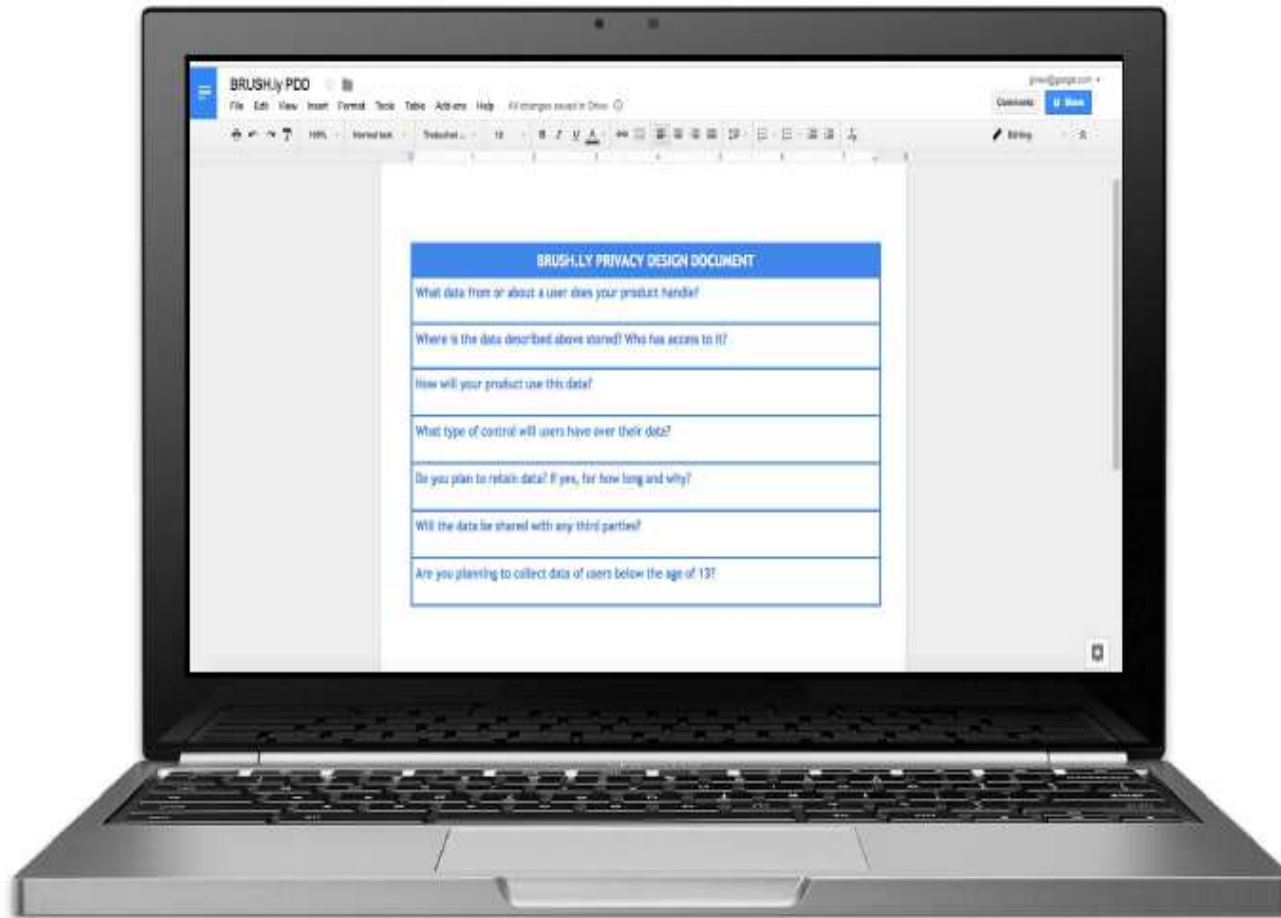
Research data will be made
available to researchers and
academics



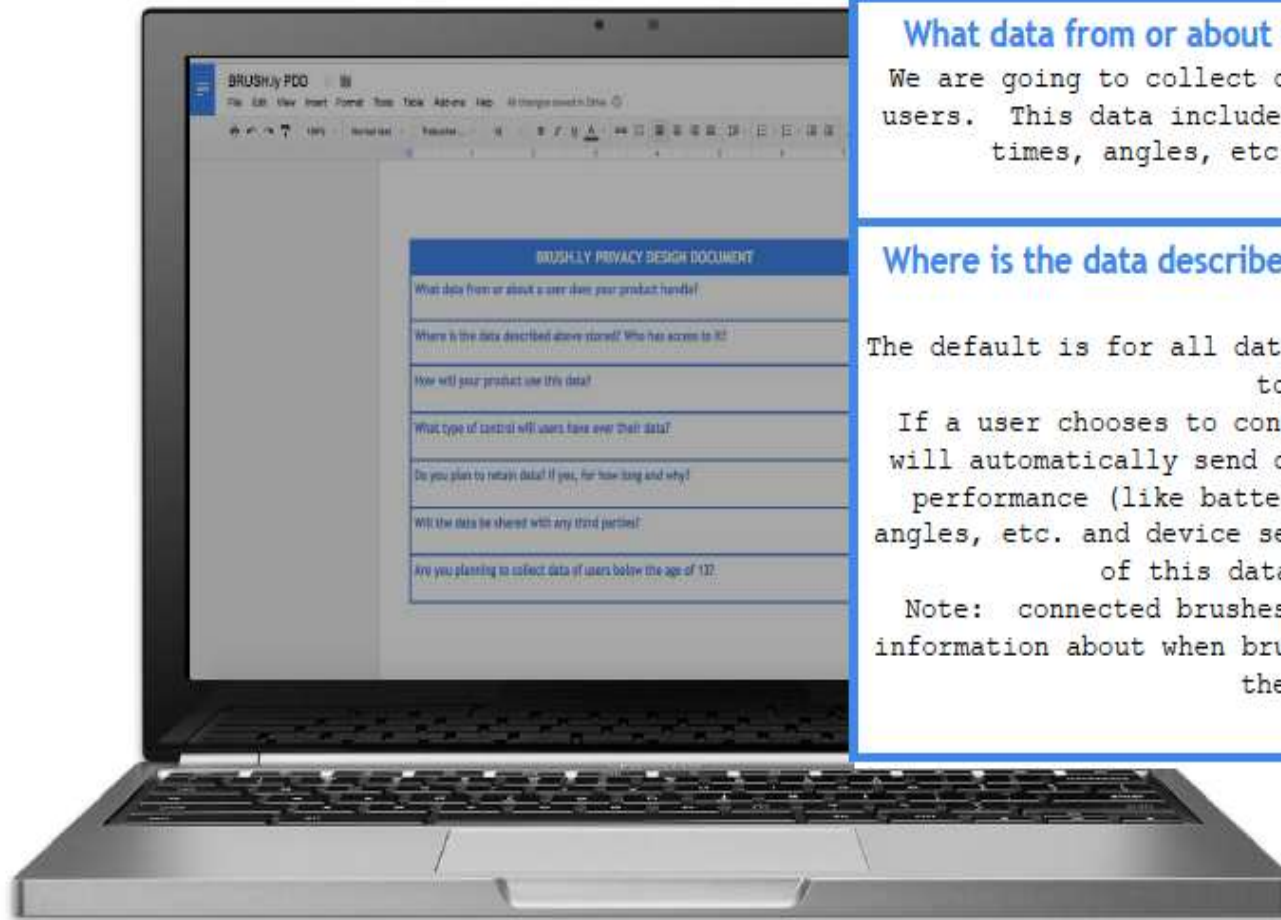
Roadmap



Privacy Design Document



Privacy Design Document



What data from or about a user does your product handle?

We are going to collect data from the toothbrush, not from users. This data includes: battery life, brushing speeds, times, angles, etc. and device serial number.

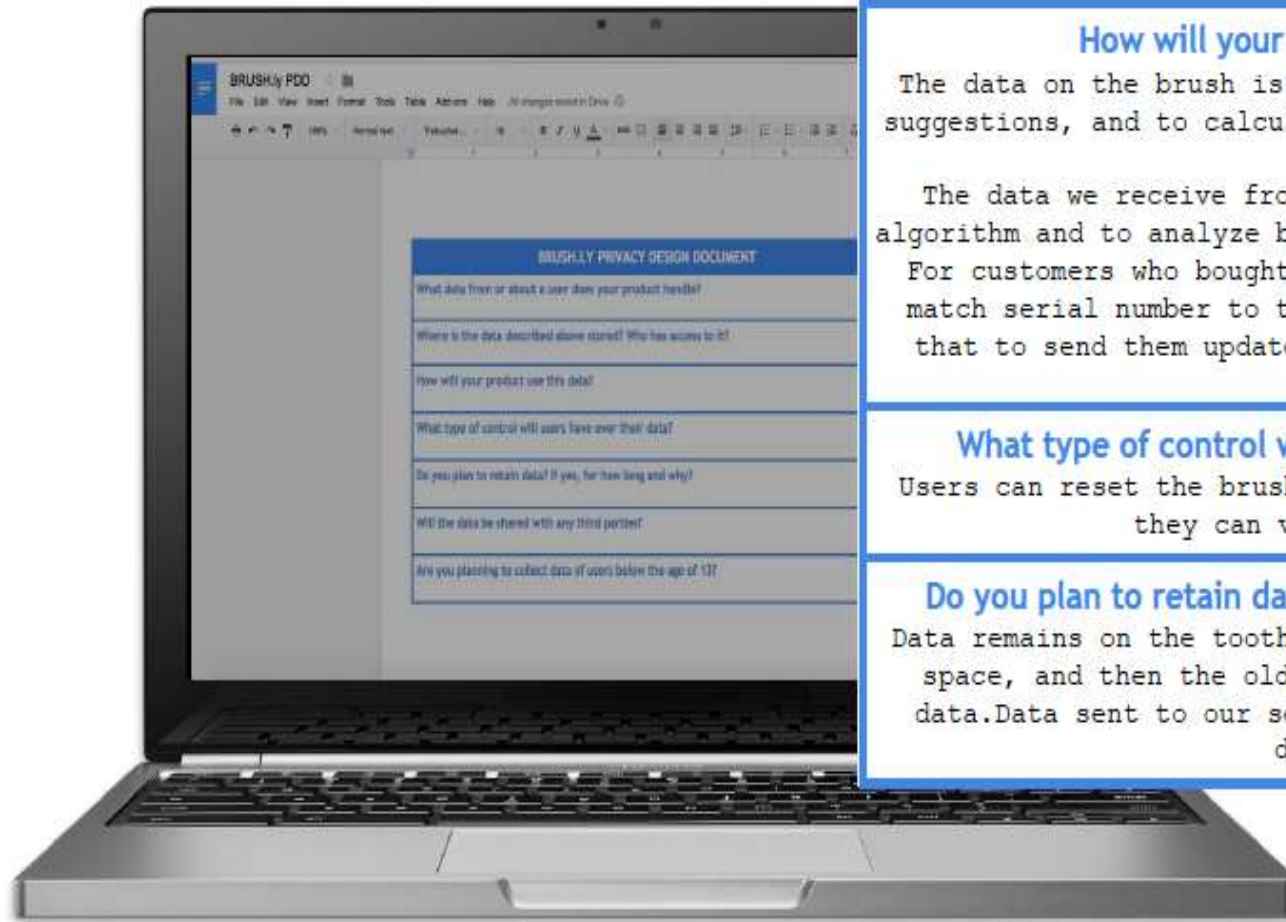
Where is the data described above stored? Who has access to it?

The default is for all data to be stored in the memory on the toothbrush.

If a user chooses to connect their brush with the app, we will automatically send data from the toothbrush about its performance (like battery life, brushing speeds, times, angles, etc. and device serial number) to our servers. None of this data is tied to a user.

Note: connected brushes can receive updates, and we log information about when brushes get updates and which updates they receive.

Privacy Design Document



How will your product use this data?

The data on the brush is used to provide the user tips and suggestions, and to calculate performance scores to show the user.

The data we receive from brushes is used to improve our algorithm and to analyze bugs or other issues with the brush. For customers who bought brushes directly from us, we can match serial number to their purchase information and use that to send them updates on the product and promotions.

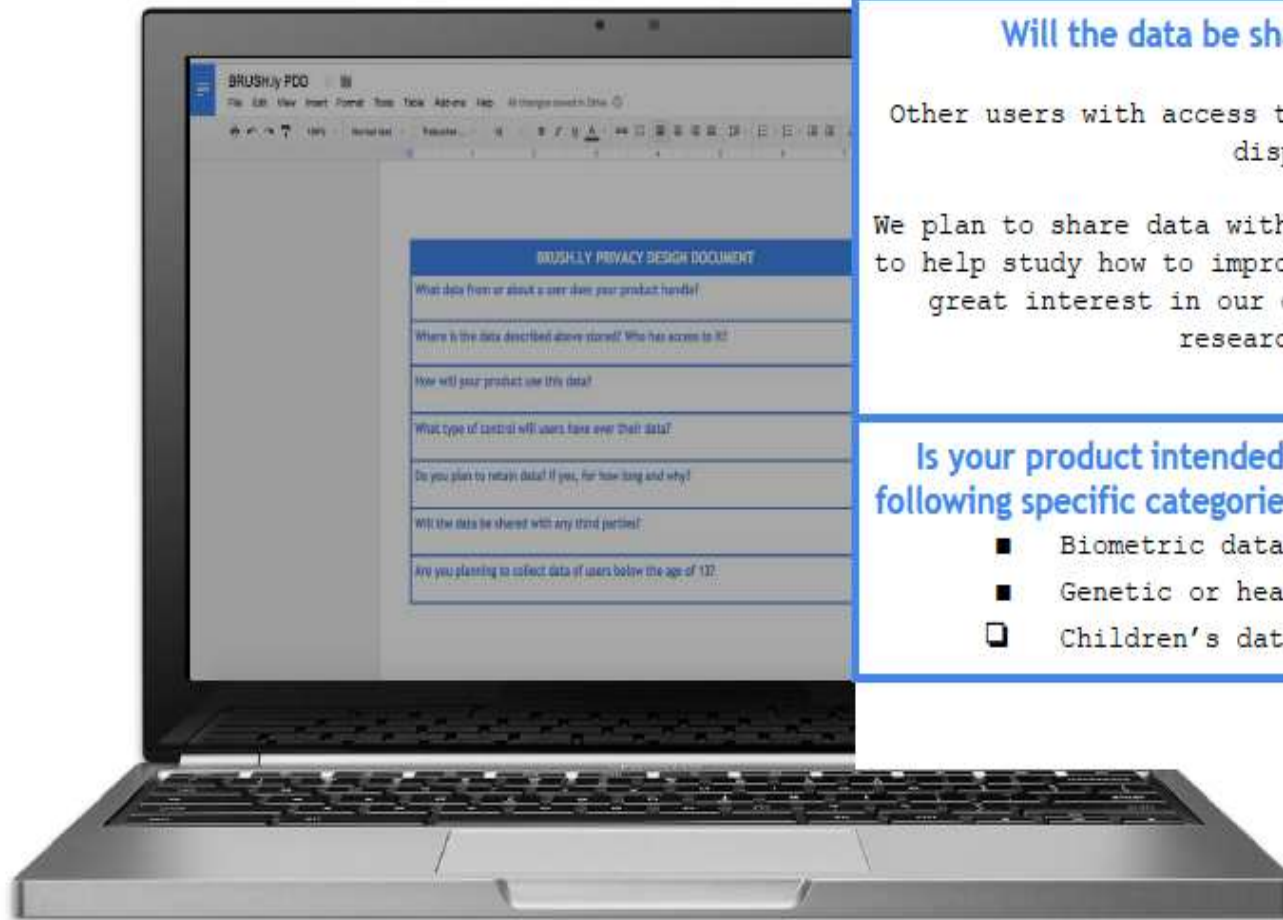
What type of control will users have over their data?

Users can reset the brush if they want to remove data, and they can view it in the app.

Do you plan to retain data? If yes, for how long and why?

Data remains on the toothbrush until the memory runs out of space, and then the oldest data is overwritten with new data. Data sent to our servers is kept until we decide to delete it.

