GSMA’s IoT Privacy by Design Decision Tree

1. What data is needed/collected?
2. Is Data “personal” & regulated in law?
3. How will data be used & what for?
4. Conduct Privacy Impact Assessment (PIA)
5. Design User Interface: Transparency, Choice & Control
6. Could the use of data impact an individual’s privacy?

- Initial interaction / activation of service/product

**CONSUMER TRUST IN THE IOT SERVICE IF IT MEETS:**

(I) PRIVACY & DATA PROTECTION OBLIGATIONS

(II) CONSUMER PRIVACY RIGHTS

(III) CONSUMER PRIVACY EXPECTATIONS

---

E.g. will it be shared with 3rd parties or used for purposes non-obvious to the user?
Decision Tree: 1. What data do you need & how will you collect it?

- What data do you need to collect from/about the consumer so that your IoT service or product can function properly?
  - ‘static’ Vs ‘dynamic’ data
- Will data be collected automatically or through consumer’s manual sign-up?
- How will you obtain the consumer’s consent/permissions in relation to using such data e.g. through:
  - The registration form? Online webpage? Smartphone app?
  - Other media interface?
  - What if your device only has sensors but no screen? (see also step 5)

Have you considered the consumer-journey when designing the activation process? Do consumers understand how their data will be used across the value chain & the impact, if any, to their privacy?
Decision Tree: 2. Is Data “personal” & regulated in law? (compliance and due diligence)

2 Is Data “personal” & regulated in law?

- What is the definition of “personal” data in each of the markets you operate in?
- Is the data collected “personal” & regulated in law? If so, have you identified the legal basis that allows you to process such data?
- Are you subject to any privacy-related licence conditions (e.g. telco)
- Are there any federal, state, local or sector-specific laws that apply in addition to general data protection laws? e.g.:
  - Financial / payment services, healthcare regulations
  - Potential restrictions on cross-border data transfers
Decision Tree: 3. How will data be used & what for? (compliance and due diligence)

- Is data kept secure both when stored and transmitted?
- Clearly set out the data flow: Identify how the data will be used and shared across the value chain and for what purposes
- Justify why the data is needed in specific context
- Define/agree privacy responsibilities with your partners from the outset (and ensure the product design reflects these)
  - Contractual agreements (e.g. limiting the use of data by Analytics providers for their own commercial purposes)
  - Consider Principles / Codes of Conduct / Guidelines
Conducting a Privacy Impact Assessment (PIA) is about:
- Identifying and reducing the privacy risks of your project
- Reducing the risk of harm to individuals through the possible misuse of their personal information
- Designing a more efficient and effective process for handling data about individuals

Questions to help you assess the need for a PIA include:
- Will the project result in you/your partners making decisions or taking action against individuals in ways that can have a significant impact on them?
- Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private?
- Will the project require you to contact individuals in ways that they may find intrusive?

References: [UK's Information Commissioner's Office](https://www.ico.org.uk), [International Association of Privacy Professionals (IAPP)](https://iapp.org)
Decision Tree: 4. Conduct a Privacy Impact Assessment – cont’d
(Assessing and mitigating risk)

Impact of risk

Likelihood of risk materialising

- Manage
- Avoid
- Accept
- Control
Have you met your obligations and consumers’ rights in law... but also their expectations? e.g.:
- Is the consumer aware?
- Can they make informed choices?
- Have you obtained their consent? (where legally required)
  - Key elements of consent include: disclosure, comprehension, voluntariness, competence, agreement)
- Is data secure in transit and at rest?
- Is there a set period for which consumer data will be kept?

Does the consumer journey help gain their trust?
- Can consumers express their privacy preferences in simple steps e.g. via
  - web ‘permissions dashboard’, ‘just-in-time’ prompts, a call centre, a mobile app, a voice activated command etc.
Even if the data is not defined as ‘personal’…

- Could the data be used to impact an individual’s privacy? For example:
  - Could (non-personal) data from your service/product be combined with other data from different sources to draw inferences about a consumer’s lifestyle and impact on his/her ability to get health insurance…Or price discriminate against the consumer?

- What happens if your service changes in the future? For example:
  - Functionality of device or service changes (e.g. starts to collect consumers’ location data)
  - Data or customer profiles shared/sold to 3rd parties (e.g. advertisers) who start using consumer data for different purposes than those originally obtained for

- If any such changes occur you should:
  - Check possible impact on your business if new laws are invoked as a result of change
  - Establish processes to inform the consumers and obtain their consent where necessary
  - Provide the means for consumers to change their privacy preferences
Have you considered the roles/responsibilities of all your IoT partners? For example:
- partner mobile operator(s)
- device manufacturer(s)
- SIM vendor(s)
- Service delivery platform owner(s)
- Other 3rd party in the value chain?

Who does the customer expect to be responsible for their personal data and who would they turn to if things go wrong?
- Have you an agreement in place with your partners on how privacy complaints or concerns should be handled?
Yiannis Theodorou
Senior Manager, Regulatory & Public Policy, GSMA

YTheodorou@gsma.com, @yiathe