Modellierung und Validierung von Datenschutzanforderungen in Prozessmodellen

Sven Feja[1], Sören Witt[1], Andreas Brosche[1], Andreas Speck[1] und Christian Prietz[2]

[1]Arbeitsgruppe Angewandte Informatik (Wirtschaftsinformatik)
Christian-Albrechts-Universität zu Kiel

[2]Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

25. März 2010

Überblick

Grundlagen
- Datenschutz
- Datenschutzanforderungen
- Prozessmodelle

Integrierte Datenschutzmodellierung
- G-CTL – Grafische Anforderungsmodellierung
- MultiView – Komplexität in Modellen beherrschen
- Validierung

Zusammenfassung

Datenschutz – wieso?

- Einerseits gesetzliche Verpflichtung
- Andererseits Chance
- Missachtung birgt erhebliches Schadenspotential

Datenschutzanforderungen

Rechtlicher Hintergrund

- Gesetz regelt Rechte, Pflichten und Voraussetzungen im Umgang mit personenbezogenen Daten
- In Deutschland:
  - Bundesdatenschutzgesetz
  - Landesdatenschutzgesetze
  - bereichsspezifische Regelungen
- Gesetze unterliegen ständigem Wandel
  - vgl. Steuergesetze und Wartungsaufwand für Software
- Gesetze sind oft auslegungsbedürftig
- Anforderungen schwierig abzuleiten

Datenschutzanforderungen

Rechtlicher Hintergrund

Grundprinzipien beim Umgang mit personenbezogenen Daten:

- Zulässigkeit
- Zweckbindung
- Beachtung der Rechte Betroffener
- Datenvermeidung & Datensparsamkeit

Datenschutzanforderungen

Schutzziele

- Fundamentale/abstrakte Beschreibung von Anforderungen i.Z.m. der Verarbeitung personenbezogener Daten
- Beschrieben und systematisiert durch Rost/Pfitzmann (ULD/TU-Dresden)
- unabhängig von konkreten Gesetzestexten
- Beispiele: Vertraulichkeit, (Un-)verkettbarkeit, Transparenz
- Aber: Nicht alle Anforderungen werden durch Schutzziele erfasst (z.B. Zulässigkeit, Einverständnis)

Datenschutzanforderungen

Schutzziele

- Annahme:
  Einhaltung der Schutzziele bedeutet weitgehende Einhaltung der datenschutzrechtlichen Bestimmungen
- Schutzziele ermöglichen einfacheres Ableiten von Anforderungen
- Bestimmte Anforderungen müssen aus Gesetzen abgeleitet werden

Datenschutzmanagement

Eine wichtige Grundlage:

Definierte und abgesicherte Prozesse

Eine wichtige Aufgabe:

Prozesse müssen Datenschutzanforderungen genügen

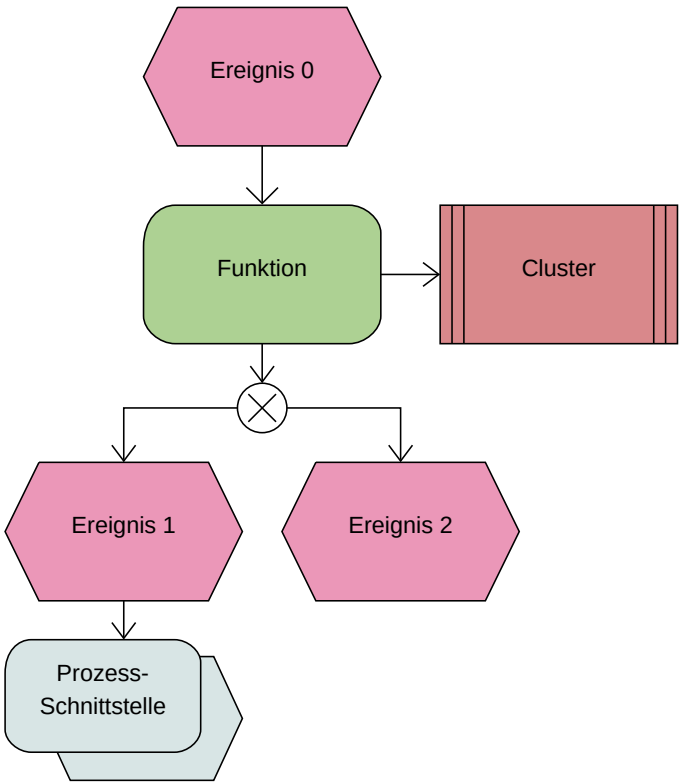
Überblick

Grundlagen
- Datenschutz
- Datenschutzanforderungen
- Prozessmodelle

Integrierte Datenschutzmodellierung
- G-CTL – Grafische Anforderungsmodellierung
- MultiView – Komplexität in Modellen beherrschen
- Validierung

Zusammenfassung

Ereignisgesteuerte Prozesskette (EPK)



