DATENSCHUTZ UND AGILE SOFTWAREENTWICKLUNG

Erfahrungen und Vorgehen in der Praxis

Softwareentwicklung bei der Deutschen Telekom

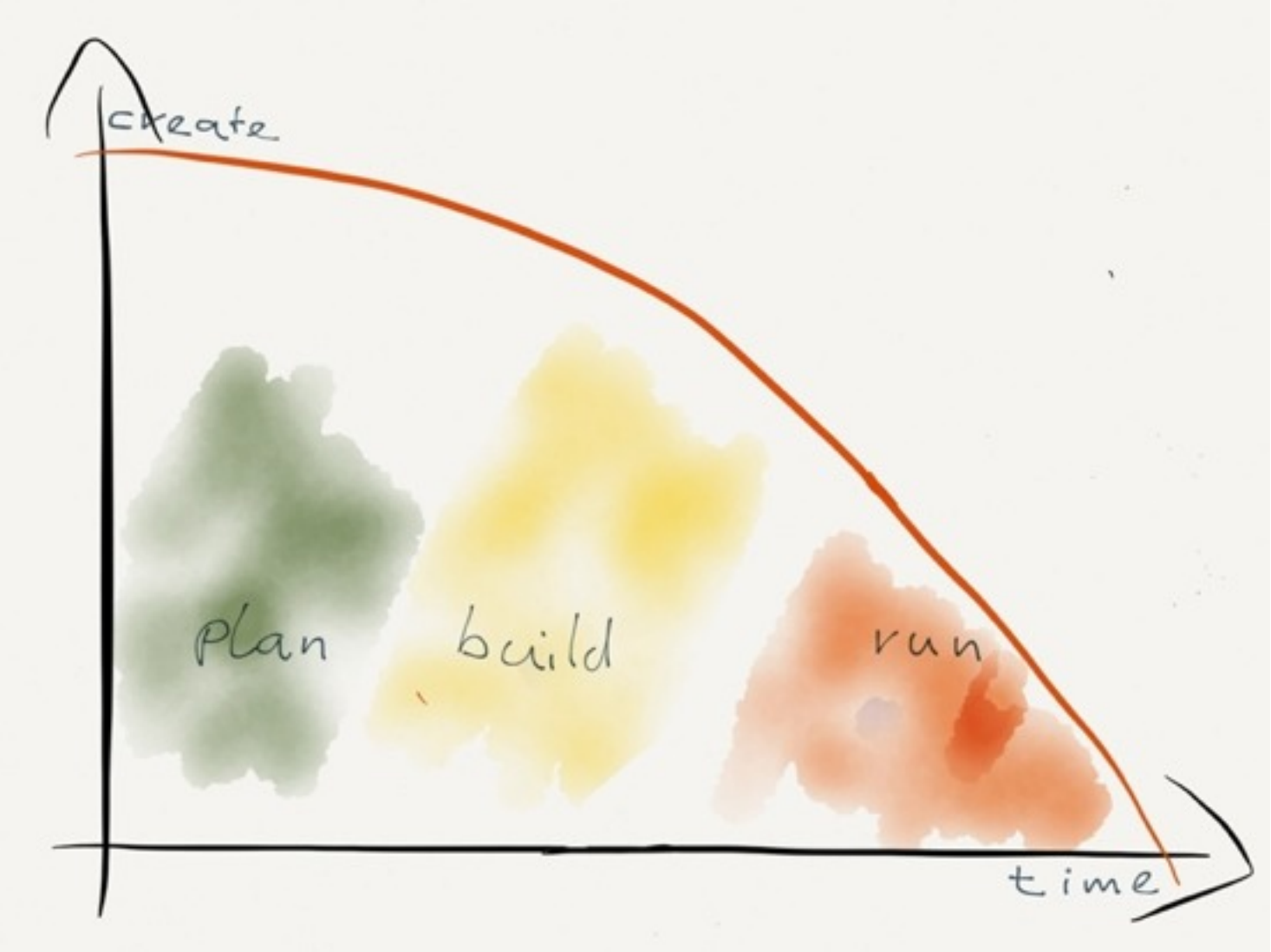
Historie:

