The Bluffer's Guide to Agile Integration For Privacy Professionals

This guide is intended for a Privacy Pro that is just tipping their toes into the agile pool and finding the water cold. Corners have been cut, snark attempted, and purists annoyed.

Product Owner. This is the most important person whom a Privacy Pro must convert to their cause. They're already stressed out, and you'll be yet another source of constraints. Befriend them, buy them a drink.

Service Design (SD). The key activity where a Privacy Pro can ensure that contextual integrity holds. Befriend Service (or UX, User Experience) Designers as well as *Product Owners*, and buy them drinks as well.

Technical Project Manager (TPM). If you see them, it could be a sign of complex inter-team initiative or an organization in transformation. You need to figure out what they do in your organization – often they are key people for networking.

Jira. Some hate it, and some loathe it. But really, it's just a ticketing system, and it is how it's used that annoys people. Don't go with the haters. See "*Backlog items*".

Backlog items. These are the things that an agile team has on their plate. They come in different abstraction levels. Privacy activities and risk mitigations need to become backlog items, otherwise they do not exist.

Epic. A *backlog item* that encapsulates a larger business value. Often split into tasks. Don't let privacy to be relegated into a "Privacy Epic", to be paid lip service there, unless that Epic truly has a business value proposition, and as an initiative, a beginning and an end.

User Story. A way to describe what a user expects to happen and why. Often used as a *backlog item* type. Try to get contextual integrity expressed by a user story.

Threat modeling. A security activity that is about finding architectural and design level risks. If you find someone advocating this, try to figure out how to do PIAs together.

Scrum Master. In some teams who do textbook Scrum, this person removes the team's impediments. Probably a coach-y type. They will be able to tell you how to best introduce privacy-related activities in that specific team.

Scrum. *Kanban* with training wheels. A way to manage Work in Progress limits by selecting a subset of things and working only on them for a couple of weeks. Doesn't really make a difference privacy-wise whether the team does Scrum or Kanban. Just don't assume agile equals Scrum.

Kanban. A way to manage Work in Progress limits by pulling in new work when previous one is ready. Always accompanied with a Toyota backstory. An adult alternative to *Scrum*. Doesn't really make a difference privacy-wise whether the team does Scrum or Kanban.

SAFe. An enterprise agile framework. Privacy Pros will be most interested in the *Portfolio Kanban* because that might hold a place to introduce DPIAs and discussions of legality. But not everyone does Portfolio Kanban.

Developers. When they're happy and believe in your mission, they're our best safety net against stupid privacy mistakes. Try not to annoy them with mandatory checklists.

Definition of Done (DoD). The team's description of when whatever they're building is ready. Usually quality aspects. Many have tried to enforce compliance through mandatory DoDs, and most of them have failed. Don't use DoD as a compliance gate.

Definition of Ready (DoR). The team's criteria of when they believe they understand what they're going to do. If you can get the team to assess a need for a PIA here, it has a chance of survival. But the PIA itself should be a *Backlog item*. Don't confuse DoR with the *Definition of Done (DoD)*.

Acceptance Criteria. The *backlog item* might have a list of Acceptance Criteria that describe when the item is complete. Privacy and security needs could live here, too, if separate backlog items turn out to be a hard sell. But better to have PIAs and privacy features as real backlog items instead.

Sprint. A typically 2-week timebox that is used to limit the Work in Progress in *Scrum*. Don't assume every team does sprints.

Program Increment (PI). A typically 2-month timebox that is used in *SAFe*. If your org has these, probably a good idea to attend PI planning events to see what's up and whether you've missed the train already. Then talk to Product Owners directly.

DevOps. A culture and a set of practices and tools that allows a development team to have ownership of their product over its complete lifecycle. Privacy-wise, most interesting discussions revolve around operational security and DSAR.

Product Briefs. These are documents that describe what is going to be built, sometimes for product portfolio planning. You should try to get a "privacy considerations" section into this template.

Architectural Decision Records (ADRs). Essentially short memos of important decisions that usually live in the version control system. If your organization does these, see if these encapsulate any privacy-related concerns. Then try to increase awareness of privacy in the crowd who tend to write these, and you get stickiness.

Developer Experience (DX). Good DX means that developers are happy and can get into the flow. The quickest way to destroy DX is to introduce a mandatory compliance checklist that needs to be gone through in a milestone meeting.

By Antti Vähä-Sipilä, avs@iki.fi.
https://fokkusu.fi/tbgtai.pdf