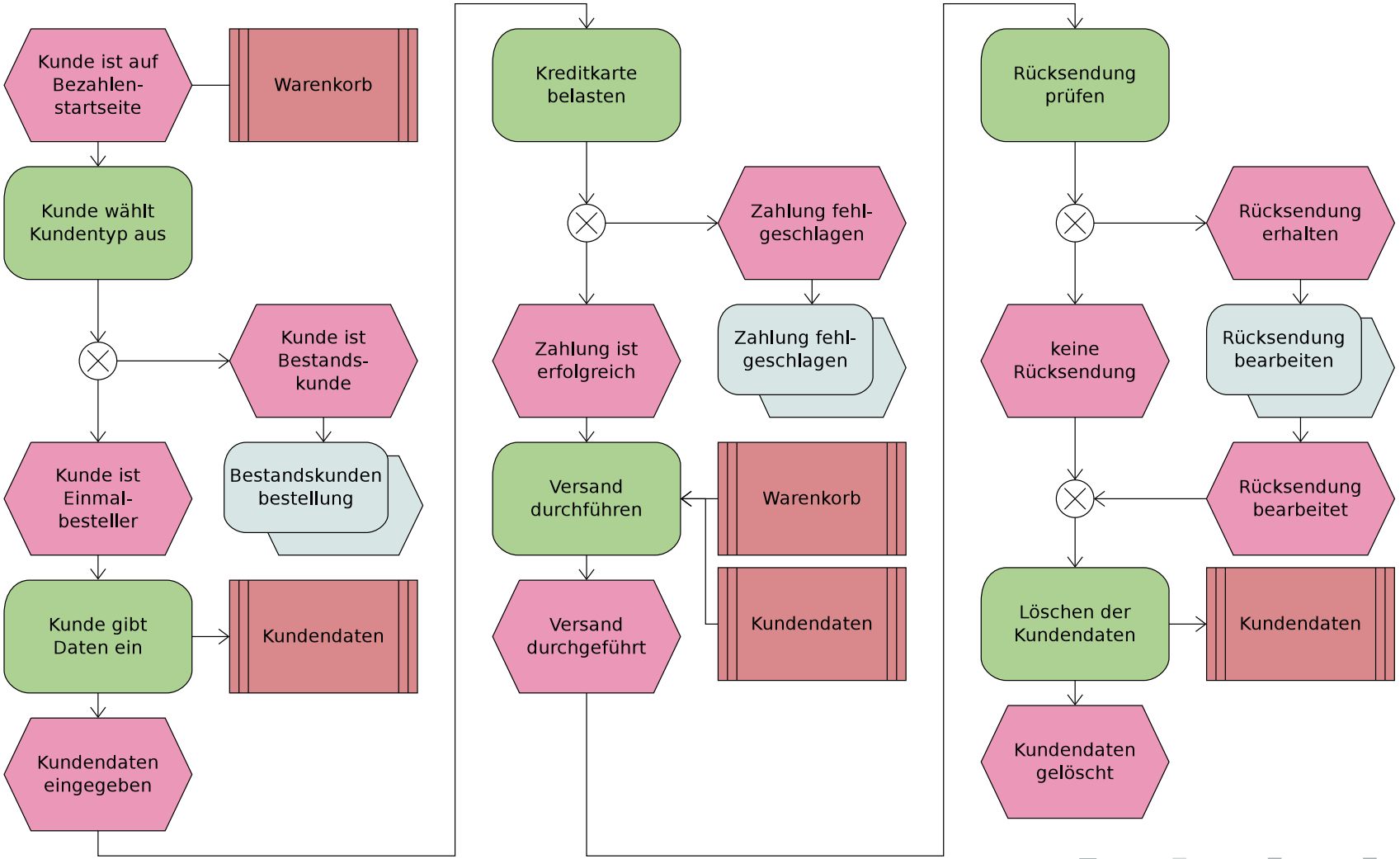
Wesentliche Bestandteile einer EPK:

- Ereignisse
- Funktionen
- Operatoren und Kontrollfluss
- Cluster (Daten)
- Prozessschnittstellen

Eigenschaften:

- Verständlich für (Nicht-)Informatiker
- Formalisierbar bei Einhaltung einer definierten Syntax und Semantik
- Eine Basis für Modellgetriebene Softwareentwicklung

Ein Beispielprozess



Datenschutzmodellierung in EPKs

Problem:

- Es fehlen Ausdrucksmöglichkeiten für...
  - formale Anforderungen, die Prozesse erfüllen müssen (z.B. die Löschung nicht mehr benötigter Daten)
  - Datenschutzbelange (z.B. Kennzeichnen, ob ein Datum überhaupt datenschutzrechtlich relevant ist)
- Überprüfung: Genügen die Prozesse den Anforderungen?

Überblick

Grundlagen
- Datenschutz
- Datenschutzanforderungen
- Prozessmodelle

Integrierte Datenschutzmodellierung
- G-CTL – Grafische Anforderungsmodellierung
- MultiView – Komplexität in Modellen beherrschen
- Validierung

Zusammenfassung

Integrierte Datenschutzmodellierung

- Formale, grafische Notation für Anforderungen **auf Prozessmodellebene**
- Möglichkeit zur Verallgemeinerung der Anforderungen (Wiederverwendbarkeit)
- Annotation von Prozessen mit Metainformation
- Validierung der Prozessmodelle auf Einhaltung der Anforderungen

Überblick

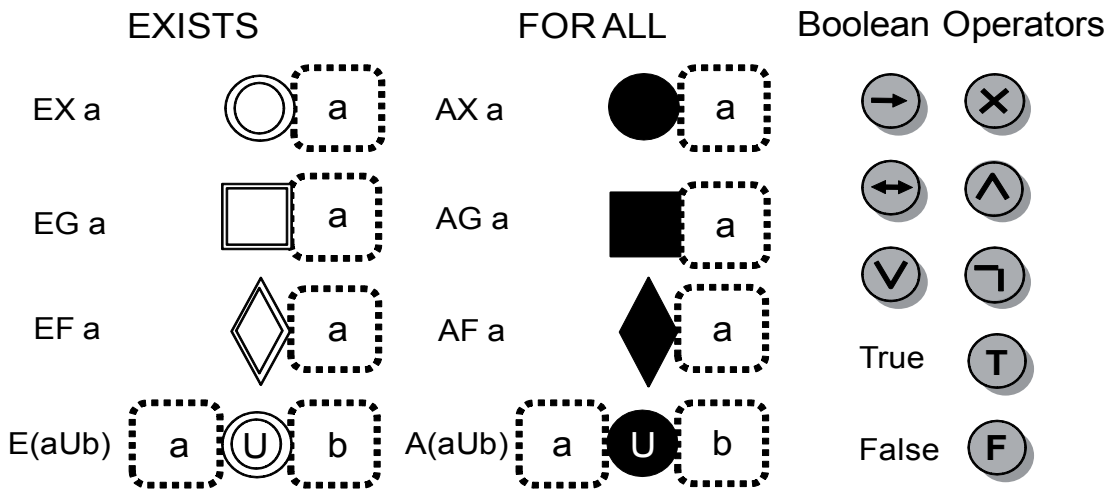
Grundlagen
- Datenschutz
- Datenschutzanforderungen
- Prozessmodelle