- explizite Datenschutzberatung von Software- und Systementwicklungen seit 1996

- Vorgaben für die Dokumentation datenschutzrechtlich relevanter Merkmale (technische und organisatorische Maßnahmen)“Datenschutzkonzept - DSK“ seit 2001

- standardisierte Datenschutz- und Datensicherheitskonzepte - SDSK seit 2010

Grundvoraussetzung: frühzeitige Beteiligung



Die 7 Grundprinzipien von Privacy by design

Der 1. Grundsatz Proactive not Reactive;
Preventative not Remedial betont die Notwendigkeit eines proaktiv auch beratenden, im Unterschied zu einem bloß reaktiv sanktionierenden Datenschutz.

Der 2. Grundsatz Privacy as Default;
betont den maximal erreichbaren Grad von Privatssphäre, der dann gegeben ist, wenn in jedem System in der Standardeinstellung zunächst einmal keinerlei personenbezogene Daten verarbeitet werden (dürfen). Wenn eine Person von sich aus nicht agiert, soll sie sicher davon ausgehen können, dass ihre Privatsphäre intakt ist und bleibt.

Der 3. Grundsatz Privacy Embedded into Design;
betont, dass der Schutz der Privatssphäre in die Systeme ganzheitlich und integrativ eingebaut sein muss, ohne deren Funktionalität zu beeinträchtigen.

Der 4. Grundsatz Full Functionality – Positive Sum, not Zero-Sum;
soll ermutigen, dass es durch Abstimmung aller Interessen zu einer Win-Win-Situationen kommen und Mehrsummengewinne eingestrichen werden können.

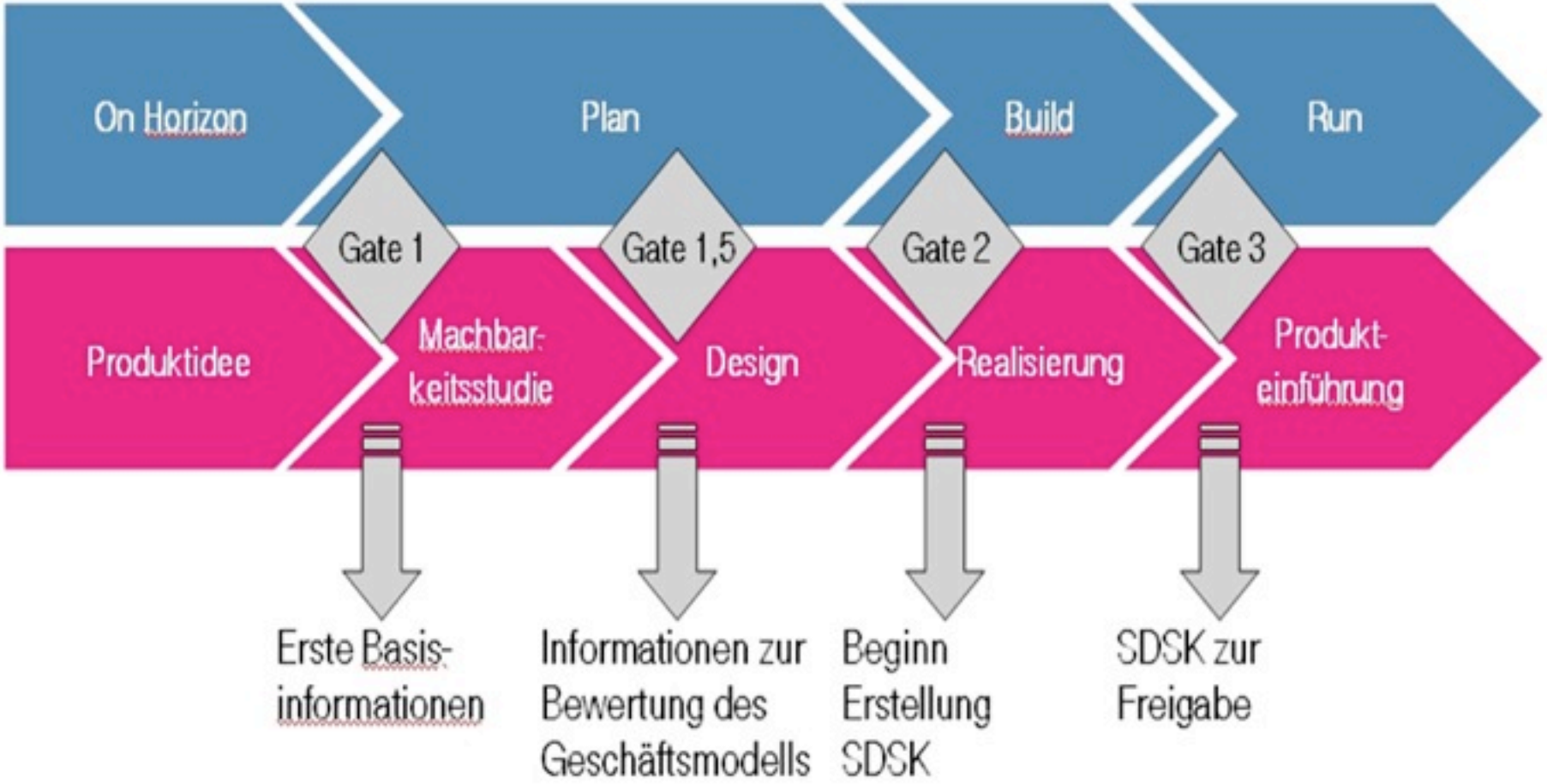
Die 7 Grundprinzipien von Privacy by design

