Context: It is very important to be clear about WHAT PbD Principles mean before we can operationalize and document them in software engineering.

**Principle 2: Privacy as the Default Setting (a.k.a. “Privacy by Default”)**

**Rationale:** This principle:
- is the strongest level of data protection and most closely associated with limiting use of data to the intended, primary purpose of the collection – the embodiment of purpose specification and use limitation;
- is the most under attack in the current era of ubiquitous, granular and exponential data collection, use and disclosure; and
- has the most impact on managing privacy risks, by effectively eliminating risk at the start of the information life cycle.

**Discussion:** After the commitment to proactively address privacy risks and issues, the starting point for designing all information technologies and systems is NO collection of personally identifying information — unless and until a specific and compelling purpose is defined.

As a rule, default user settings should be maximally privacy-enhancing. This approach is sometimes described as “data minimization” or “precautionary principle,” and must be the first line of defense. Non-collection, non-retention and non-use of personally-identifiable information support all of the other PbD principles.

Following the Work Plan, we are starting with specific processes, in this case:

**“Purpose Specificity”**

**Rationale:** Apart from having a privacy program in place, all privacy commitments must logically begin with the purpose(s) for collecting, using and disclosing personally-identifiable information. Purposes may be described in other terms, such as goals, objectives, requirements, or functionalities.

**Discussion:** Links to other Privacy Principles, notably limits on collection, use, retention, and disposal requirements, but also:
• End-to-End Security (Safeguards / Accuracy)
• Visibility and Transparency (Openness, Accountability)
• Respect for User Privacy (Informed Consent, Access, Redress)
• Embedded into Design
• Full Functionality (Positive-Sum – Win-Win)

Global Best Practices:

A broad review of current FIPPs along with relevant guidance and support documents (e.g., PIAs, TRAs, privacy evaluation frameworks and audit criteria, other relevant standards) indicate that the common “core” criteria for Purpose Specification are that purposes for collection, use and disclosure of personally-identifiable information must be:

1. identified and documented (usually in a privacy policy)
2. made known to the individual
3. the measure against which all use(s) must be assessed

Additional guidance elaborates on these core requirements, e.g. purposes must be:

• “explicit” and “relevant” to circumstances
• “Fair and lawful”
• Made “easily available”
• Timely (e.g., made available not later than time of collection)
• “Clear,” in plain language, easy-to-read,
• Subject to special conditions in the case of sensitive data
• Not subject to any change without additional notice and consent
• Subject to periodic review and assessment
• Commutative, i.e., transferable (to third parties)

Privacy by Design aspires to the highest global standard of privacy protection. To these core requirements we add:

• **Purposes must be limited and specific**

e.g. Global Privacy Standard (GPS): 3. **Purposes**

An organization shall specify the purposes for which personal information is collected, used, retained and disclosed, and communicate these purposes to the individual at or before the time the information is collected. Specified purposes should be clear, limited and relevant to the circumstances.

• **Purposes must be written in such a way so to be amendable to engineering controls**

This may involve creating sub-purposes/objectives/requirements. Examples of purposes that are far too broad and vague include: “To serve you better” “to improve performance” “To combat fraud” and “to comply with laws” etc.
Specified purposes typically apply to organizations as a whole, and are predominantly non-technical (policy) in nature, e.g., have a written policy and make it available to customers.

**TO SUMMARIZE:** Do not collect, use or disclose PII unless a positive case is made for the processing of each data item!

Purpose specificity does NOT mean collection, use and disclosure is prohibited by default!

Depending on the application or domain, building a positive case may entail, for example, creating detailed data flow maps, carrying out privacy risk and impact assessments, documenting legal requirements, and seeking/obtaining user consent.

**Questions / Challenges for TC Members:**

- How to adapt Purpose Specificity to the (internal) software engineering process?
- How to express Purpose Specificity in software engineering terms?

Needed: inventory of methods and techniques for Software Engineers to express Privacy by Default / data minimization in Purpose Specificity, e.g. privacy-enhancing architectures that minimize visibility, linkability, and identifiability of personal data processing, e.g.:

- De-identification methods
- Client-side processing (e.g. Zero-Knowledge proofs)
- Controls on use, disclosure and retention

+++