Privacy Design Document



Will the data be shared with any third parties?

Other users with access to the brush could view data on the display screen.

We plan to share data with medical researchers and academics, to help study how to improve dental health. We know there is great interest in our data and have heard from several research labs already.

Is your product intended to collect and process any of the following specific categories of data (check all that may apply):

- ☒ Biometric data (e.g., fingerprints)
- ☒ Genetic or health information;
- ☐ Children's data

What does....

...a User Trust expert say about best practices?

- Transparency and control
- Communication about privacy
- Being trustworthy

...an Eng Expert say about best practices?

- Encryption
- Multi-users
- Hardware privacy vulnerabilities
- Sharing for research

...a Privacy Lawyer say about legal obligations?

- Notice & Consent
- Retention
- Accuracy in settings

Brush.ly Fact Sheet

WiFi and Bluetooth enabled to connect to phones



Companion mobile app to sync with Brush.ly Account



Keeps detailed data in local storage about:

- Brush position
- Accelerometer and gyro readings of detailed movements
- Brushing time



Small screen displays brushing statistics

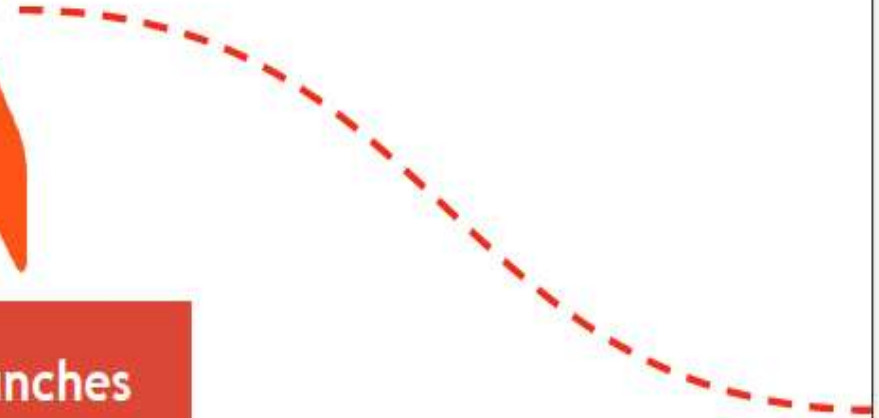


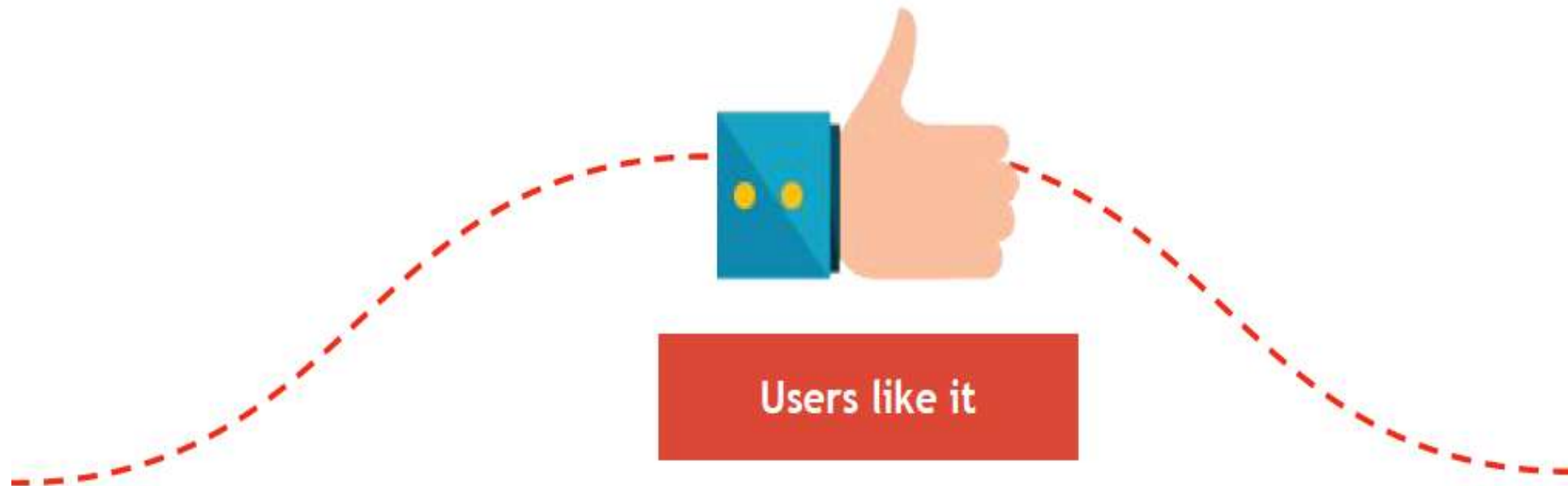
Research data will be made available to researchers and academics





Brush.ly launches



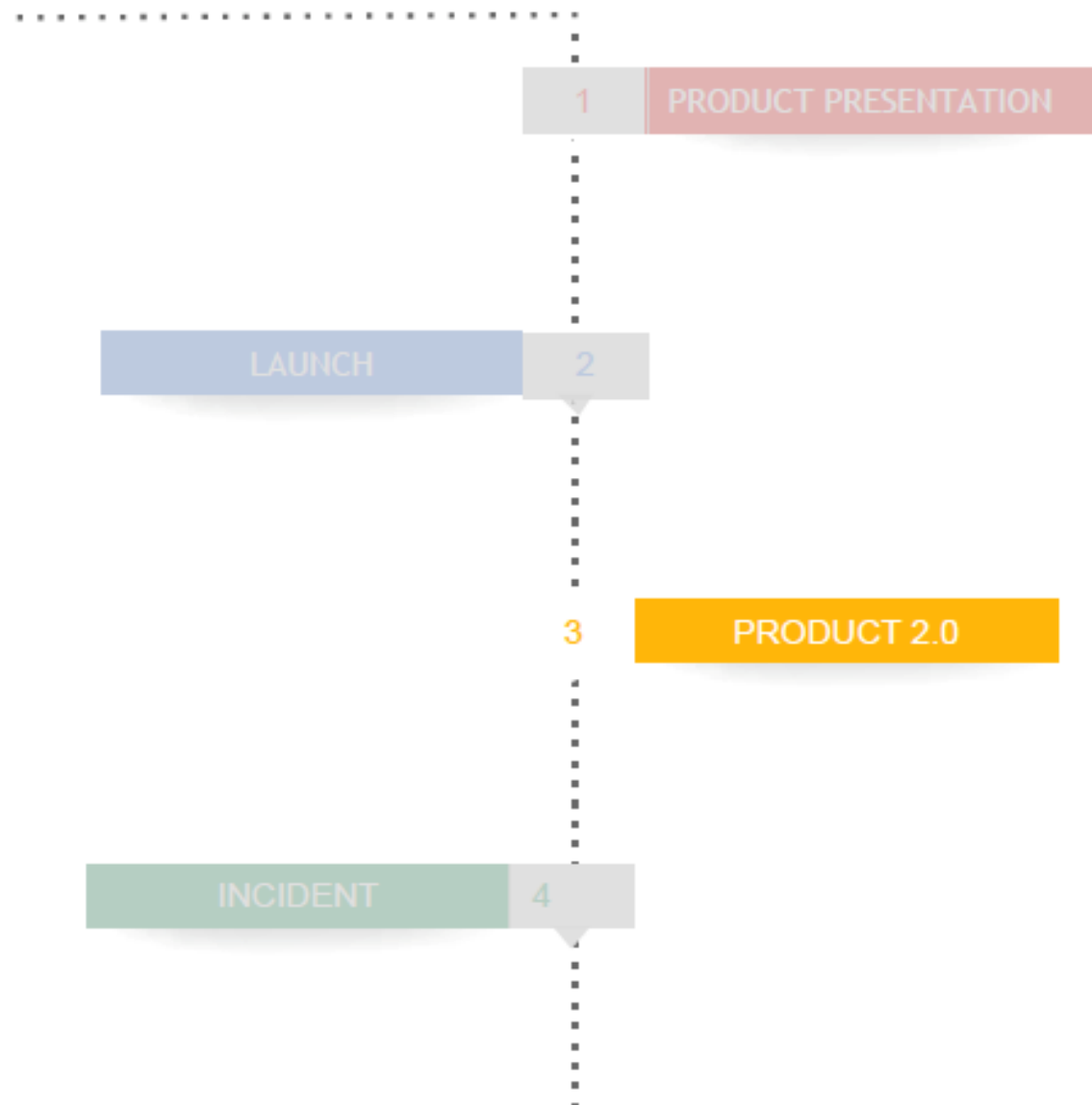


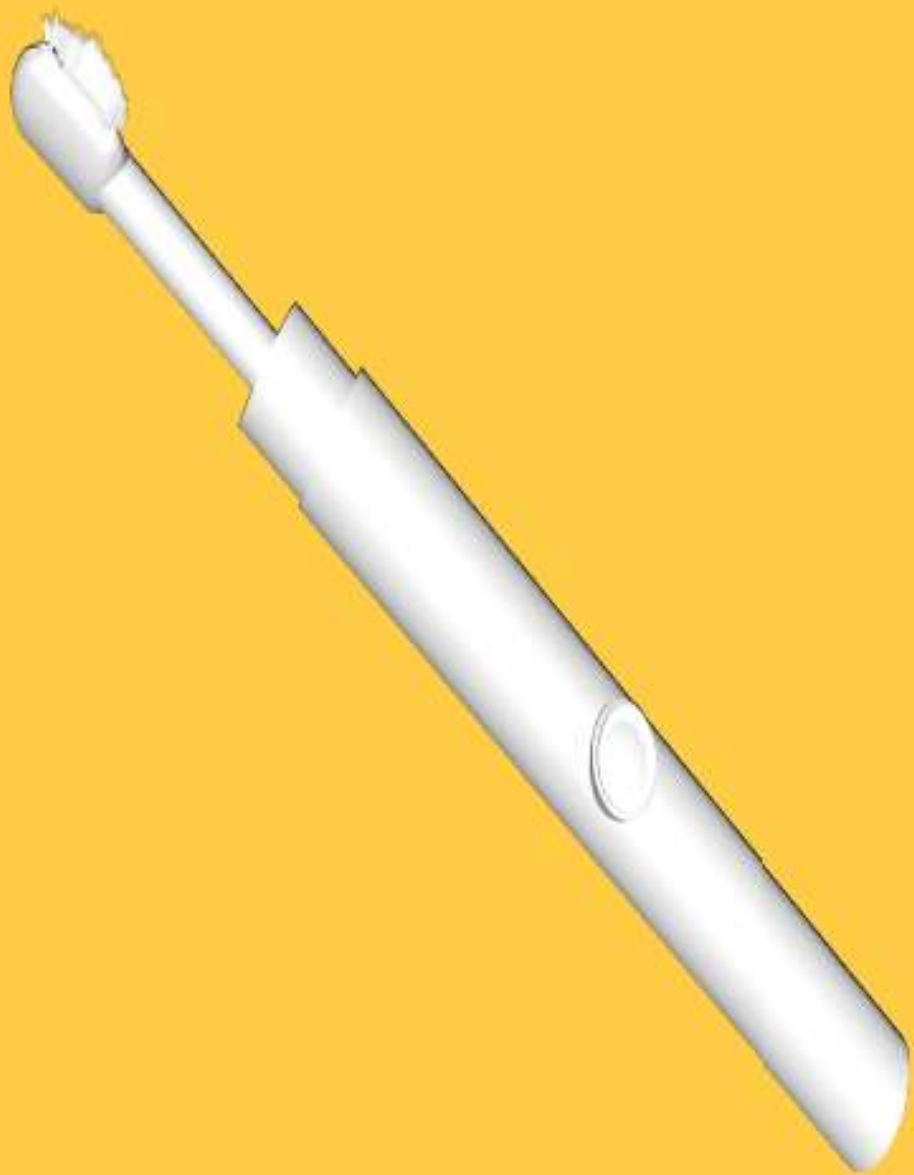
Users like it



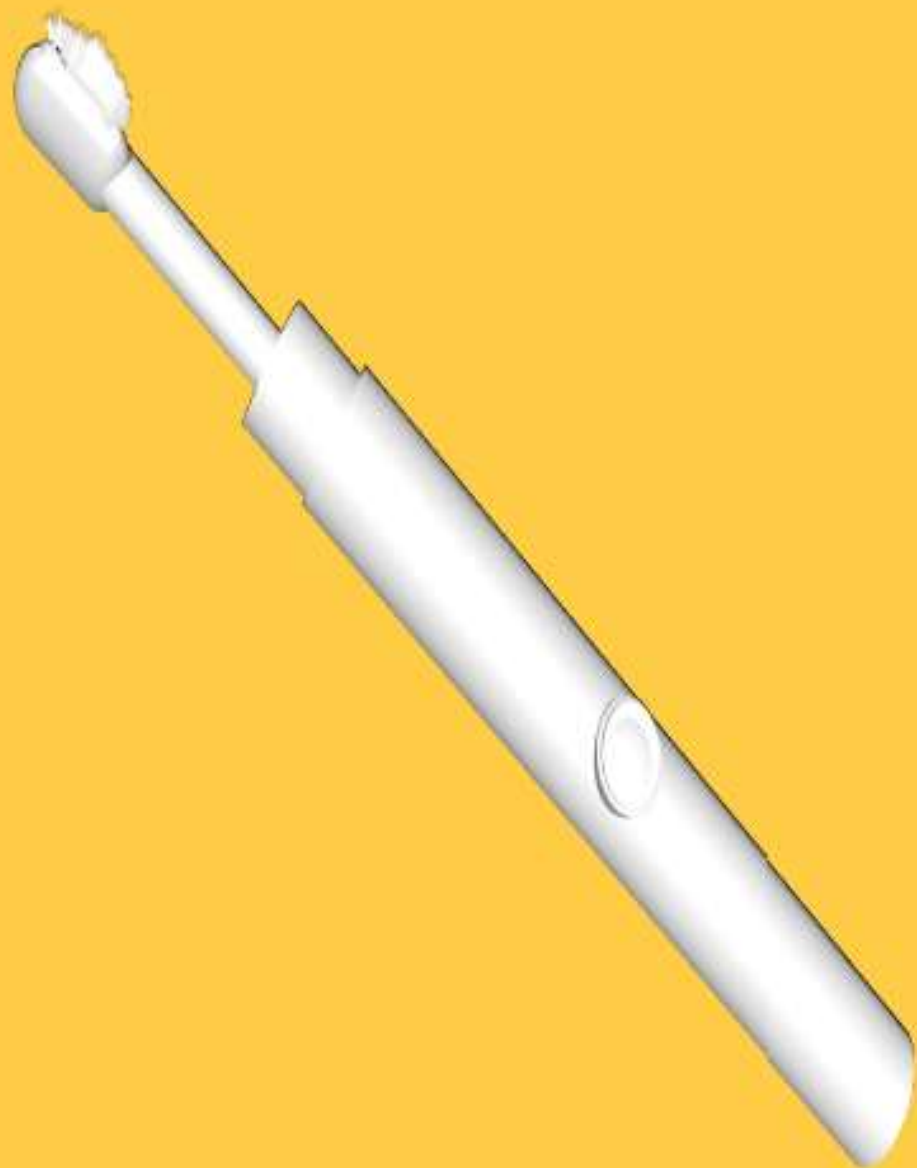
...3 months later...