Der 5. Grundsatz End-to-End-Security – Lifecycle Protection;
betont die Angewiesenheit des Privatsphärenschutzes auf die Mechanismen zur Herstellung von Datensicherheit. Auf der Prozessebene bedeutet dies, dass die Prozesse der Datenverarbeitung immer von Anfang bis Ende zu betrachten sind.

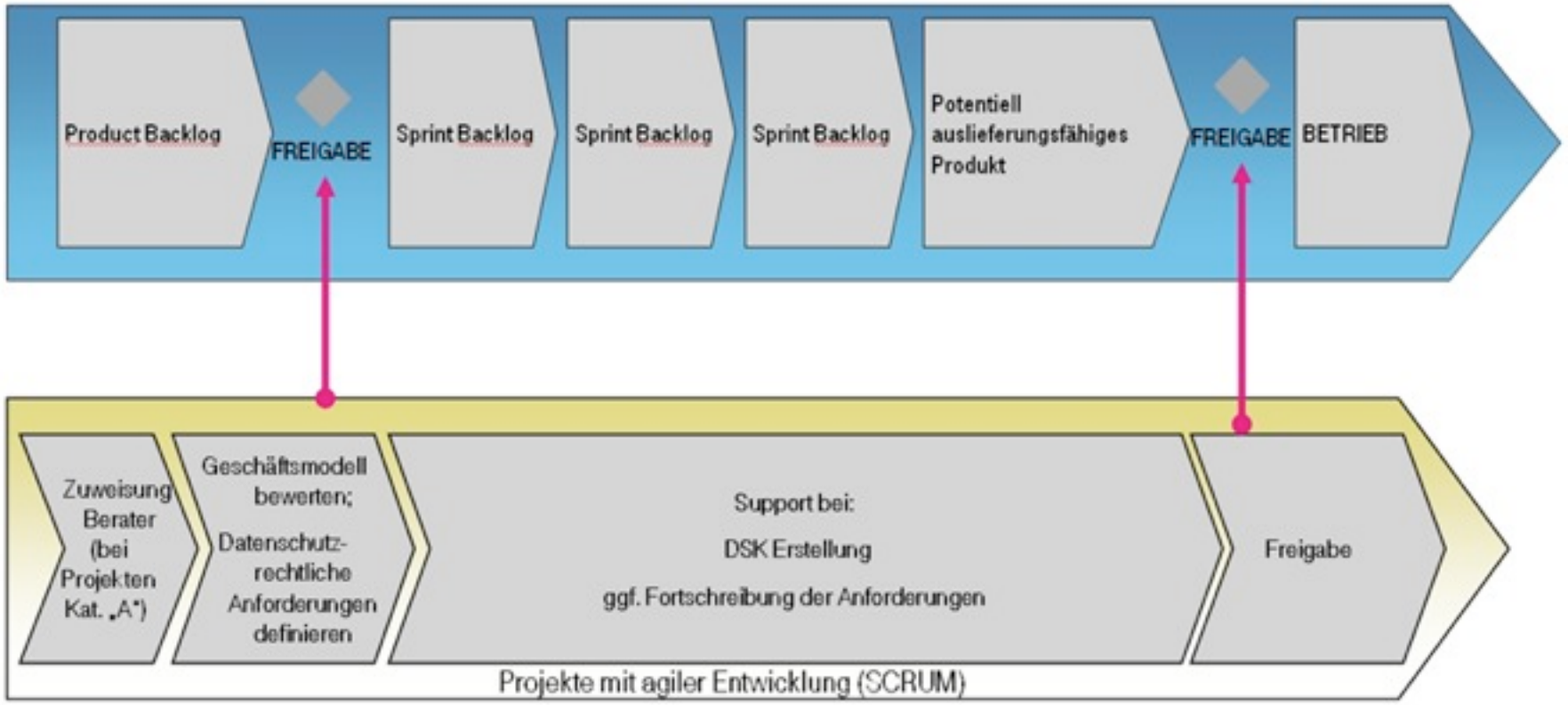
Der 6. Grundsatz Visibility and Transparency;
stellt auf die Notwendigkeit der Prüfbarkeit von Systemen und Prozessen der Verarbeitung personenbezogener Daten ab. Transparenz mit Blick auf die Prozesse und technischen Systeme in den Organisationen ist eine Voraussetzung für jede Prüfbarkeit bzw. Prüffähigkeit.

Der 7. Grundsatz lautet Respect for User Privacy;
Dieser Grundsatz bildet den Abschluss der Auflistung der Grundsätze, und zugleich den Anfang von allem, was im Zentrum der Bemühungen von PbD stehen soll. Aber dieser Grundsatz ist nicht nur Appell, sondern hat wiederum eine operative Seite und den Anspruch, dass Techniken nutzerzentriert funktionieren sollen.

Softwareentwicklung nach dem Wasserfallmodell