Integrierte Datenschutzmodellierung
- G-CTL – Grafische Anforderungsmodellierung
- MultiView – Komplexität in Modellen beherrschen
- Validierung

Zusammenfassung

G-CTL – Grafische Anforderungsmodellierung

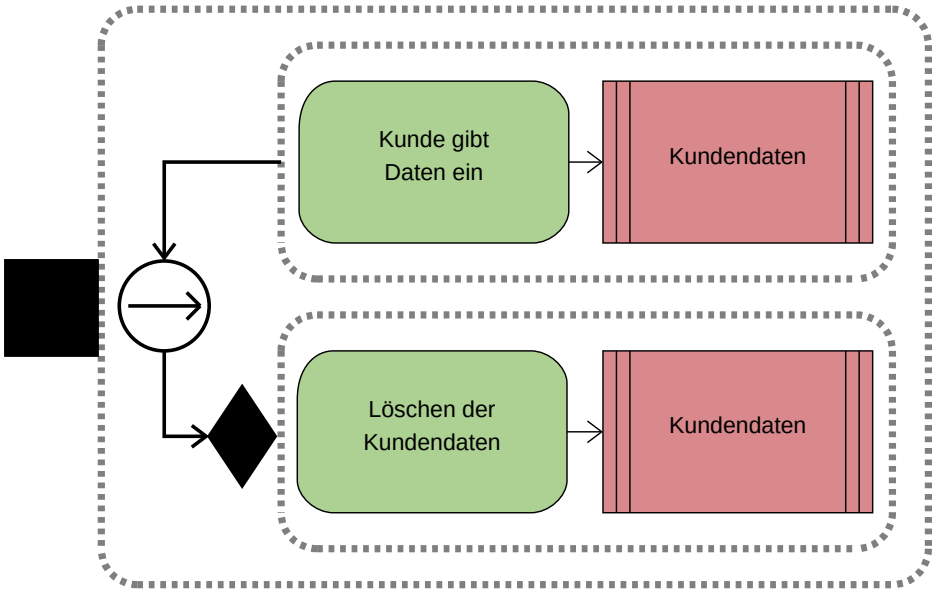
- Grafische Notation für “Computation Tree Logic” (CTL)
- Grafische Umsetzung der CTL-Operatoren



- Atomare Aussagen in G-CTL werden durch Muster aus Prozesselementen beschrieben
- Anforderungen werden durch eine oder mehrere G-CTL-Regeln ausgedrückt

Datenschutzanforderung in G-CTL

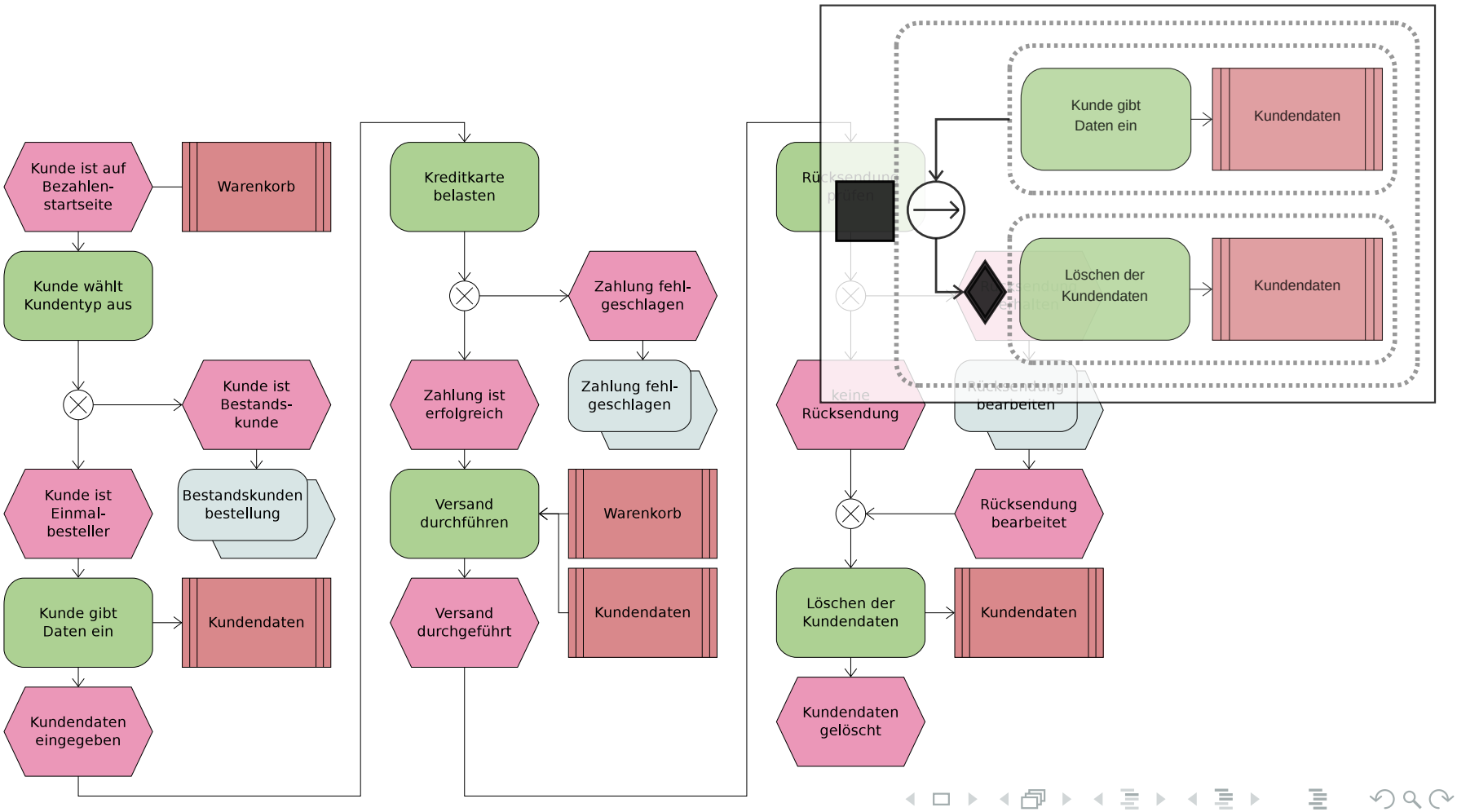
Beispiel: Löschregel



Prosa: Existiert eine Funktion *Kunde gibt Daten ein*, die ein Cluster *Kundendaten* erzeugt, dann muss auf jedem darauf folgenden Pfad eine Funktion *Löschen der Kundendaten* existieren, die das Cluster *Kundendaten* löscht.