Roadmap



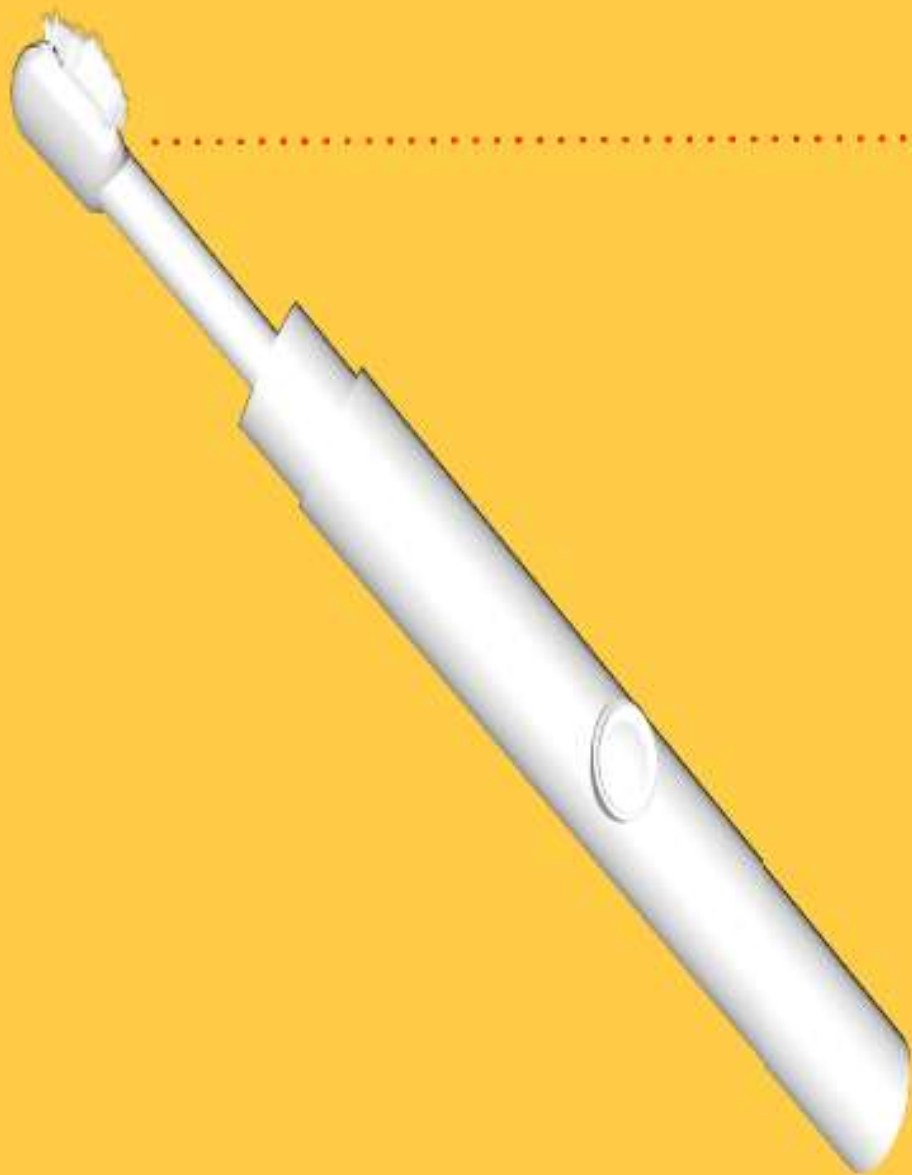


Super Smile
Brush.ly?
(fictional)



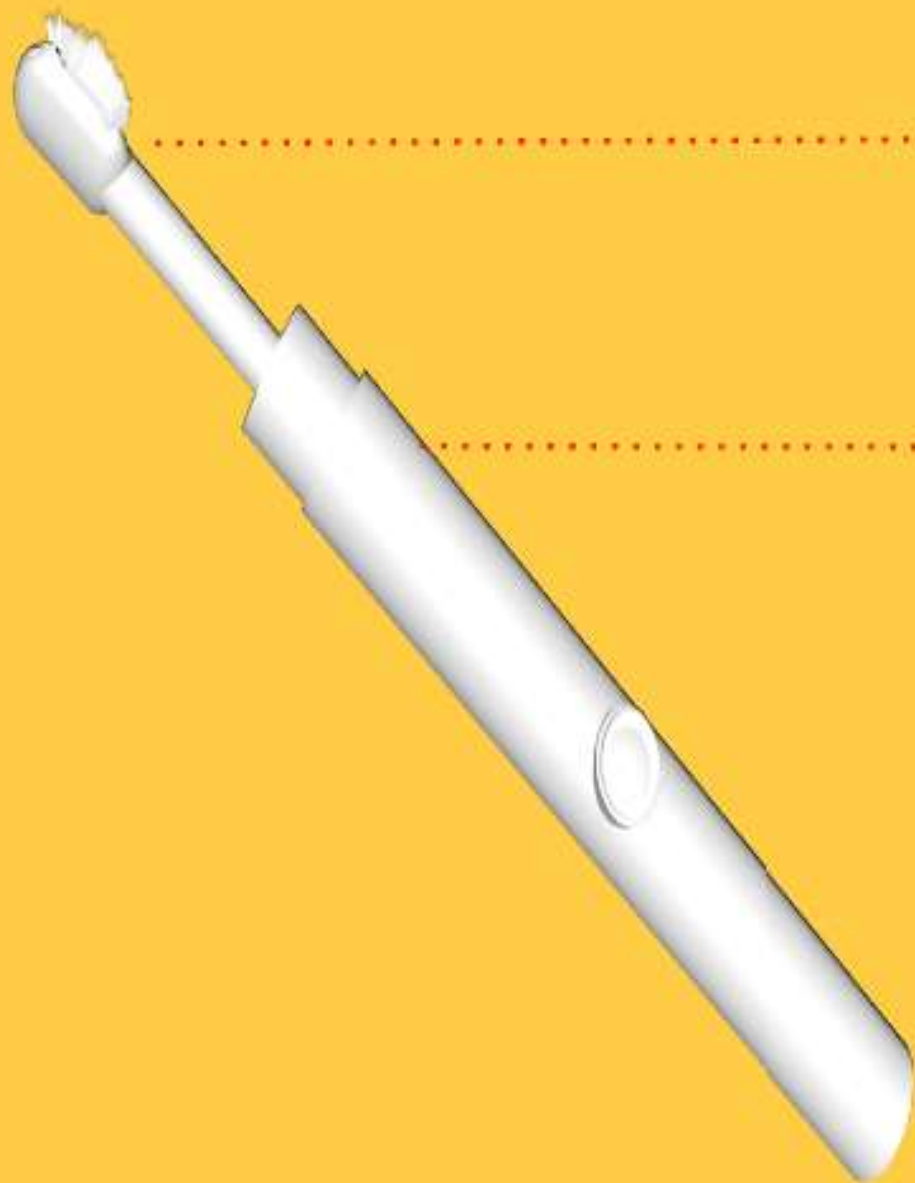
It will include all features of
Brush.ly





Sensors on brush can detect the presence of gum disease

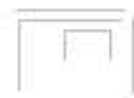


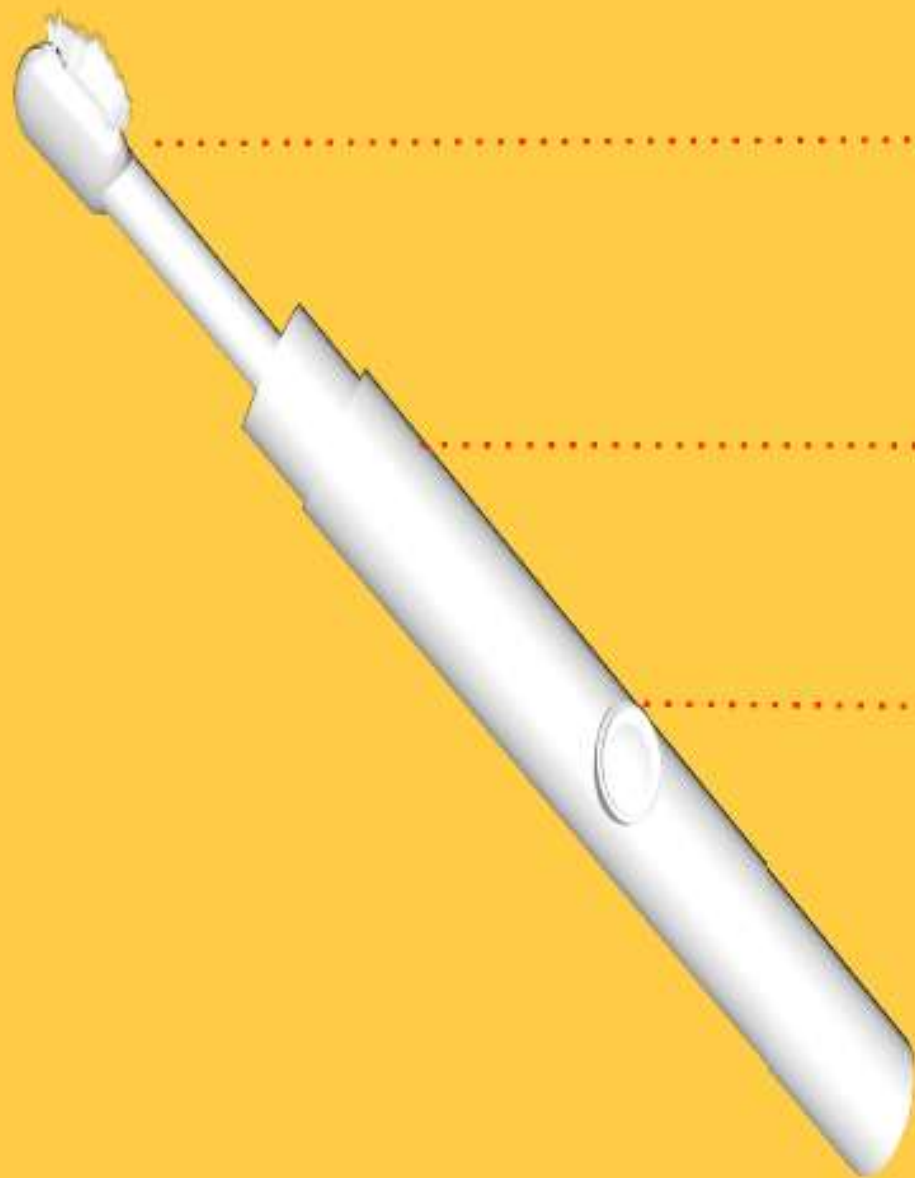


Sensors on brush can detect the presence of gum disease



GPS-enabled to detect user's location when using Brush.ly

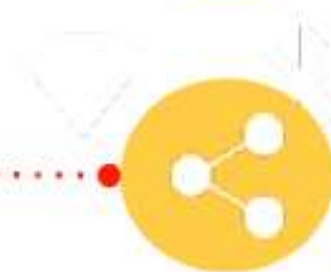




Sensors on brush can detect the presence of gum disease

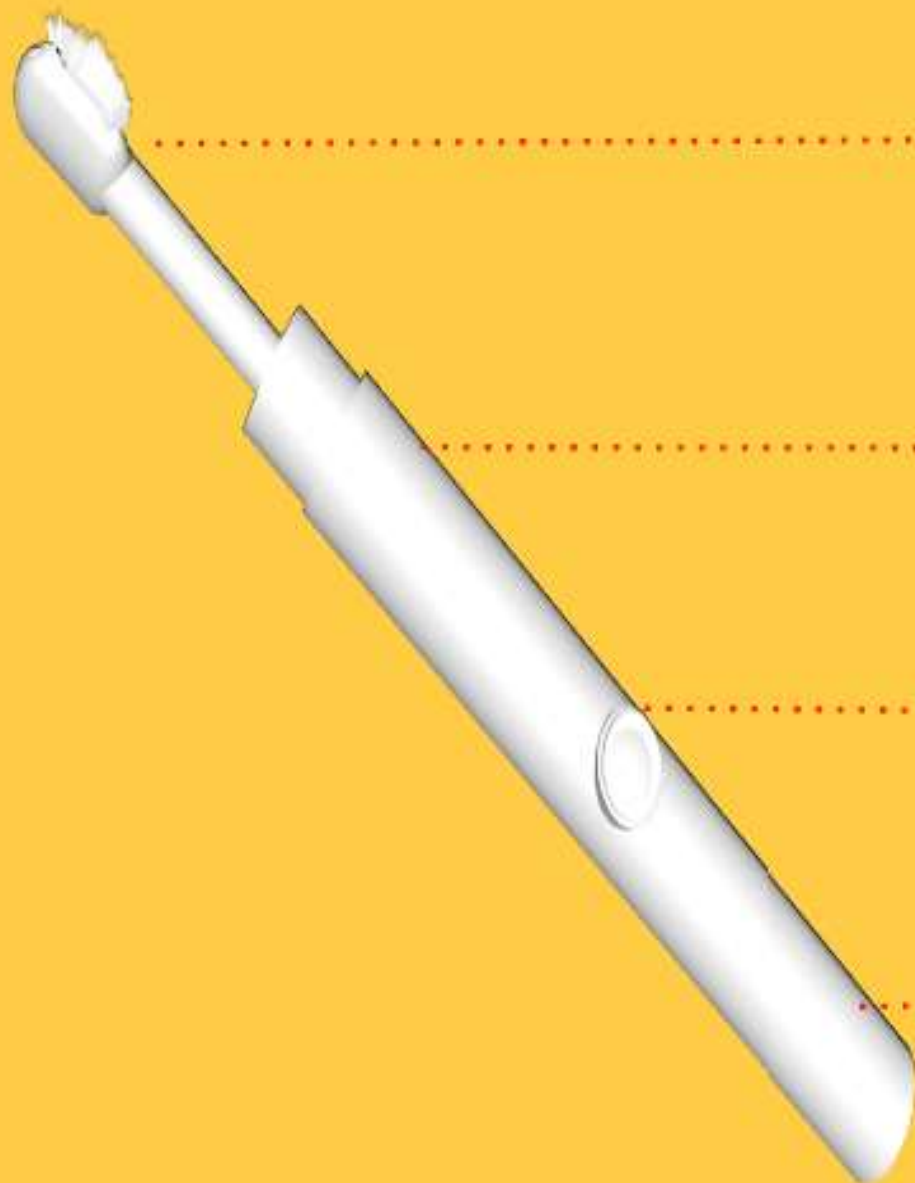


GPS-enabled to detect user's location when using Brush.ly



Users will be able to share their info with their dentists. Dentists can install a Brush.ly App for Doctors





Sensors on brush can detect the presence of gum disease



GPS-enabled to detect user's location when using Brush.ly



Users will be able to share their info with their dentists. Dentists can install a Brush.ly App for Doctors