Softwarentwicklung nach Scrum



Grundannahmen

Auch bei agiler Softwarentwicklung muss dokumentiert werden. Am Ende eines Scrum Zyklus steht eine fertiges Produkt inclusive der erforderlichen Dokumentation.

Der Idealzustand - Datenschutzkompetenz ist immanent im Entwicklungsteam vorhanden - wird nur selten erreicht.

Übergeordnete Anforderungen (Privacy, Legal, Compliance) werden bei aller Euphorie und Agilität leicht vergessen.

Ganz böse Zungen behaupten, man müsse SCRUM nur rückwärts lesen...

Erfahrungen, Zusammenfasung

Datenschutz und agile Softwarentwicklung ist kein Widerspruch.

Frühzeitige Einbindung ist unabdingbar. Ebenso regelmäßiger Austausch, insbesondere bei Änderungen im Product Backlog bzw. an definierten Verarbeitungen personenbezogener Daten u.ä.

Die Benennung eines Verantwortlichen für Datenschutz im Projekt ist dringend empfohlen.

Wenn möglich sollen Anforderungen des Datenschutzes definiert vorliegen. (Requirement sets)

Eine minmale Dokumentation soll bereits zu Beginn erstellt werden. (Steckbrief)

Vielen Dank !

frank.wagner@telekom.de