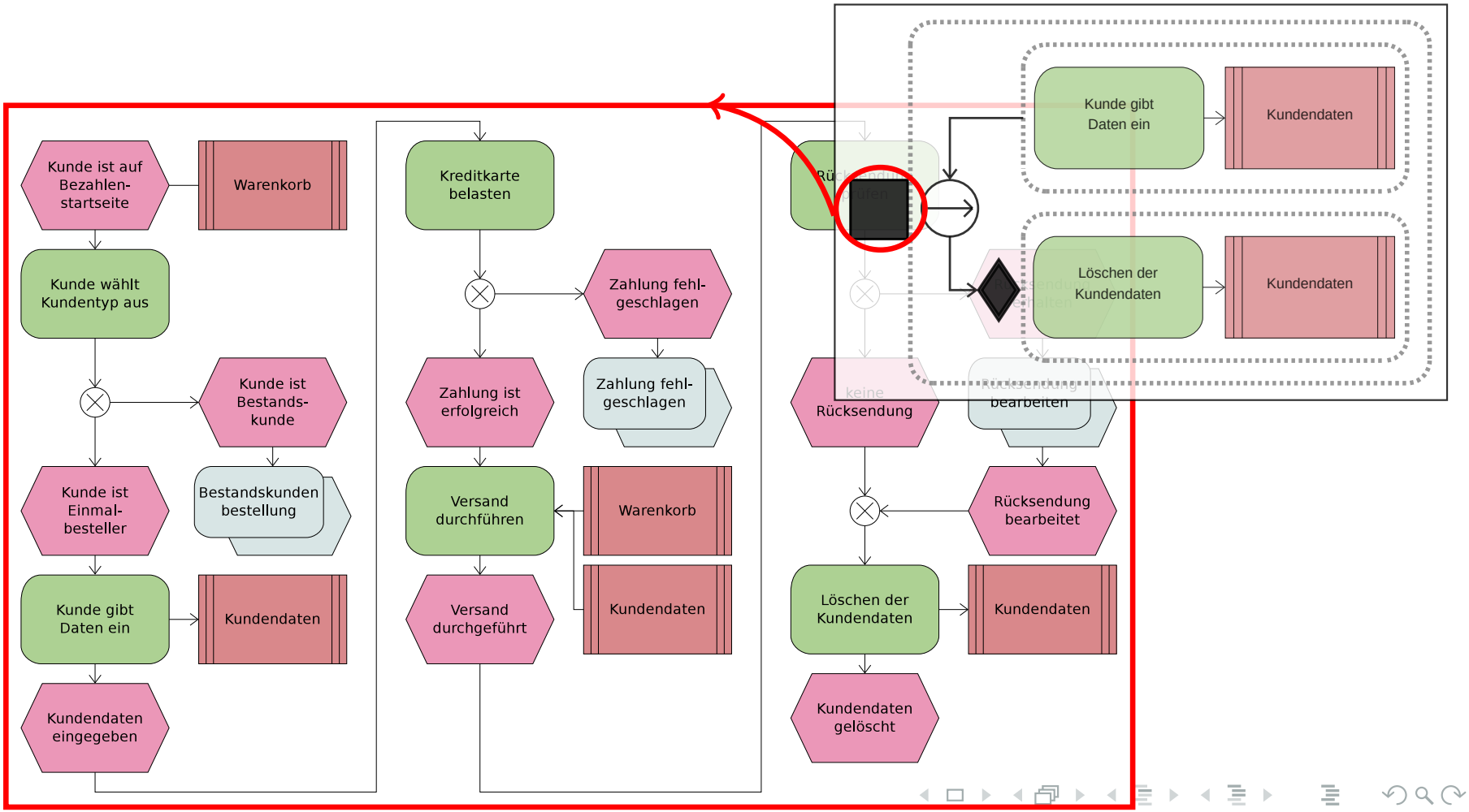
Datenschutzanforderung in G-CTL

Beispiel: Löschregel



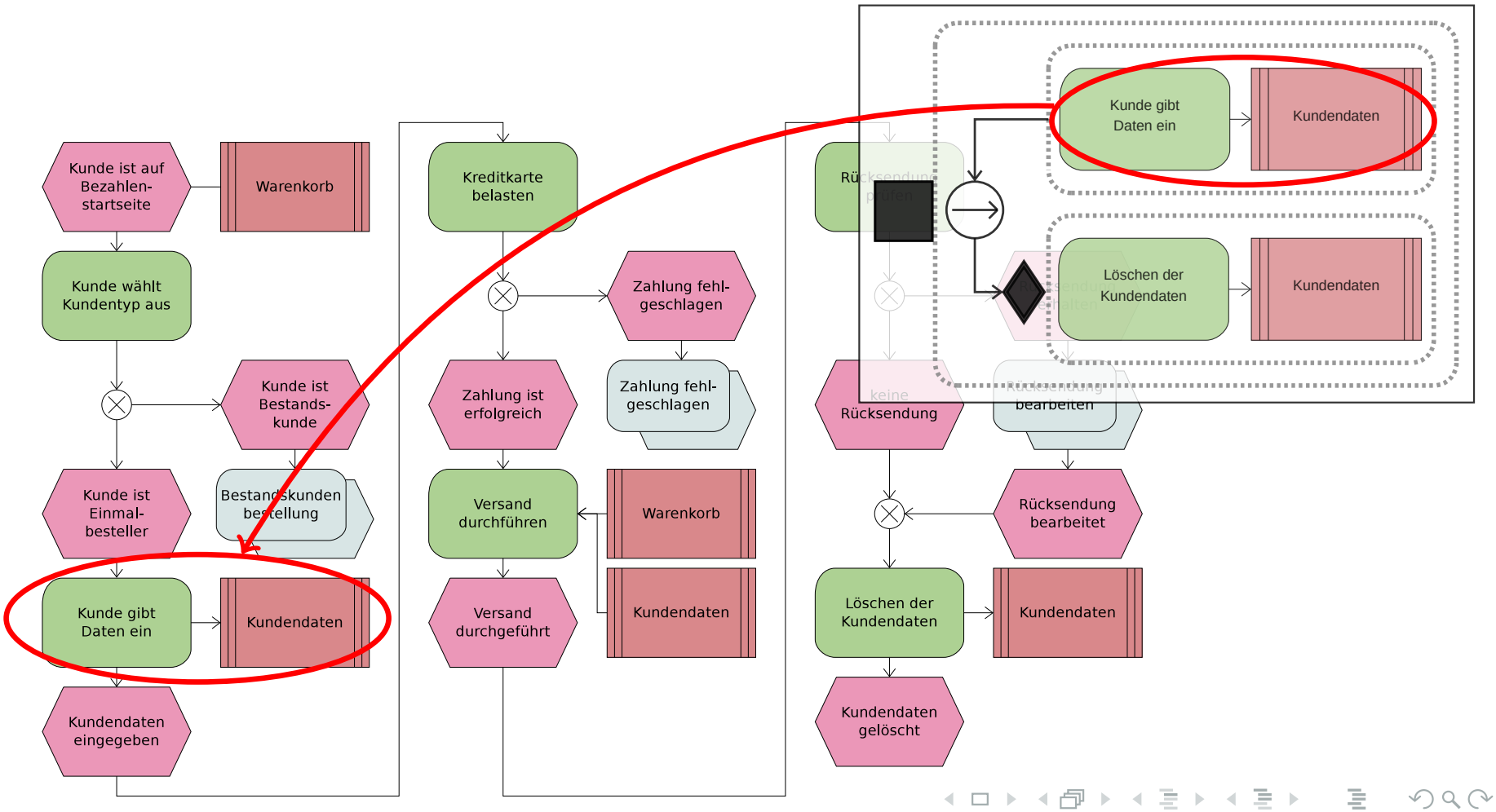
Datenschutzanforderung in G-CTL

Beispiel: Löschregel



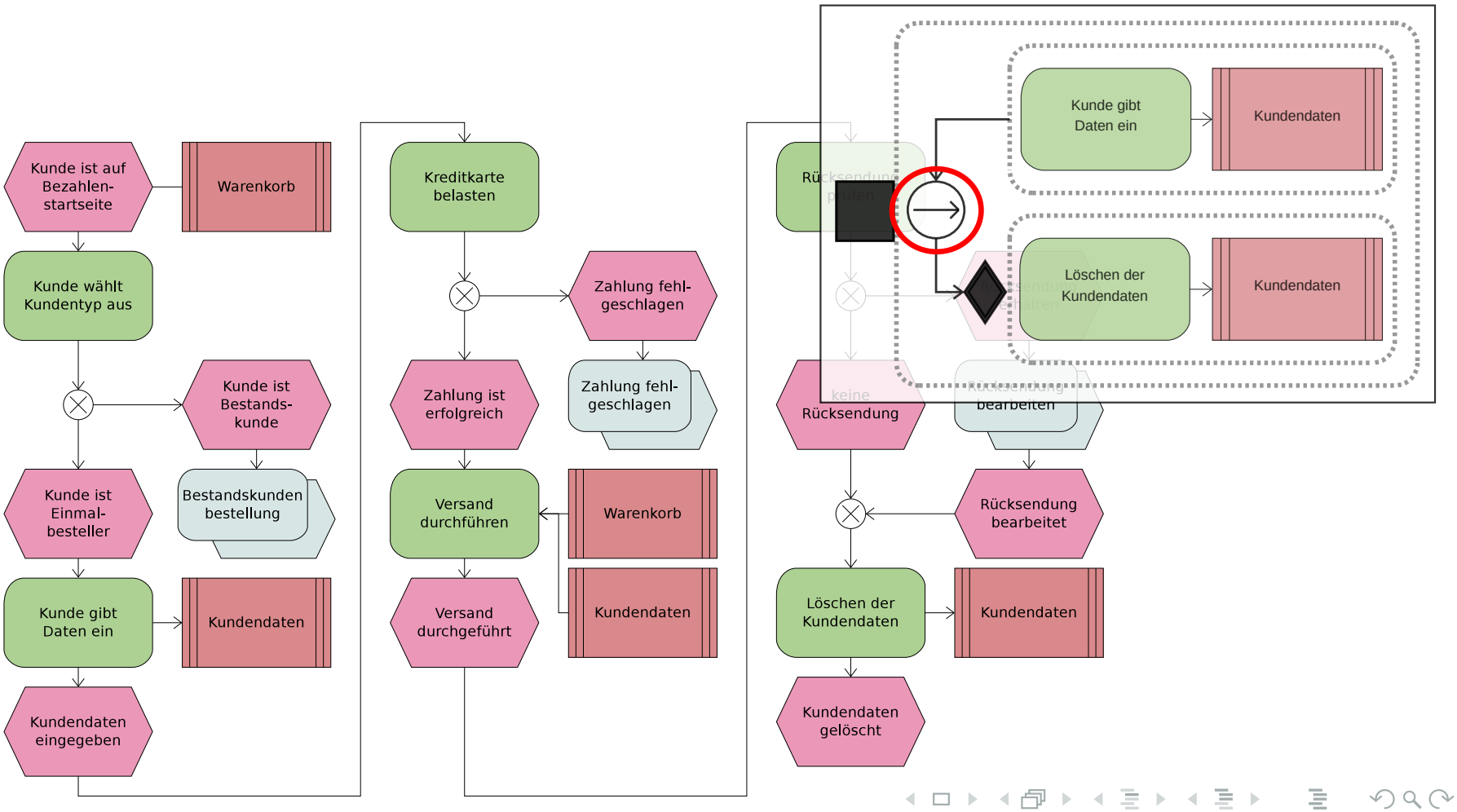