Special features for kids

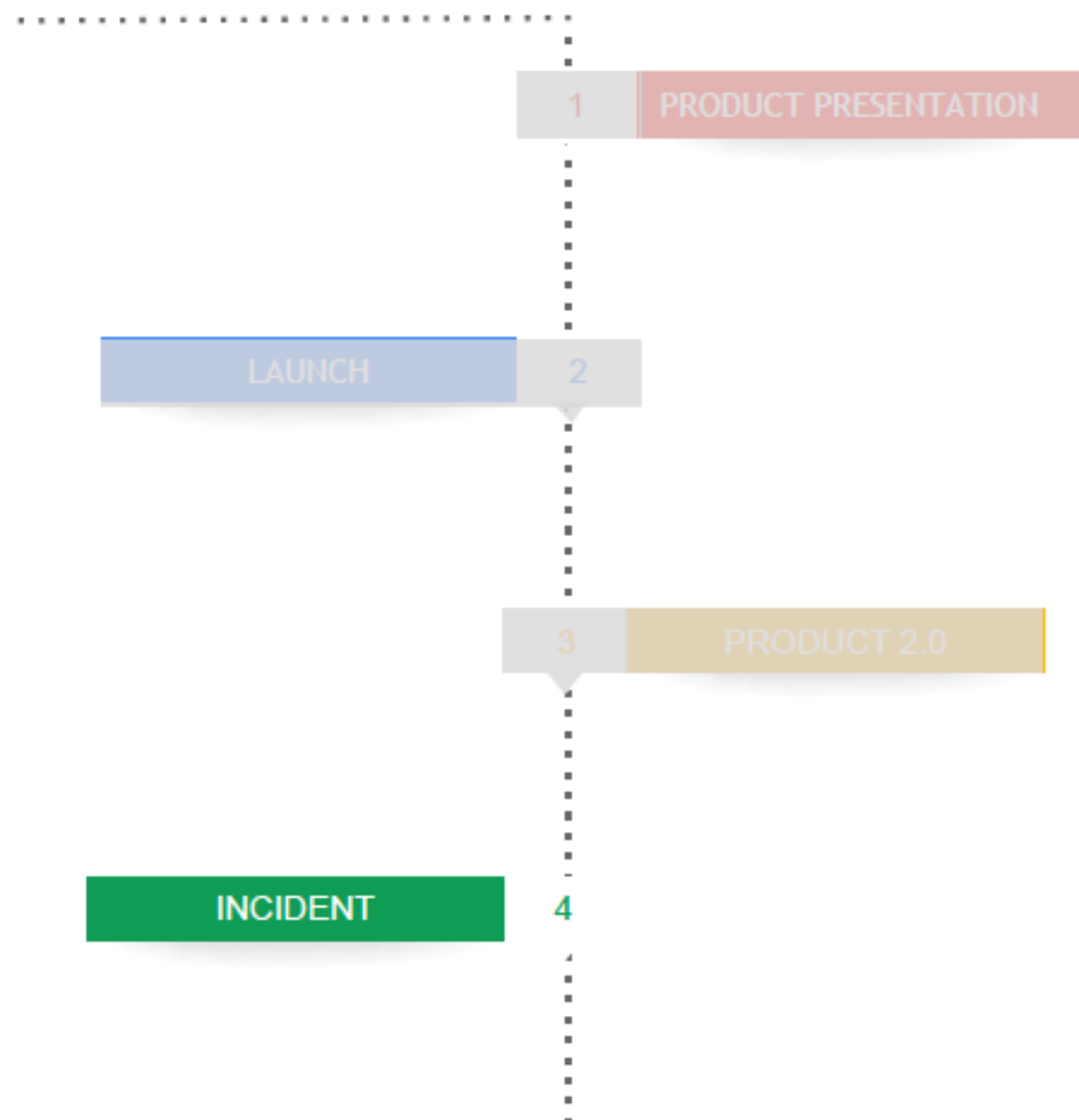


Users like it

Assessment of Super Smile Brush (fictional example)

Issue	User Trust	Legal	Privacy Eng
Health condition data is sensitive	How are you gaining user's trust to provide the data?	Opt-in consent and retention controls.	Storage and access restrictions.
Location data from a toothbrush	What if there are users who don't find this beneficial?	Privacy Policy allows using location, but notify users?	Shared device, so how do you avoid abuse of location data?
Sharing data with dentists	Can users remain aware of who has access to their data?	High Risk Processing considerations/processing conditions	How do you ensure the right doctor gets access to the right data?
Gathering data from kids	Do you understand how kids may interact differently with the brush?	Do you need parental consent?	What supervision features are in place for kids accounts?

Roadmap





Incident!

What happened?



One of the engineering teams develops an update to the companion app



The new functionality allows users to book appointments with dentists that have installed Brush.ly App for Doctors



The update contains a bug in the code that unintentionally causes the name and email address of users who have used this feature to become available to all the dentists that have installed the companion Brush.ly App for Doctors

What happened?



One of the engineering teams develops an update to the companion app



The new functionality allows users to book appointments with dentists that have installed Brush.ly App for Doctors



The update contains a bug in the code that unintentionally causes the name and email address of users who have used this feature to become available to all the dentists that have installed the companion Brush.ly App for Doctors

What happened?



One of the engineering teams develops an update to the companion app



The new functionality allows users to book appointments with dentists that have installed Brush.ly App for Doctors



The update contains a bug in the code that unintentionally causes the name and email address of users who have used this feature to become available to all the dentists that have installed the companion Brush.ly App for Doctors



...a month later...

Fixing the bug



1-2 days of extra
engineering work
required

Fixing the bug



1-2 days of extra
engineering work
required



Extra week necessary for
formal review and
approval

Fixing the bug



1-2 days of extra
engineering work
required

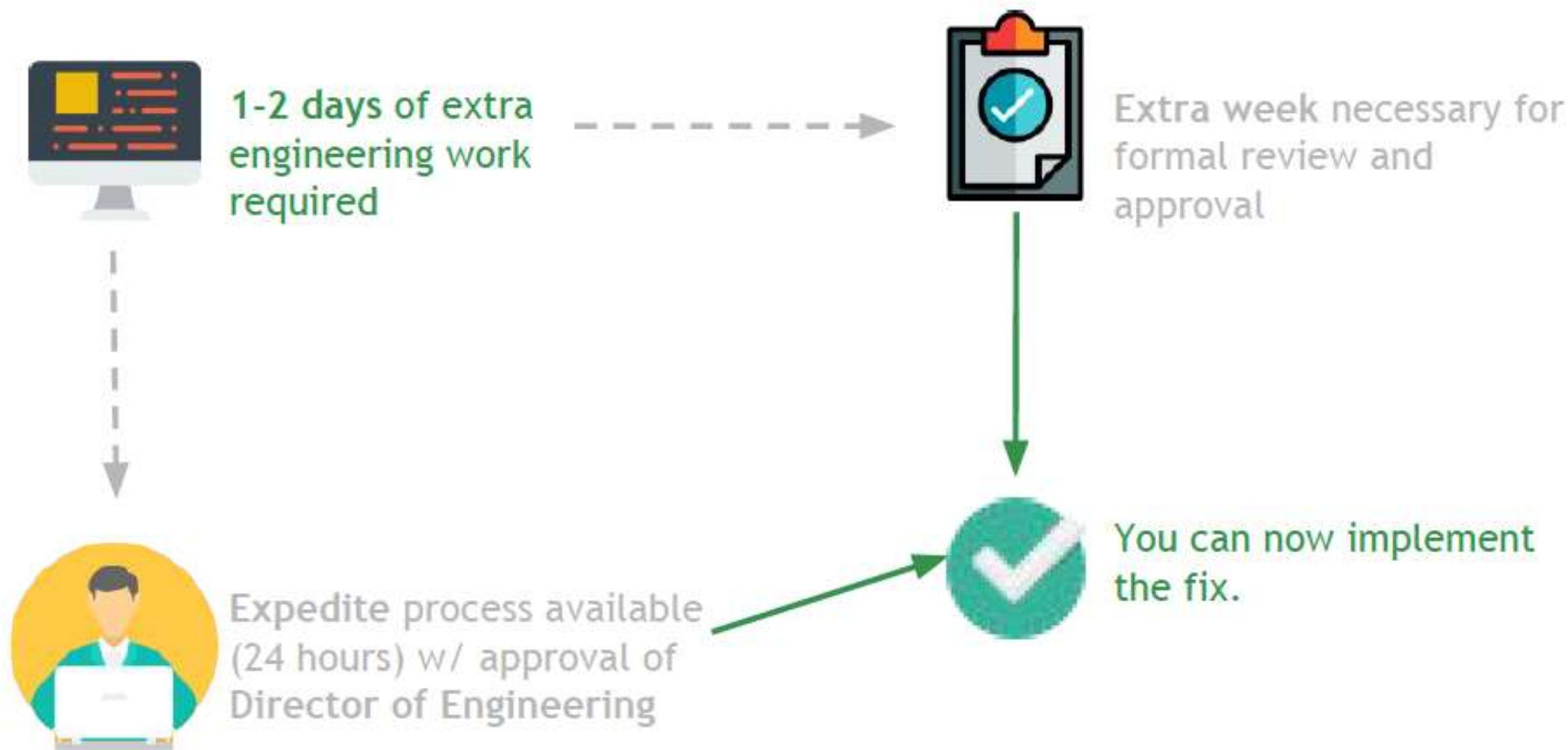


Extra week necessary for
formal review and
approval



Expedite process available
(24 hours) w/ approval of
Director of Engineering

Fixing the bug





What Privacy by Design issues are **highlighted** in this incident?



What Privacy by Design issues are **highlighted** in this incident?

What Privacy by Design issues come into play when **fixing the bug?**



Breach notification?

Thank You





Centre for
Information
Policy
Leadership
Hunton Andrews Kurth LLP



PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

Session IV

Regulator Perspectives on Accountability and How to Incentivise It

- ❖ **Raymund Liboro, Commissioner and Chairman, Philippines National Privacy Commission**
- ❖ **Stephen Wong, Commissioner, Hong Kong Privacy Commissioner for Personal Data**
- ❖ **Zee Kin Yeong, Deputy Commissioner, Singapore Personal Data Protection Commission**

ACCOUNTABILITY AND COMPLIANCE FRAMEWORK AND THE FIVE PILLARS

Raymund Enriquez Liboro
Privacy Commissioner and Chairman
August 1, 2017

1) PERSPECTIVES ON ACCOUNTABILITY AND
HOW TO INCENTIVIZE IT

2) The Greatest Secret on how to be accountable.

Raymund Enriquez Liboro
Privacy Commissioner and Chairman
JULY 26, 2018
Carlton Hotel, Singapore

Blind Trust



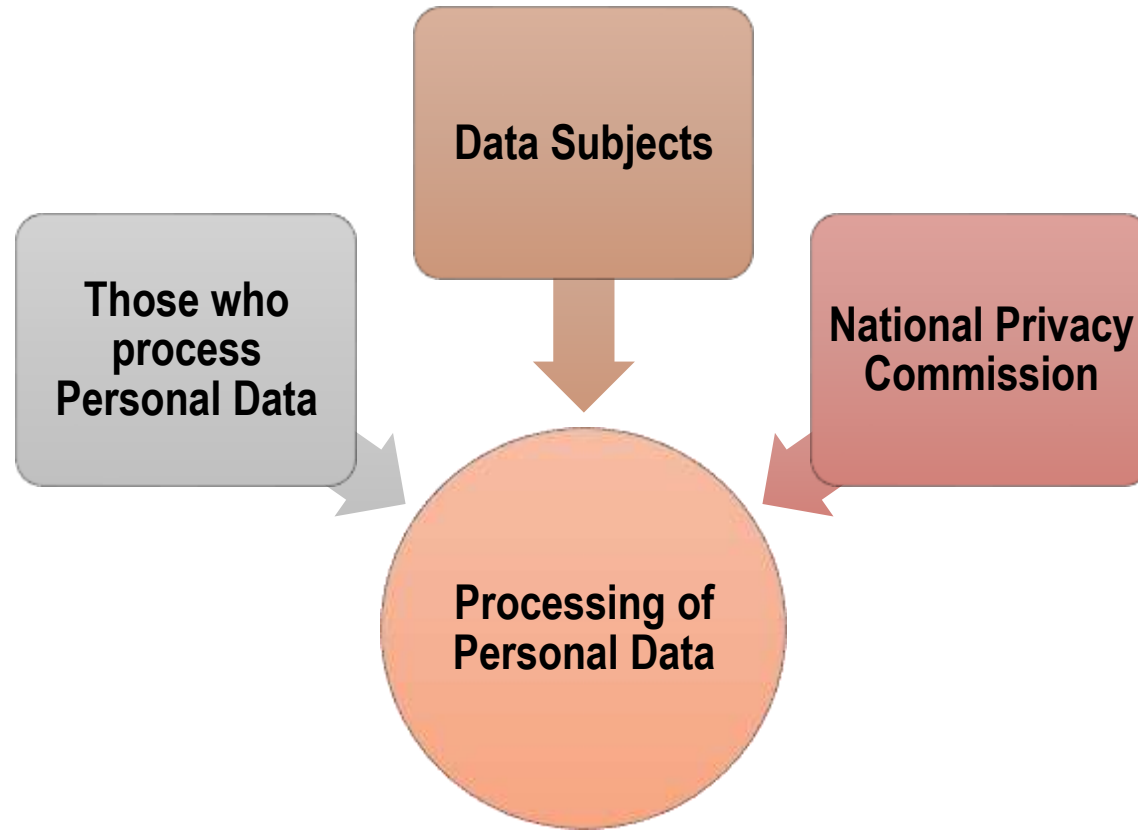
Image from: <https://www.collective-evolution.com/2009/12/22/adam-and-eve/>

Now you've got to prove it!



Image from: <https://www.thoughtco.com/ten-commandments-700216>

SCOPE OF THE LAW and the Privacy Ecosystem



- **PERSONAL INFORMATION CONTROLLERS (PIC) and PERSONAL INFORMATION PROCESSORS (PIP) *PROCESSING* PERSONAL DATA of DATA SUBJECTS**



Risk-based approach | Prevention & mitigation | Building the culture of data privacy & protection

5 PILLARS OF DATA PRIVACY ACCOUNTABILITY & COMPLIANCE



Commit to comply:
Appoint a Data Protection Officer



Know your risks:
Conduct a Privacy Impact Assessment



Be accountable:
Create a Privacy Management Program

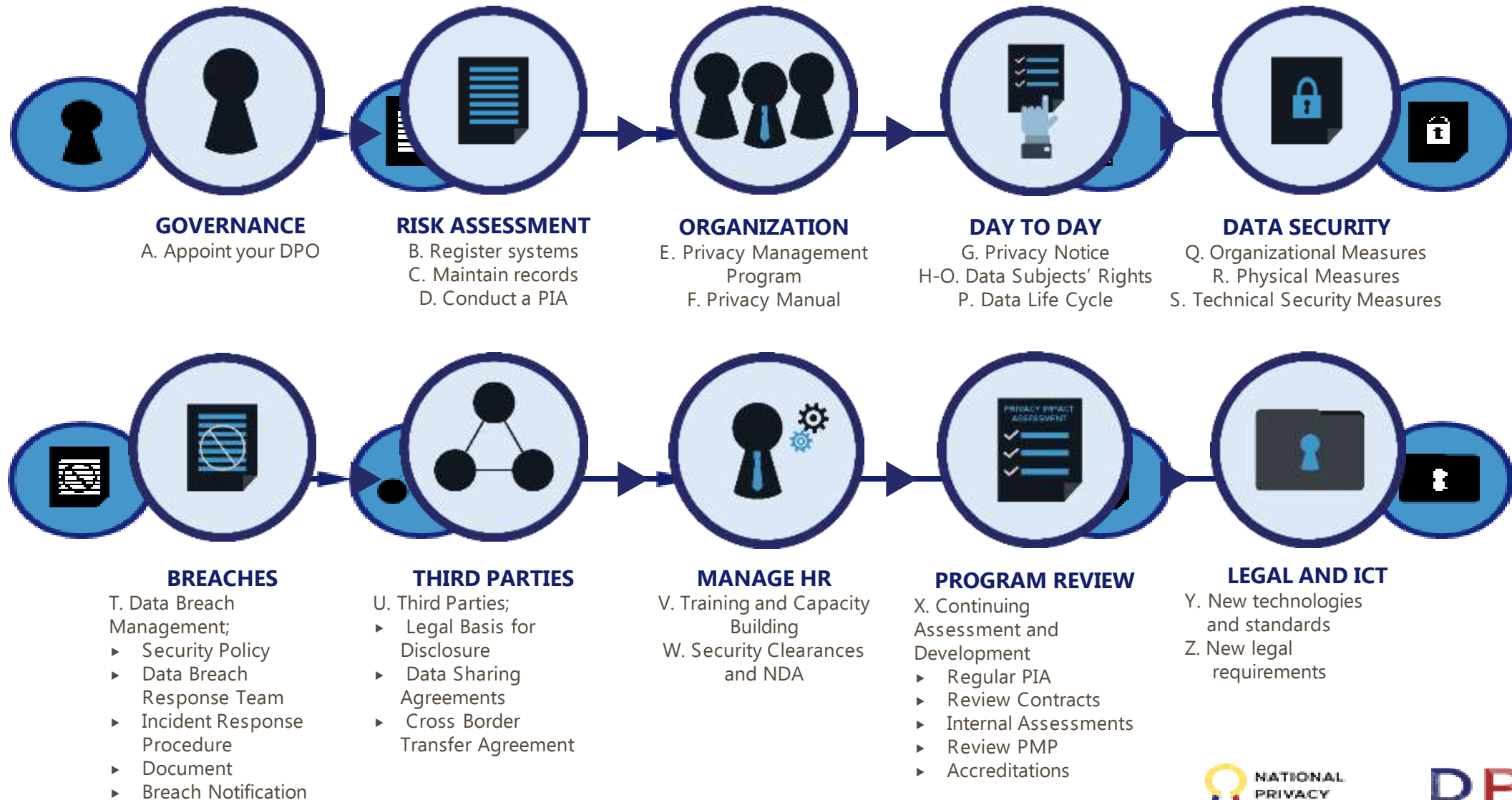


Demonstrate compliance:
Implement Data Privacy and Security Measures



Be prepared for breach:
Regularly exercise Breach Reporting Procedures

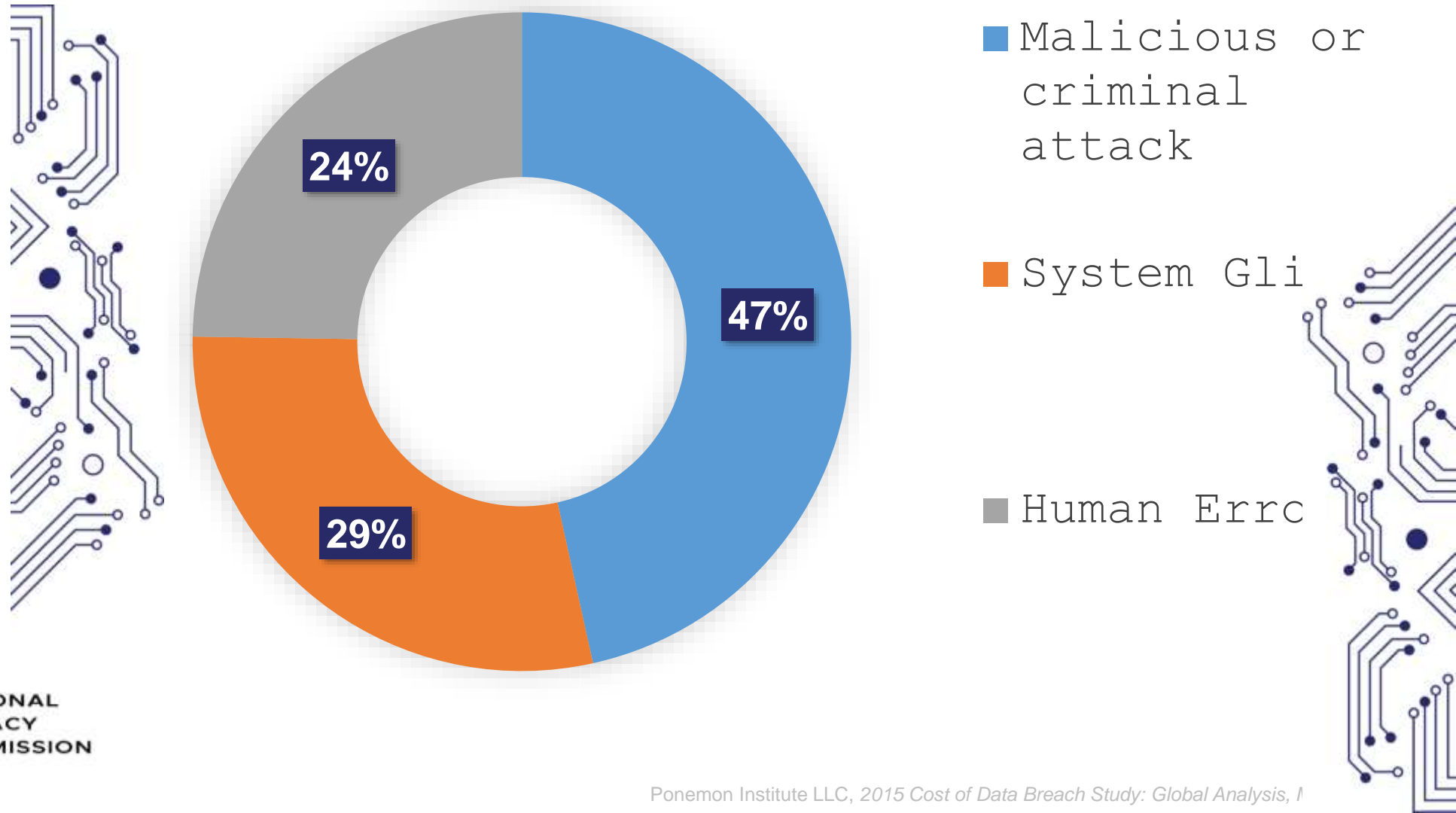
THE DATA PRIVACY ACCOUNTABILITY AND COMPLIANCE FRAMEWORK



What do we look for when the NPC comes knocking at your door?

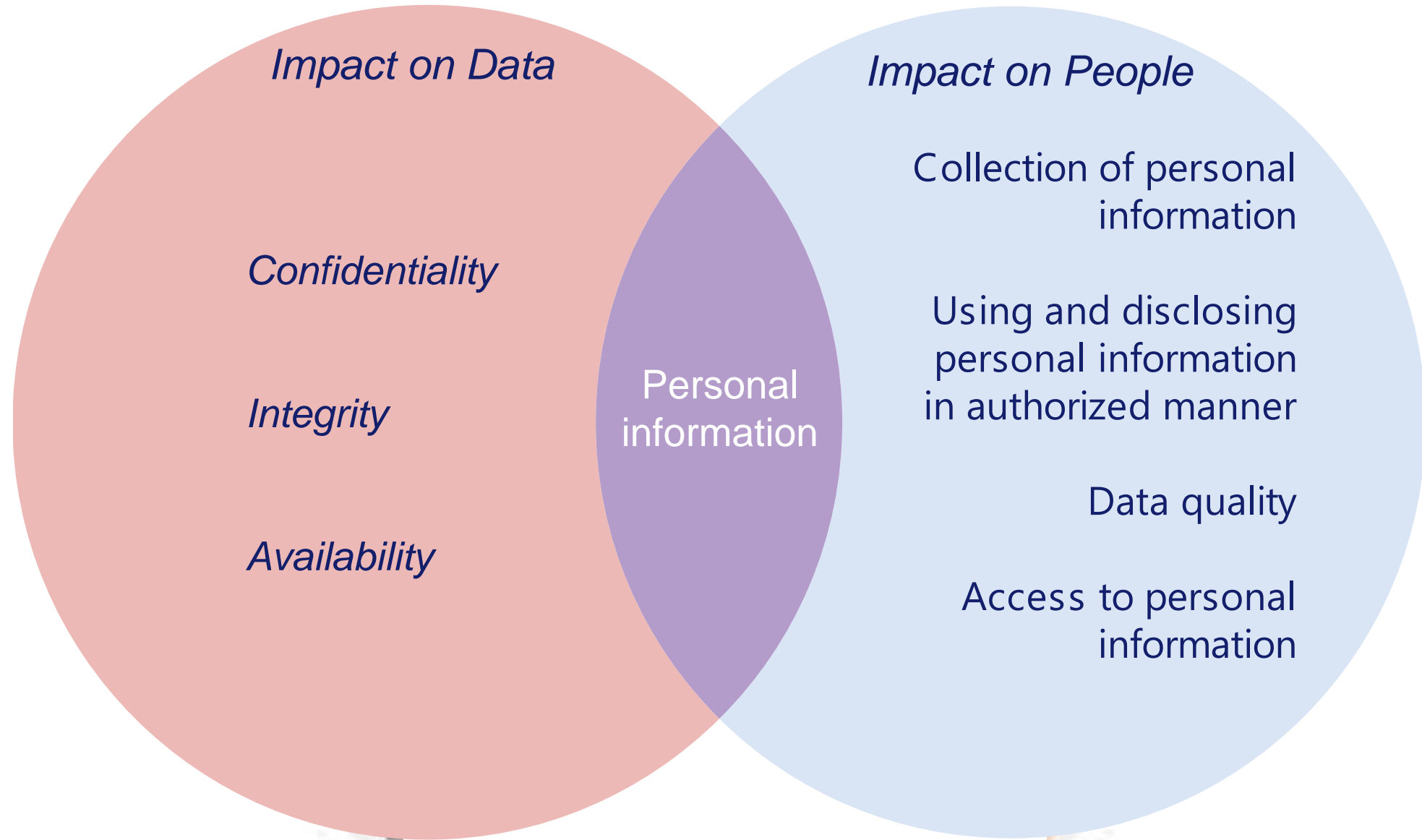
1. Can we feel that culture of privacy?
2. Do you have a sensible data privacy program and do you implement it?
3. Is it based on risk ?
4. Do you train your staff in data privacy and protection?
5. Are you prepared for breach?

ROOT CAUSES OF BREACH



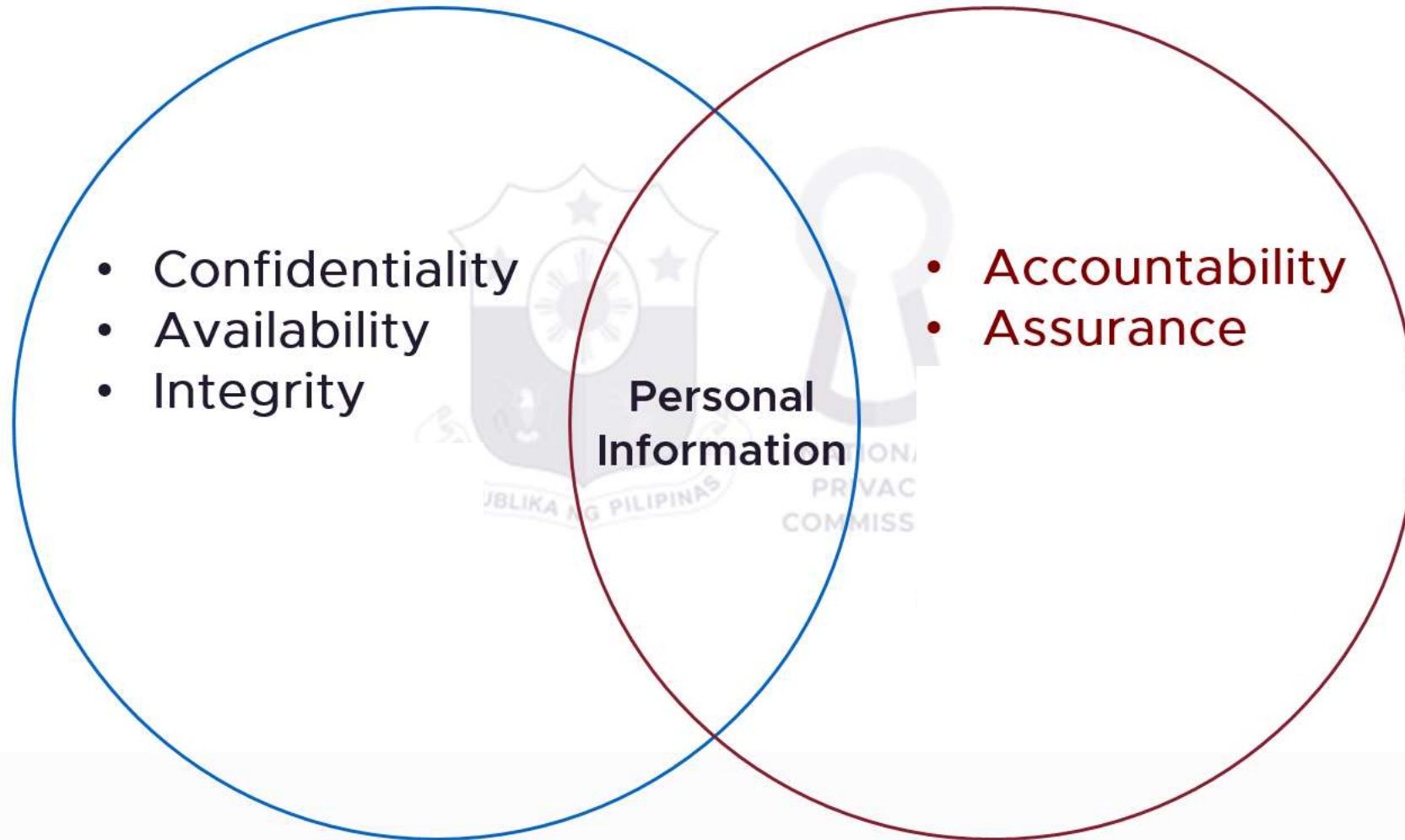
SECURITY

PRIVACY

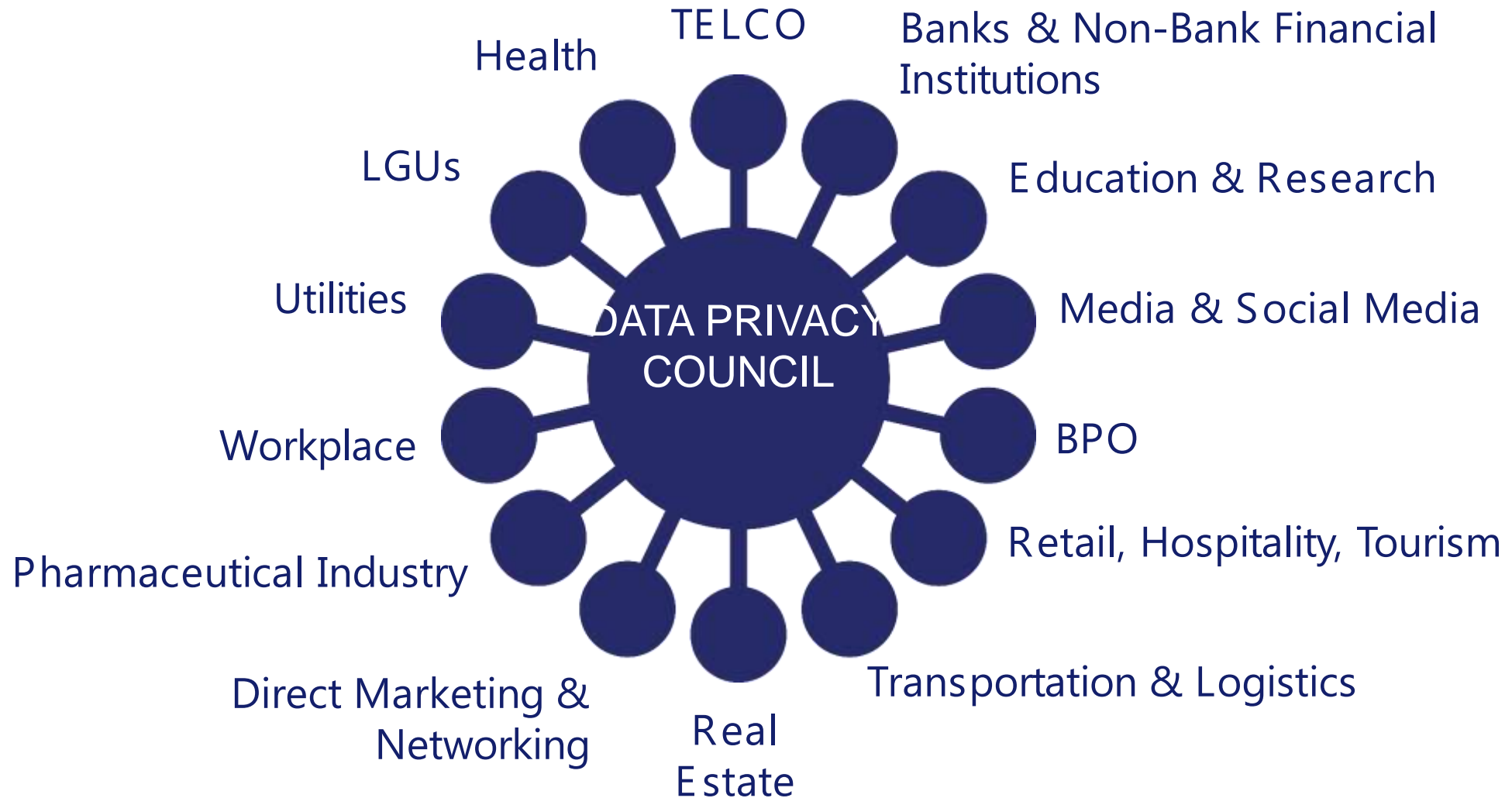


Data Security

Data Privacy



THE DATA PRIVACY COUNCIL





DPO Lifestyle

Haligi ng maunlad na ekonomiya ang pag-iingat ng **personal data**.