Datenschutzanforderung in G-CTL

Beispiel: Löschregel



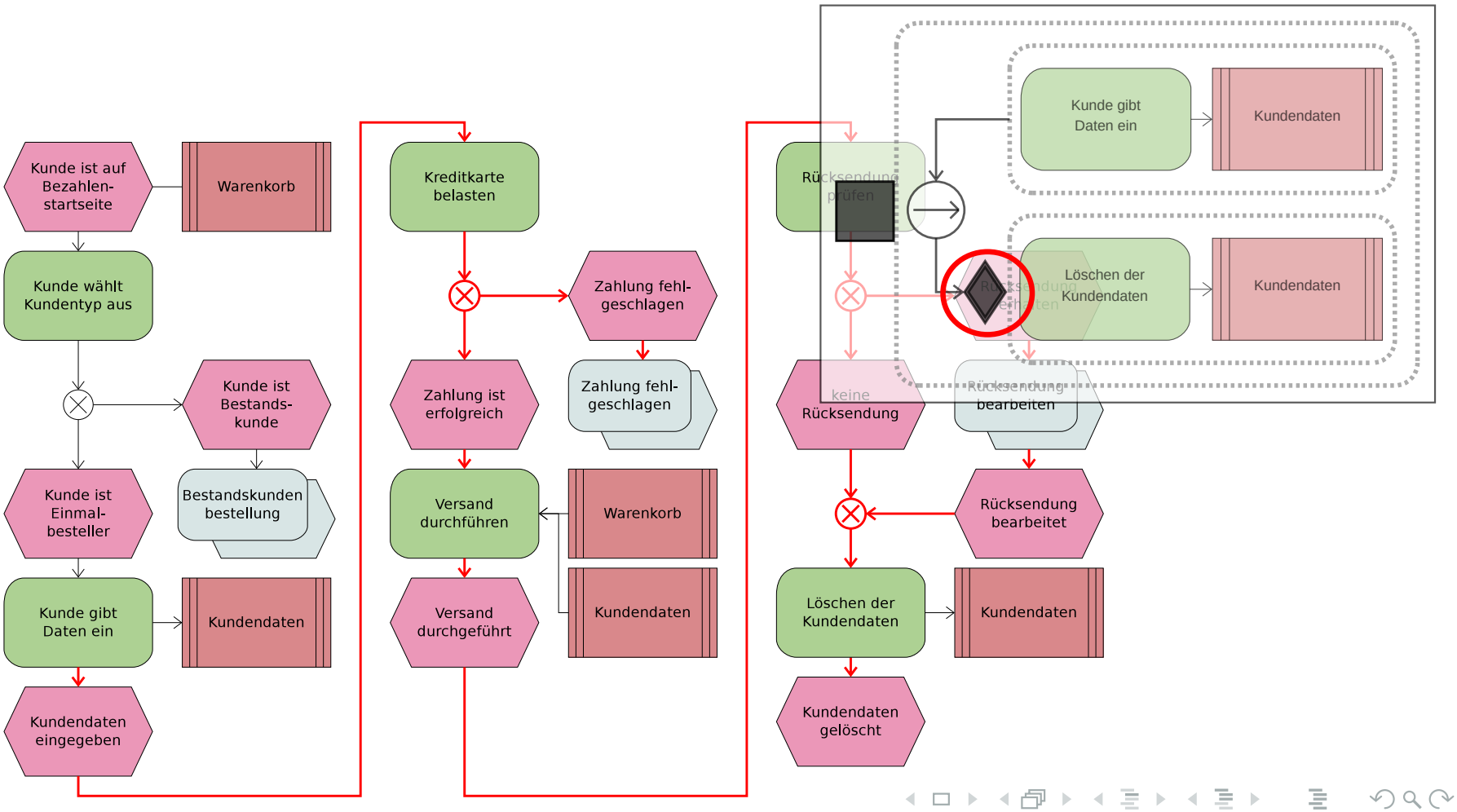
Datenschutzanforderung in G-CTL

Beispiel: Löschregel



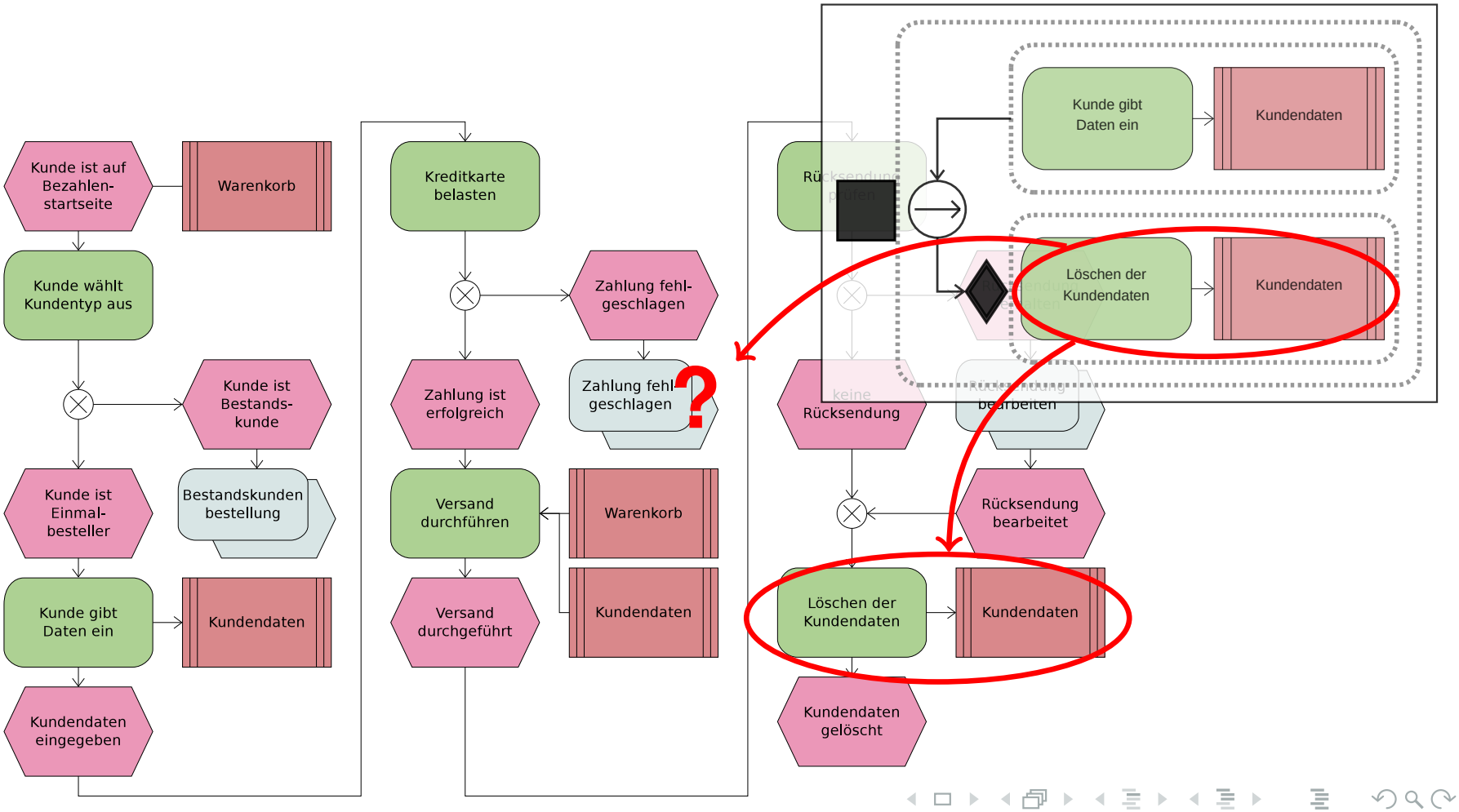
Datenschutzanforderung in G-CTL