Sa ilalim ng **Data Privacy Act (DPA) ng 2012**, tungkulin ng mga organisasyon na protektahan ang personal data na ipinagkatiwala sa kanila ng mga mamamayan. Dulot ng pag-iingat na ito ay ligtas na kalakalan sa merkado at masiglang pag-usad ng kabuhatan.



5 PILLARS OF DATA PRIVACY ACCOUNTABILITY & COMPLIANCE



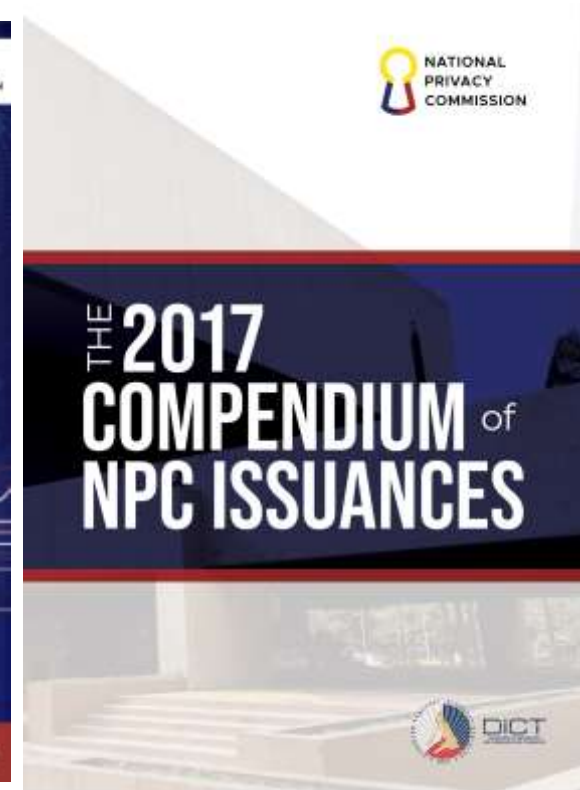
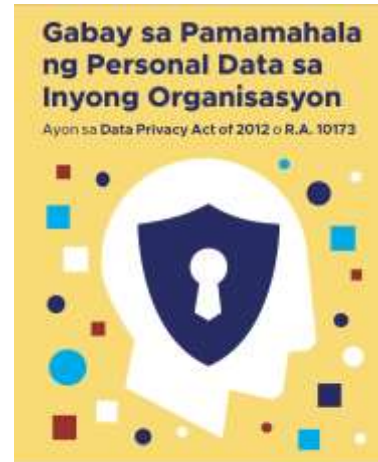
DPO Support



Kapag ang personal data ay hindi protektado, may panganib sa mga tao!

Para sa dagdag na kaalaman,
makipag-ugnayan sa National
Privacy Commission (NPC).

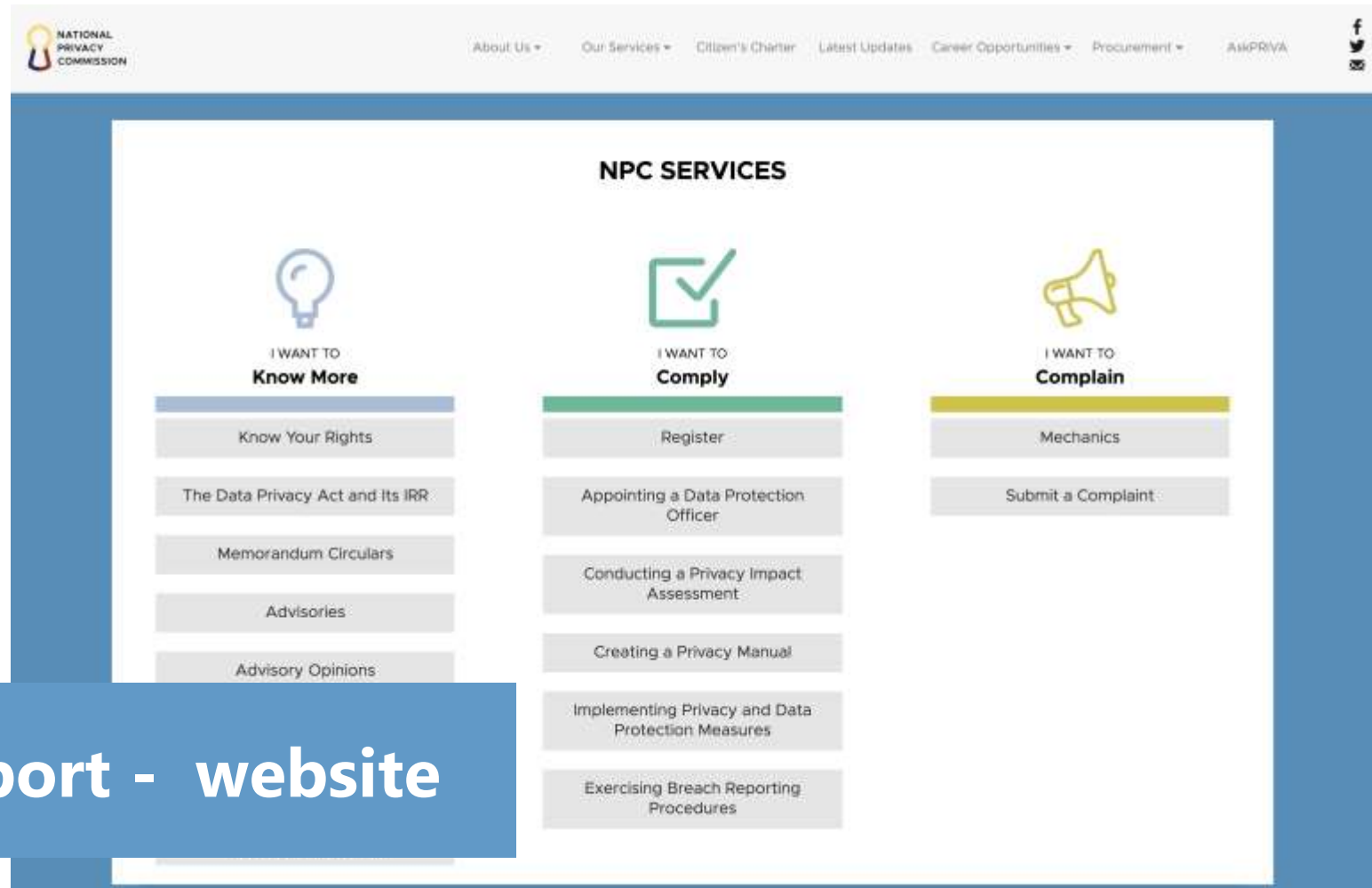
✉ info@privacy.gov.ph
🌐 privacy.gov.ph
☎ 920-0101 local 7021



DPO Support - knowledge materials



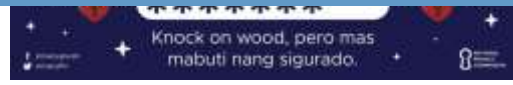
DPO Support- events



DPO Support - website



DPO Support - Social media



So how do we incentivize accountability?

- Incentivize the people.
- Be clear with the message.
 - the pain
 - the benefit
- Walk the talk.
- Engage the stakeholders.

PRIVACY GOLDEN RULES:

IF YOU CAN'T
PROTECT IT, DON'T
COLLECT IT

PRIVACY GOLDEN RULES:

DO NOT DO UNTO
OTHERS WHAT YOU
DO NOT WHAT DONE
UNTO YOU

PRIVACY.GOV.PH

facebook.com/privacy.gov.ph
twitter.com/privacyph
info@privacy.gov.ph



Centre for
Information
Policy
Leadership
Hunton Andrews Kurth LLP



PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

Session IV

Regulator Perspectives on Accountability and How to Incentivise It

- ❖ **Raymund Liboro, Commissioner and Chairman, Philippines National Privacy Commission**
- ❖ **Stephen Wong, Commissioner, Hong Kong Privacy Commissioner for Personal Data**
- ❖ **Zee Kin Yeong, Deputy Commissioner, Singapore Personal Data Protection Commission**

A Regulator’s Perspective on Accountability and How to Incentivise It

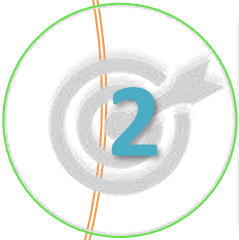
Stephen Kai-yi Wong, Barrister
Privacy Commissioner for Personal Data, Hong Kong, China



Presentation Outline



Hong Kong—Privacy Management Programme



Engaging the Data Controllers (SMEs)



Data Ethics and Trust



Hong Kong—Privacy Management Programme

Hong Kong – Privacy Management Programme



Initiated by the Hong Kong
Privacy Commissioner

Not a legal requirement

Corporate governance
responsibilities



Top-down business
imperative



Data protection policies &
procedures in place



A paradigm shift

Paradigm Shift

*From Compliance
to Accountability*

Compliance Approach

- Passive
- Reactive
- Remedial
- Problem-based
- Handled by compliance team
- Minimum legal requirement
- Bottom-up



Accountability Approach

- Active
- Proactive
- Preventive
- Based on customer expectation
- Directed by top-management
- Reputation building
- Top-down



PMP – Fundamental Principles

Top-Down Organisational Commitments

Top-management
commitment and
buy-in



Setting up of a
dedicated data
protection office
or officer



Establishing
reporting and
oversight
mechanism



PMP – 7 Practical Programme Controls



Personal Data
Inventory



Privacy
Policies



Risk
Assessment



Training
Plan



Breach
Handling



Data
Processor
Engagement



Communication

PMP – Ongoing Assessment and Revision



Develop an Oversight
and Review Plan



Assess and Revise
Programme Controls

Carrots or Sticks?

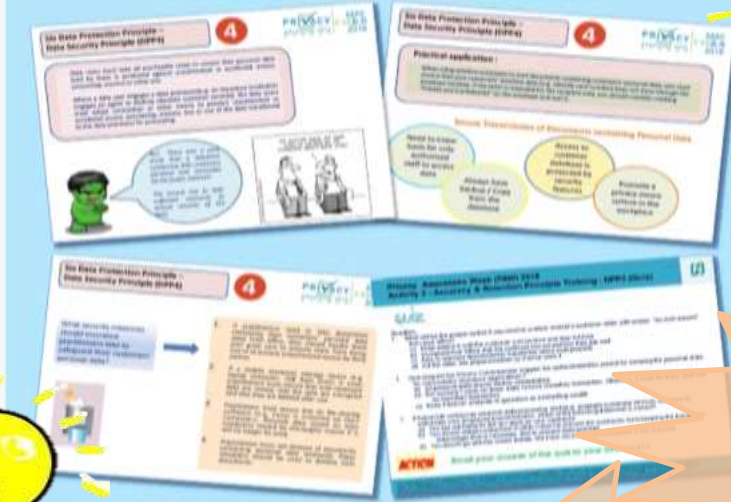


- Deterrence and punishment had limited effects
- Maximum fine for DM conviction cases - **US\$4,000 only!**
- No power to impose administrative fines
- Promoting accountability through PMP



Organisations' Sharing

• Daily Training and Quiz on Data Protection Principles Good practices on data handling were shared with the staff.



• Desktop Wallpaper Design Competition

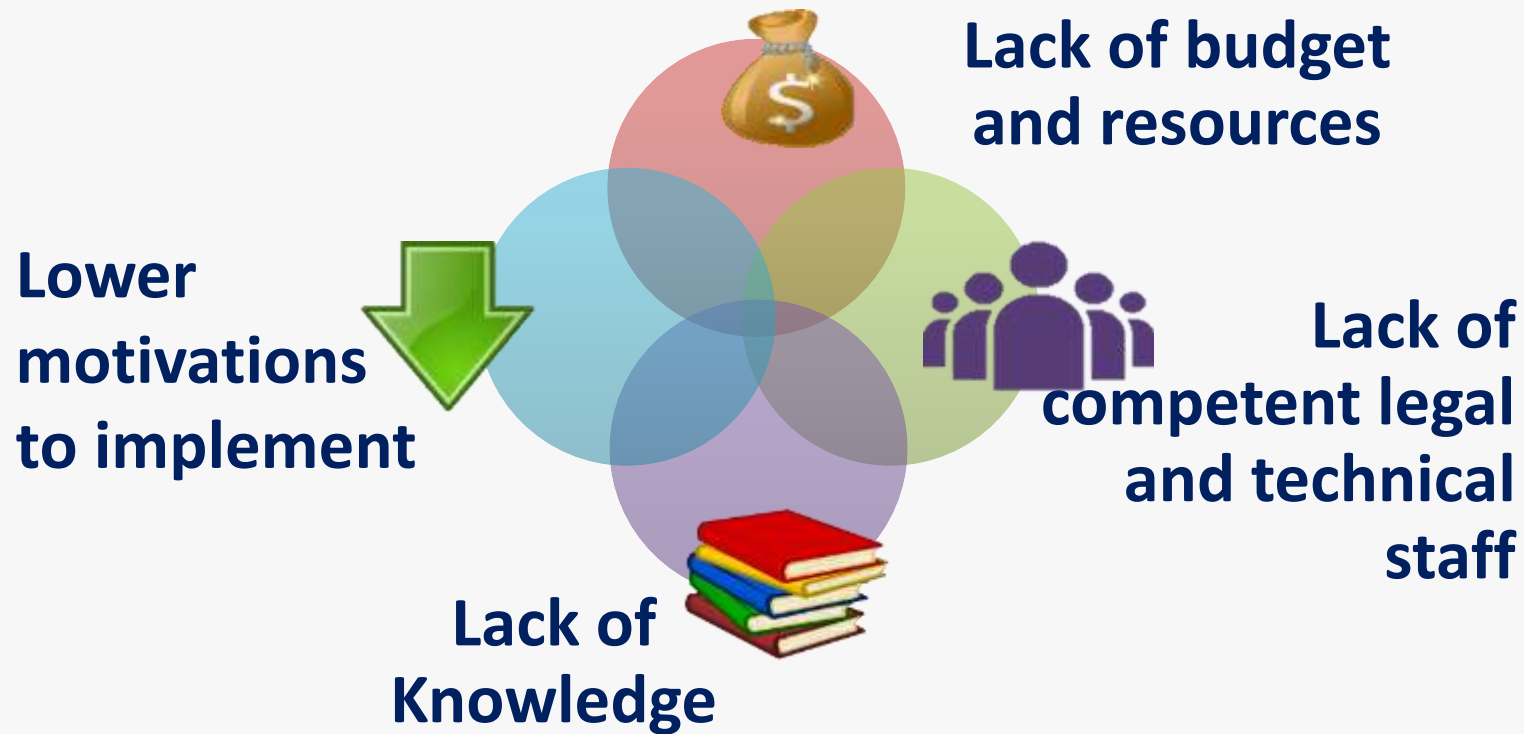


Training

Privacy
Impact/Compliance
Assessment

Conducted by the Government
on specific projects e.g. SMART
ID, e-health System, etc.

Practical Difficulties Encountered by Organisations in implementing PMP



DPA's should provide incentives

Consultancy Project on Implementation of PMP in Government

**PMP
Training**



**Consultant engaged to
facilitate bureaux
/departments to
implement PMP**

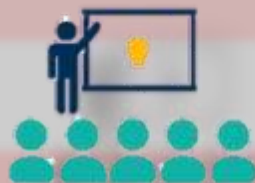
**PMP Manual
(To be completed this year)**



**Advice
provided by the PCPD**

Deliverables by the Consultant

General Reference
Guide



Workshops

PMP Manuals for
selected government
bureau/departments



Toolkits and training
materials

PMP Manuals for government departments



✓ Cover all components of a PMP

Section 1:

Overview of the Privacy Management Programme (“PMP”)

Organisational Commitment

A-1a. Roles and Responsibilities of the Departmental Data Protection Officer and Other Officers Assisting in the Implementation of PMP
A-1b. Reporting Mechanism

Section 2

Overview of the Personal Data (Privacy) Ordinance

Programme Controls

A-2b. Policies for Handling Personal Data
A-2c. Risk Assessment Tools
A-2d. Training and Education
A-2e. Breach Handling
A-2f. Data Processor Management
A-2g. Communication

Section 3:

The tailor-made PMP

Ongoing Assessment and Revision

1. Oversight and Review Plan
2. Review of PMP’s Effectiveness

PMP Manuals for government departments



Groundwork:

Understand the bureau/departments

- reviewing existing policies, guidelines, procedures, etc.
- interviewing key divisions/sections to understand their operations
- walkthrough of key privacy controls in place within the data privacy lifecycle

Report

- overview of current status of the PMP
- detailed findings and recommendations
- a road map for way forward

Worked with the bureau/departments and prepared the PMP Manual

- tailored templates, outlines/key contents of the policies and procedures, frameworks and protocol references.

PMP Manuals for government departments



Based on the observations identified



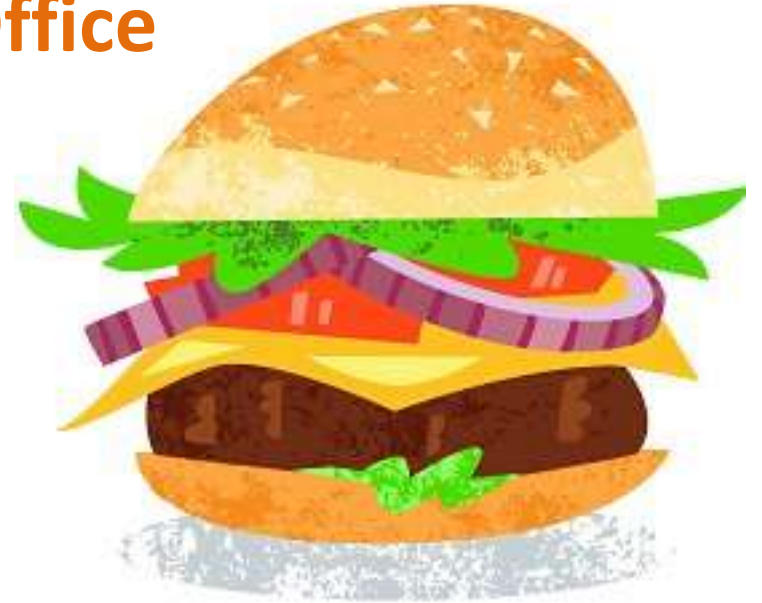
Remediate the gaps identified



PMP Manuals for government departments

Set up of Data Protection Office

Specified **roles** and
responsibilities of
Data Protection Officer,
Personal Data Privacy Officer
and
Team Coordinator



privacy respectful culture

PMP Manuals for government departments



Role	Officer	
Data Protection Officer	[Post/Title of the officer(s) - To be decided by each individual Bureau / Department.]	
Personal Data Privacy Officer		
Team Coordinator	Team 1	[Post/Title of the officer(s) - To be decided by each individual Bureau / Department.]
	Team 2	
	Team 3	
	Team 4	
	Team 5	
	Team 6	
	Team 7	



PMP Manuals for government departments



privacy respectful culture



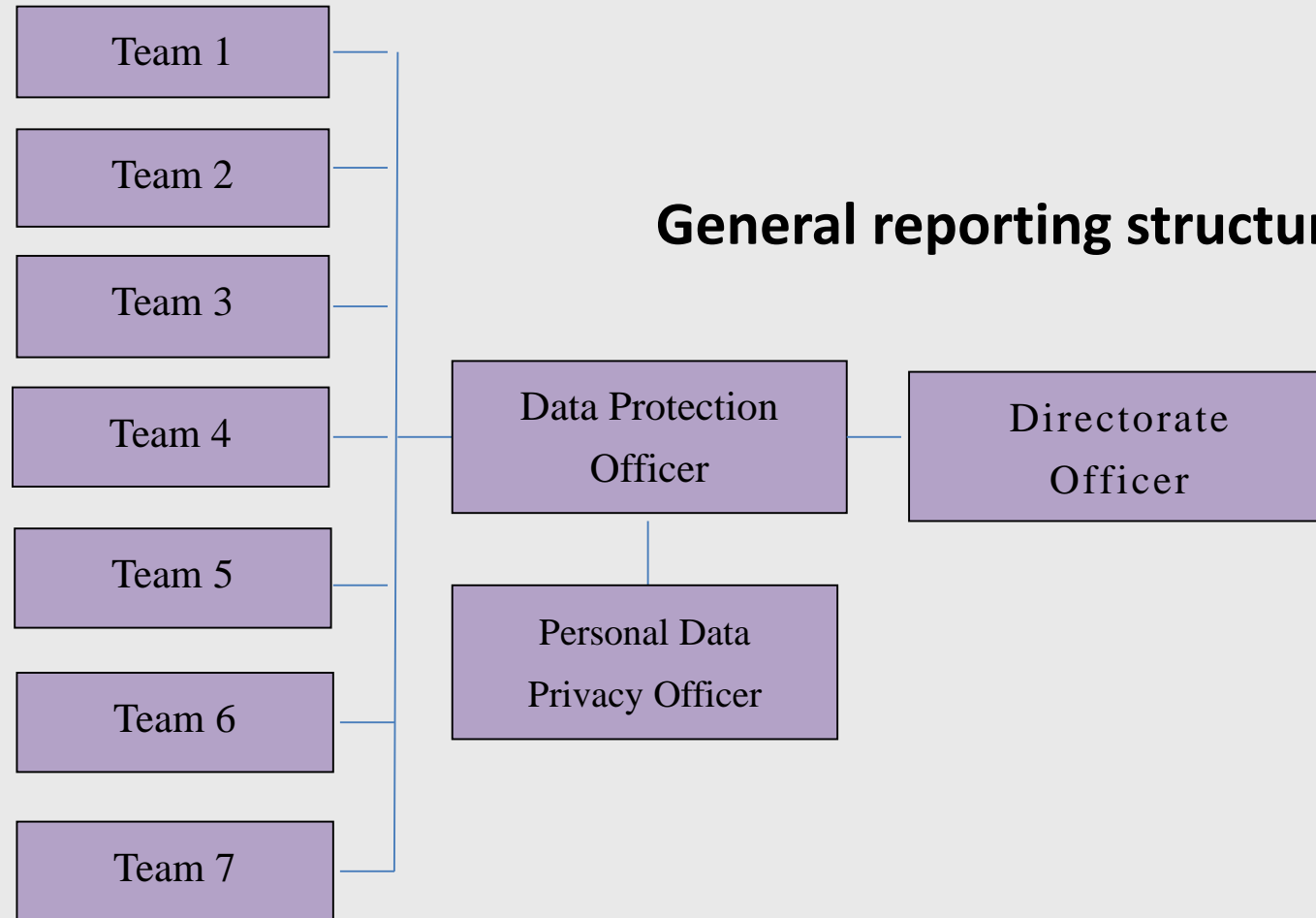
Set up of a clear **general**
reporting structure &
reporting mechanism with
respect to **data breach**
handling



PMP Manuals for government departments



Team Coordinators



PMP Manuals for government departments

Set up of reporting mechanism with respect to data breach handling





PMP Manuals for government departments



Practical Protocols

Specific steps and procedures

PMP Manuals for government departments



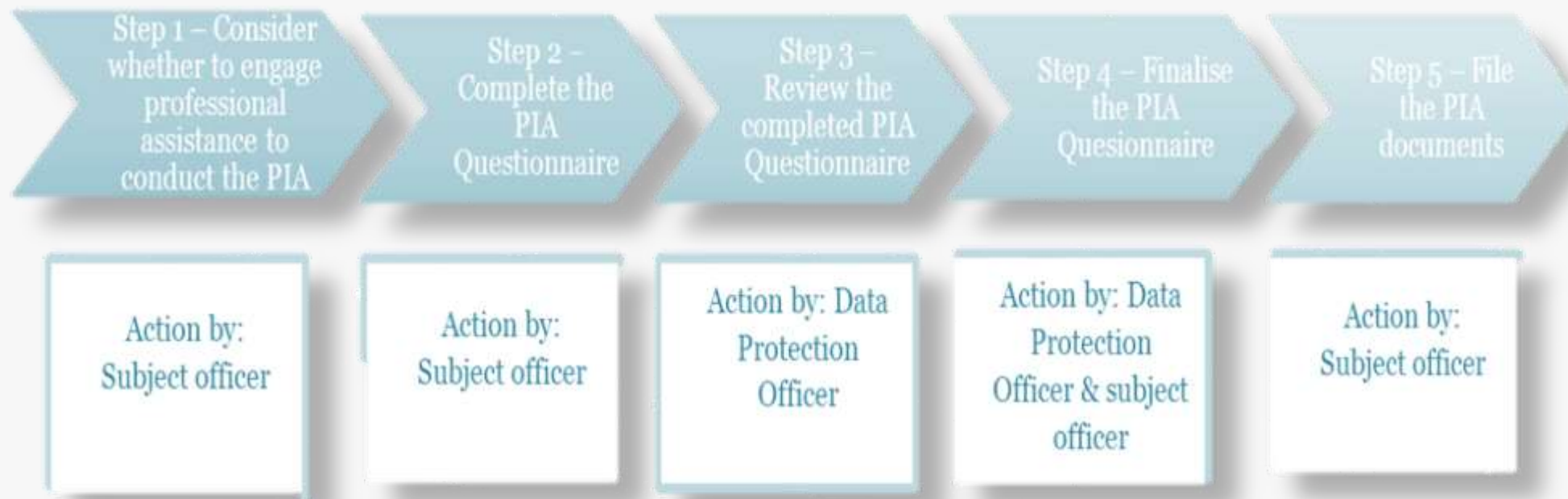
✓ Steps for Personal Data Inventory Review



PMP Manuals for government departments

✓ Specific steps and procedures

Steps for conducting a Privacy Impact Assessment





PMP Manuals for government departments



PMP Manuals for government departments

Tailored templates



Questions	Yes/No	Remarks
1) Do the contractual terms cover BUREAU / DEPARTMENT's right to audit and inspect how the data processor handles and stores personal data?		
2) Do the contractual terms cover the data processor's obligation to report immediately to BUREAU / DEPARTMENT for any loss of documents, security breaches or signs of abnormalities?		
3) Do the contractual terms cover the limitation of using or disclosing any personal data it receives or gains knowledge of that should be for a purpose which the personal data is entrusted to it?		
4) Do the contractual terms cover the sub-contract arrangement limitations and arrangements?		
5) Do the contractual terms cover the timely return, destruction or deletion of personal data by the data processor?		
6) Do the contractual terms cover the data processor's obligations to adopt practicable means to protect the data entrusted to it (e.g. appropriate security measures, personal data protection policies and procedures, adequate training to relevant staff, cross-border data		

transfer arrangement)?		
7) Do the contractual terms cover the consequence for violation of the contract?		
8) Is the Team/Section satisfied that the data processor had followed the contractual obligations in respect of personal data protection? If "Yes", please elaborate.		
9) If the answer to Q(8) above is "No", did the Team/Section take any actions?		
10) Has the Team/Section performed any scheduled audit/inspection on the data processor in the past three years (including surprise visit)? If the answer is "Yes", please state: (a) the year of the audit/inspection (b) any irregularities identified; and (c) any remedial actions taken. If the answer is "No", please explain why an audit/inspection is not required.		
11) If audit/inspection was performed on the data processor this year, has the Team/Section identified any irregularities? If "Yes", please state the details and the improvement measures taken by the data processor.		
12) Has any data breach incidents occurred which involved the data processor? If "Yes", please provide the corresponding Data Breach Information Sheet as attachment (please refer to Annex Q of the PMP Manual).		

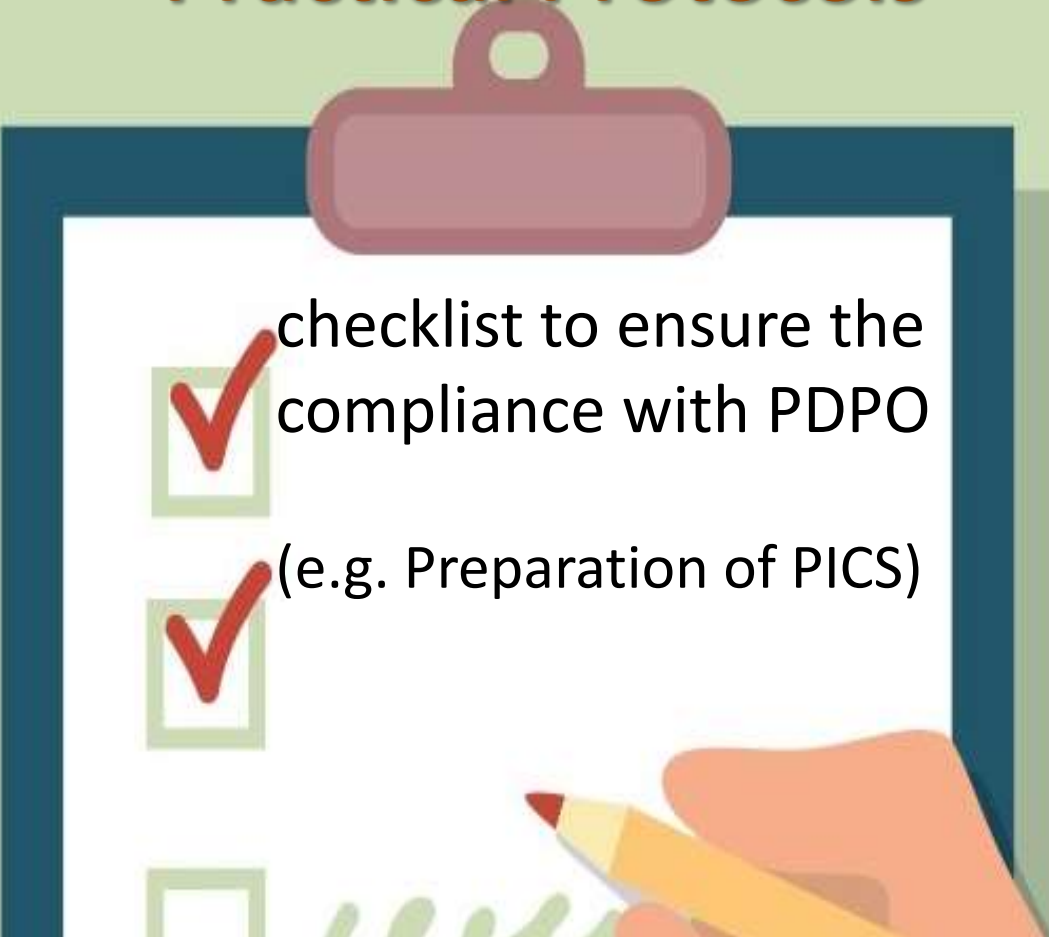
Completed by (Team Coordinator)	Reviewed by (Data Protection Officer)
Signature _____	Signature _____
Name _____	Name _____
Post _____	Post _____
Date _____	Date _____

Reviewed by (Team / Section Head)
Signature _____
Name _____
Post _____
Date _____

Data Processor
Review

PMP Manuals for government departments

Practical Protocols

- 
- checklist to ensure the compliance with PDPO
(e.g. Preparation of PICS)

PMP Manuals for government departments



Checklist
for
Preparation
of PICS



Checklist for the Preparation of PICS

Part 1: Background Information

Activity	
Team/Section	
Subject officer (Name and Position)	
Expected date of adoption of the PICS concerned	

Part 2: Required Information – Team Coordinators must include the following items when preparing a PICS

Item	Checked ☐
1. The PICS should inform the data subject of the following information:	
(a) a statement of the purpose for which the personal data collected will be used	☐
(b) a statement of whether it is obligatory or voluntary for the data subject to supply his/her personal data	☐
(bii) a statement of the consequences if he/she fail to supply his/her personal data where it is obligatory to do so	☐
(c) a statement of the clauses of persons to whom personal data collected may be transferred or disclosed	☐
(d) a statement of his/her personal data	☐
(e) a statement of his/her personal data Privacy Officer for data correction of the contact details of the Personal Data Privacy Officer for data subject to request for access or correction of their personal data	☐
(f) If applicable, a statement of the security measures adopted to safeguard the personal data to be collected	☐
(g) a hyperlink to the Privacy Policy Statement at (to be inserted with bureau / department's respective website) if the PICS is to be given online	☐

Part 3: Presentation of PICS

Item	Checked ☐
2. The PICS will be provided to the data subject on or before collecting his/her personal data.	☐
3. The purpose statement is not too vague or too wide in scope.	☐
4. User-friendly language (e.g. the choice of simple rather than difficult words and the avoidance of use of legal terms or convoluted phrases) and presentation are used.	☐
5. The layout and presentation of the PICS (including the font size, spacing, underlining, use of headings, highlights and contrasts) has been designed so that the PICS is easily readable to individuals with normal eyesight.	☐
6. The PICS is presented in a conspicuous manner (e.g. the PICS is a stand-alone section and its contents are not buried among other	☐

PMP Manuals for government departments



Practical Protocols

Policies



(e.g. collection of identity card,
use of portable electronic
storage devices, handling of
DAR & DCR)

Practical Protocols

GUIDELINES

*Guidelines (e.g. handling of PD
obtained from Hotline, record
disposal)*

PMP Manuals for government departments



Comprehensive TRAINING ACTIVITIES



Engaging the Data Controllers (SMEs)

Engaging Through Education

- Website: PCPD.org.hk



The screenshot shows the PCPD website homepage. At the top, there's a navigation bar with the PCPD logo, the text "PCPD.org.hk", and the title "香港個人資料私隱專員公署 Privacy Commissioner for Personal Data, Hong Kong". Below this is a search bar and a "A Quick Guide" button. The main content area features a large graphic titled "European Union General Data Protection Regulation 2016" with a circular diagram of icons. To the right, there's a "What's New" section with several news items. At the bottom, there are two columns: "For Individuals" and "For Organisations", each with a list of resources. The footer contains the PCPD logo and the text "PCPD.org.hk" and "香港個人資料私隱專員公署 Privacy Commissioner for Personal Data, Hong Kong".