Beispiel: Löschregel



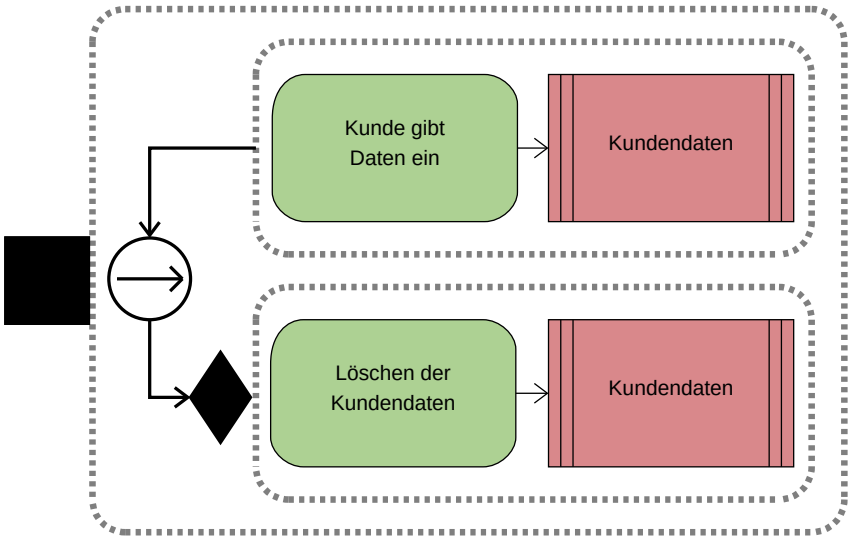
Datenschutzanforderung in G-CTL

Beispiel: Löschregel



Datenschutzanforderung in G-CTL

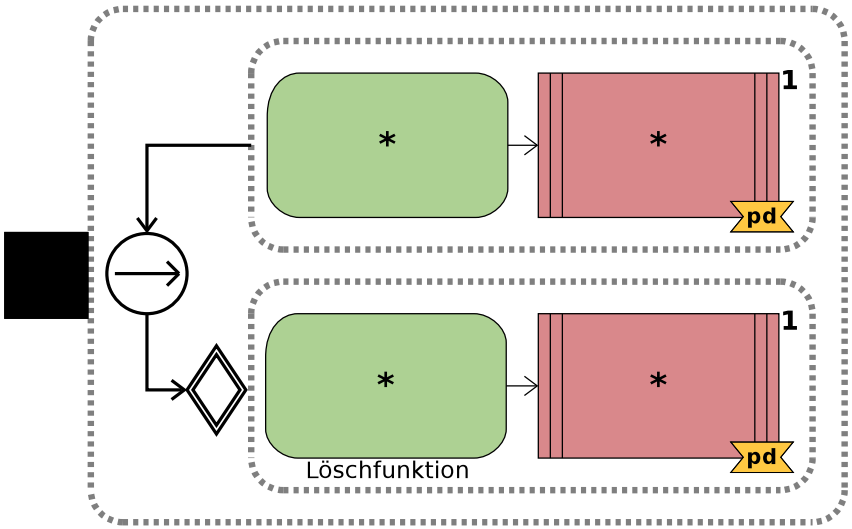
Beispiel: Löschregel



- Nur anwendbar auf Prozesse mit genau diesen Elementbezeichnern
- Greift nicht bei anderen Funktionen, die ebenfalls personenbezogene Daten verarbeiten

Naheliegender Wunsch: Allgemeinere Formulierung der Regel
Ziel: Bessere Wiederverwendbarkeit