香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

Engaging Through Education

- Thematic Websites



www.pcpd.org.hk/childrenprivacy



www.pcpd.org.hk/besmartonline



Engaging Through Education

- Social Media

www.youtube.com/user/PCPDHKSAR



www.facebook.com/besmartonlinepcpd

Engaging Through Education

- Seminars, talks, speaking engagements: self-organised or upon invitation
- Industry-specific and individual companies/organisations; chambers and associations
- Covering both public and private sectors
- In 2017: Conducted 314 professional workshops,
- talks, seminars, speaking engagements and meetings with stakeholders, with 25,038 participants



Engaging Through Education

- Industry-specific tools and guidance

Online Assessment Tool for Retail Operation



Guidance Note for Beauty Industry



Engaging Through Education

- Industry-specific tools and guidance
- at PCPD.org.hk



Engaging Through Education

- Industries engaged:



中小企保障私隱運動

Privacy Campaign for SME

中小企專用諮詢

Dedicated Enquiry Services for SME



2110 1155

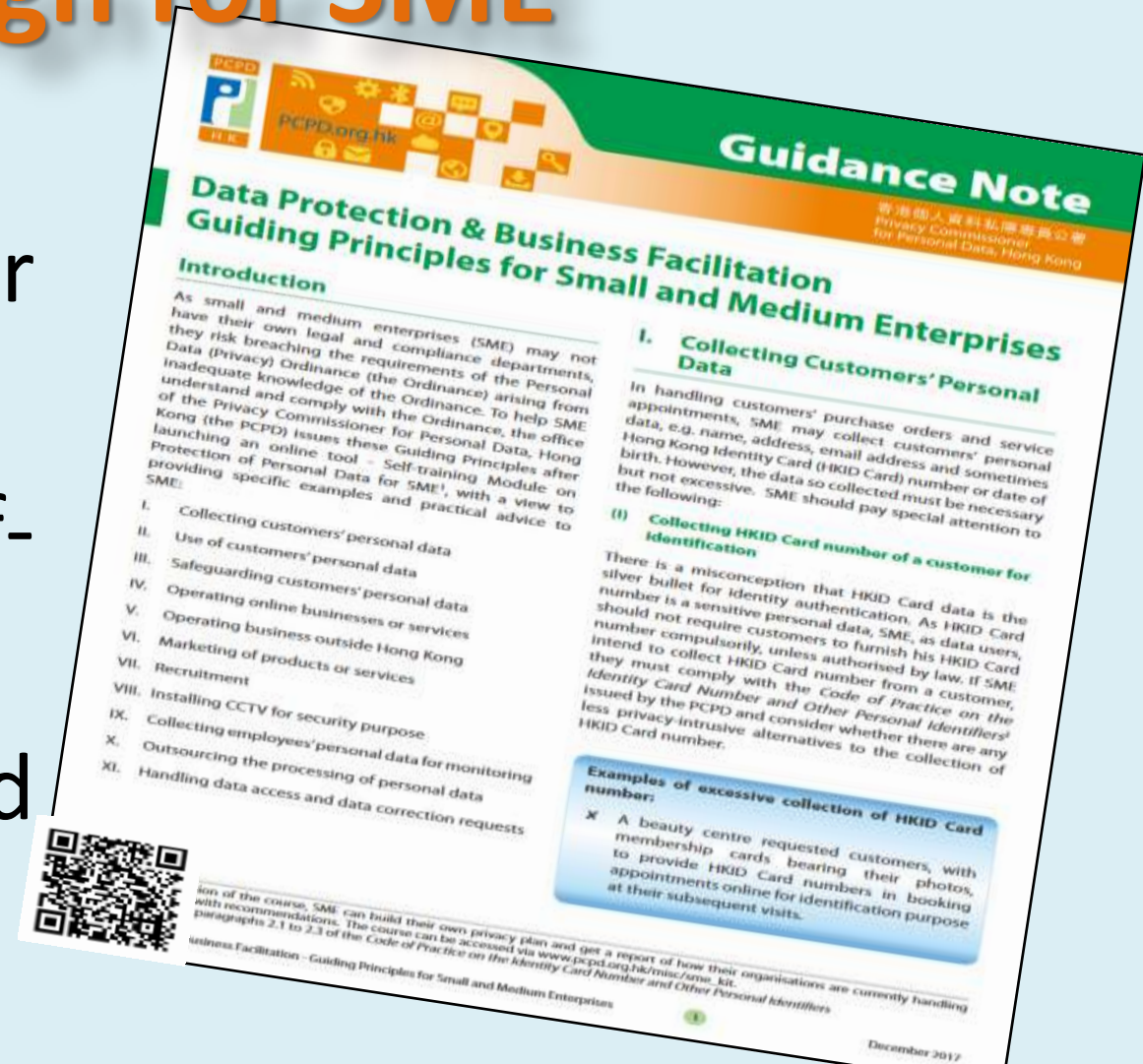


sme@pcpd.org.hk



Privacy Campaign for SME

- Guidance Note for SME
- A new toolkit dedicated for SME will be published
- Revamp the online self-training module for SME
- Engage SME chambers and associations



Engaging Through Promotion

- Media promotion

In 2017:

- Press releases: 30
- Responses to media enquiries: 217
- Media interviews: 54



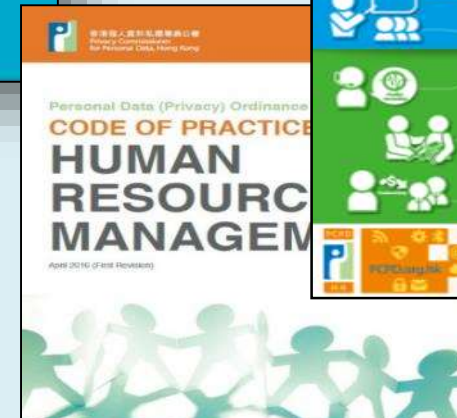
香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

- Op-ed articles



Engaging Through Promotion

- Publications
 - Topic-specific
 - Industry-specific



香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

Engaging Through Exchanges and Dialogues

- Data Protection Officers' Club
 - Established in year 2000
 - Over 550 members from public and private sectors
 - A platform for members to share and exchange views



Engaging Through Exchanges and Dialogues

- Data Protection Officers' Club
- Seminars, sharing sessions, visits, etc.



Engaging Through Exchanges and Dialogues



Data
Protection
Officers' Club

Dedicated
website and
e-newsletter



香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

Engaging Through Exchanges and Dialogues

- Work hand in hand with data controllers for issues/data breaches
- Example: data breaches by travel agents

Top News

Two more Hong Kong travel agencies hacked

By Prudence Lui / Posted on 9 January, 2018 11:28



Hack attack on popular Hong Kong travel agent WWPKG puts customer data at risk

The agency, which specialises in Japan tours, did not say how many customers were potentially affected and if data was stolen

PUBLISHED : Tuesday, 07 November, 2017, 2:48pm
UPDATED : Tuesday, 07 November, 2017, 10:53pm

SBS CANTONESE

Another hacking report on HK Travel agent



Engaging Through Exchanges and Dialogues

- Meetings with chambers, trade associations and professional bodies; conduct seminars and sharing sessions
 - Hong Kong General Chamber of Commerce
 - Chinese General Chamber of Commerce
 - Chinese Manufacturers' Association of Hong Kong
 - American Chamber of Commerce in Hong Kong
 - British Chamber of Commerce in Hong Kong
 - Hong Kong Association of Banks
 - Hong Kong Monetary Authority
 - Hong Kong Institute of Chartered Secretaries
 - Hong Kong Institute of Human Resource Management



Engaging Through Exchanges and Dialogues

- Meetings and exchange of views with multinational corporations/associations for the latest developments/initiatives with privacy implications
 - Facebook: Revised privacy setting; education programmes
 - Microsoft: seminars on privacy related topics
 - Alibaba
 - PayPal
 - Visa
 - Google



Engaging Through Exchanges and Dialogues

- Hong Kong Federation of Insurers (HKFI): Proposed database for insurance claims
 - HKFI is considering to set up a central database to combat fraud. Historical claims data will be contributed to this central database by the participating insurers.
 - HKFI and PCPD have been in dialogue on this proposed initiative.
 - HKFI has taken into account PCPD's comments and has built in privacy by design in the setup of the proposed database.





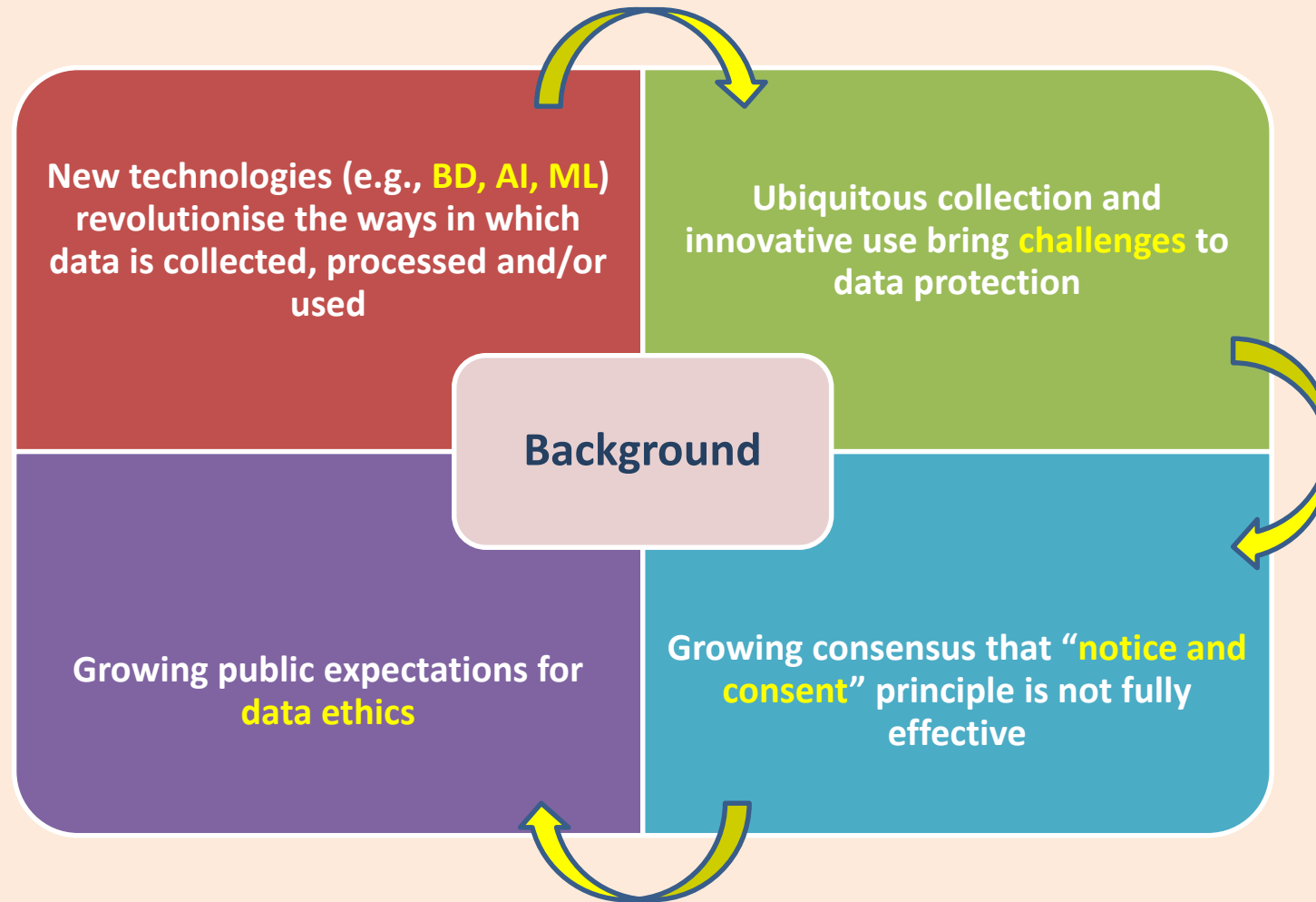
Data Ethics as a Solution

Data Ethics and Trust



- No Surprise to Consumers
- No Harm to Consumers

Promoting Ethics - “Legitimacy of Data Processing Project”



Project Background

Project
commenced in
April 2018

PCPD
commissioned a
US consultancy to
steer the Project

3 in-person
meetings in Hong
Kong

Involving 23
businesses from
different sectors



Project Objectives



What does “ethical data processing” mean?

“Fair data processing” – what would the standards be to describe what being “fair” means?

What is the direct or indirect linkage between fair/ethical data processing and legal requirements, and what aspects of ethical data stewardship go beyond the law?

What are the motivators for business to adopt the principles and standards and utilise ethical data impact assessments?

Participating Organisations

23 participating organisations



Methodology

In-person meetings

- **2 in-person meetings between the US consultancy and the participating organisations:**
 - understanding the level of maturity or “capability of privacy programs” within Hong Kong business community;
 - sharing of practical experience of the participating organisations in adopting / implementing accountability and data ethics;
 - discussing the data stewardship accountability elements and values, business specific “principles” that support the values, and ethical data impact assessment
- **2 in-person meetings (and email discussions) between the US consultancy and PCPD on project approach and issues**
- **1 in-person meeting among all parties to be held in August 2018**

Teleconferences

- **2 teleconferences between the US consultancy and participating organisations subsequent to the in-person meetings to follow up on the comments gathered at the meetings**

Deliverables by the Consultancy



PCPD's Strategic Focus



спасибо
danke 謝謝
ngiyabonga
teşekkür ederim
dank je
gracias
tapadh leat
moichchakkeram
go raibh maith agat
arigatō
dakujem
merci
ευχαριστώ
grazie
kop khun krap
sukriya
sagolun
dziękuje
hvala
maururu
bedankt
obrigado
salamat
terima kasih
감사합니다



Centre for
Information
Policy
Leadership
Hunton Andrews Kurth LLP



PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

Closing Remarks

Bojana Bellamy, President, CIPL