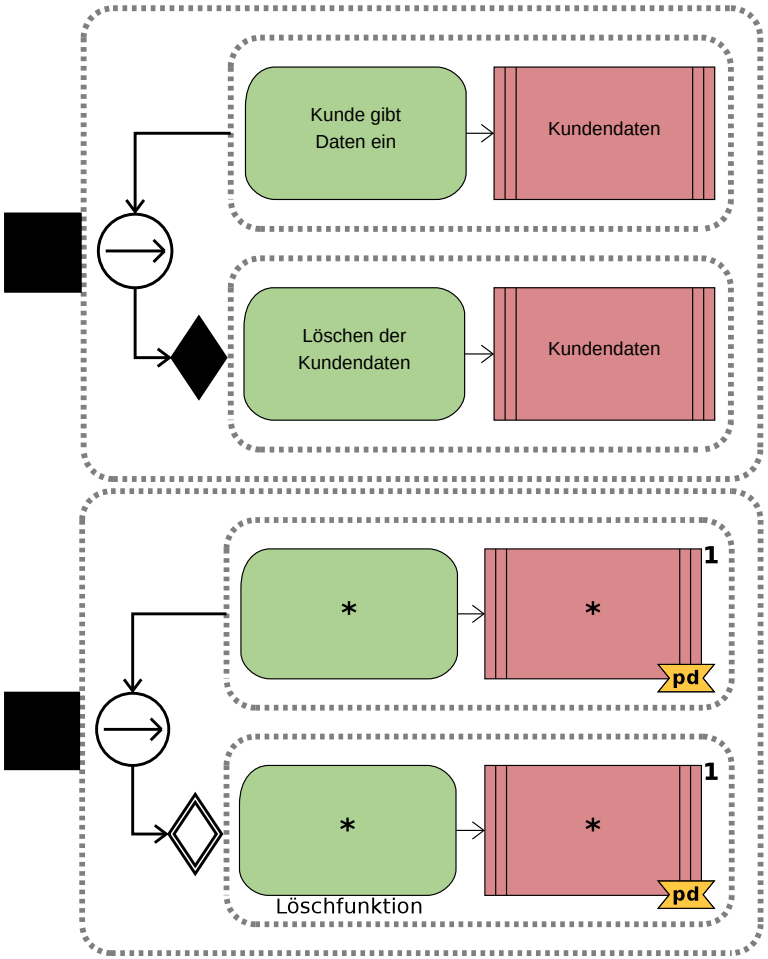
Verallgemeinerte Löschregel



Prosa: Existiert eine Funktion, die personenbezogene Daten erzeugt, so muss eine *Löschfunktion* auf mindestens einem nachfolgenden Pfad im Prozess erreichbar sein, die genau diese personenbezogenen Daten löscht.

Verallgemeinerte Löschregel

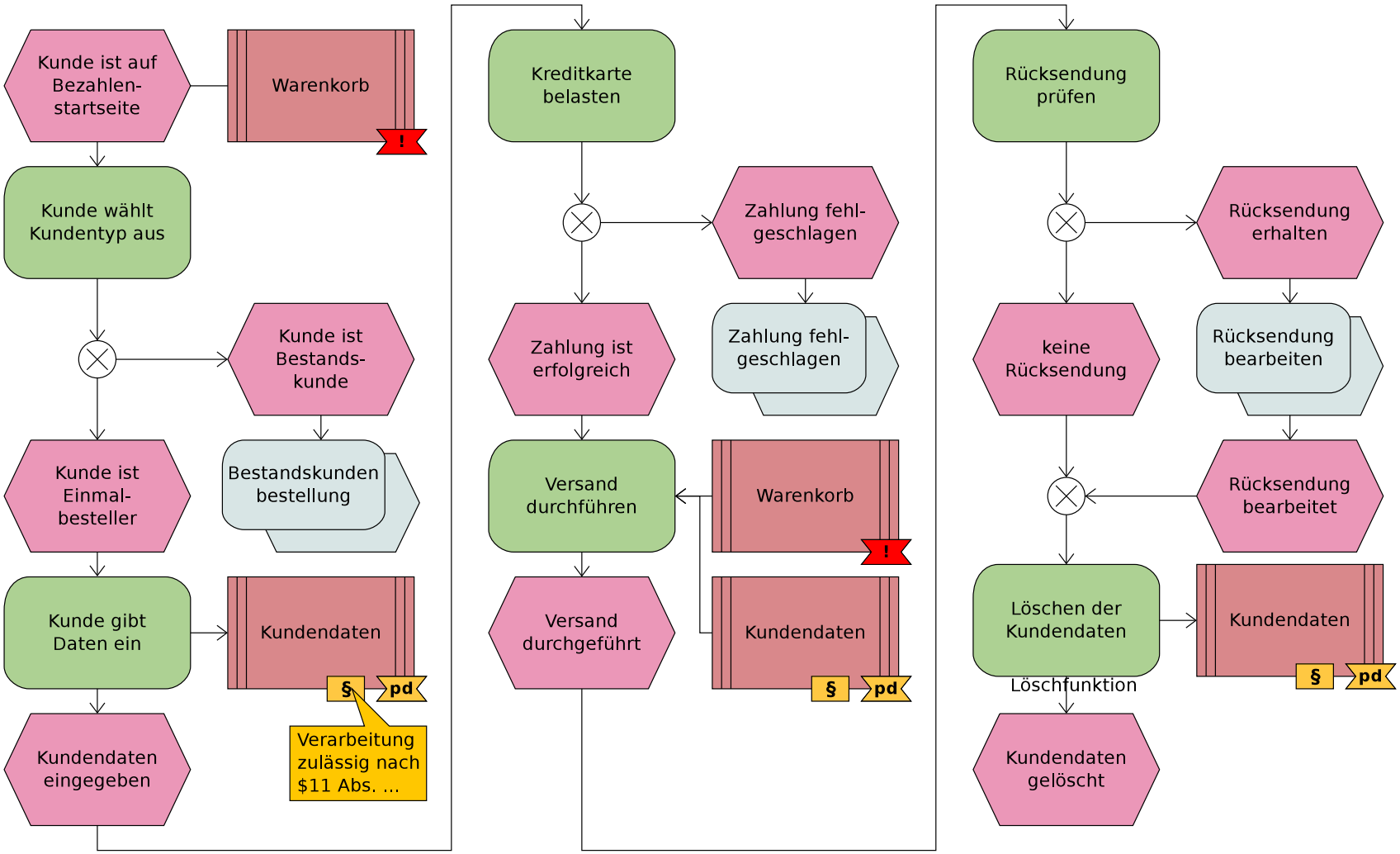
Unterschiede zur speziellen Regel



- Platzhalter statt Namen
- Erkennung relevanter Prozessteile an Eigenschaften
- Eigenschaften durch Attribute annotiert:
  - personenbezogenes Datum
  - Löschfunktion
- Identität der Cluster explizit gefordert
- Löschung erfolgt nicht zwingend – muss nur möglich sein

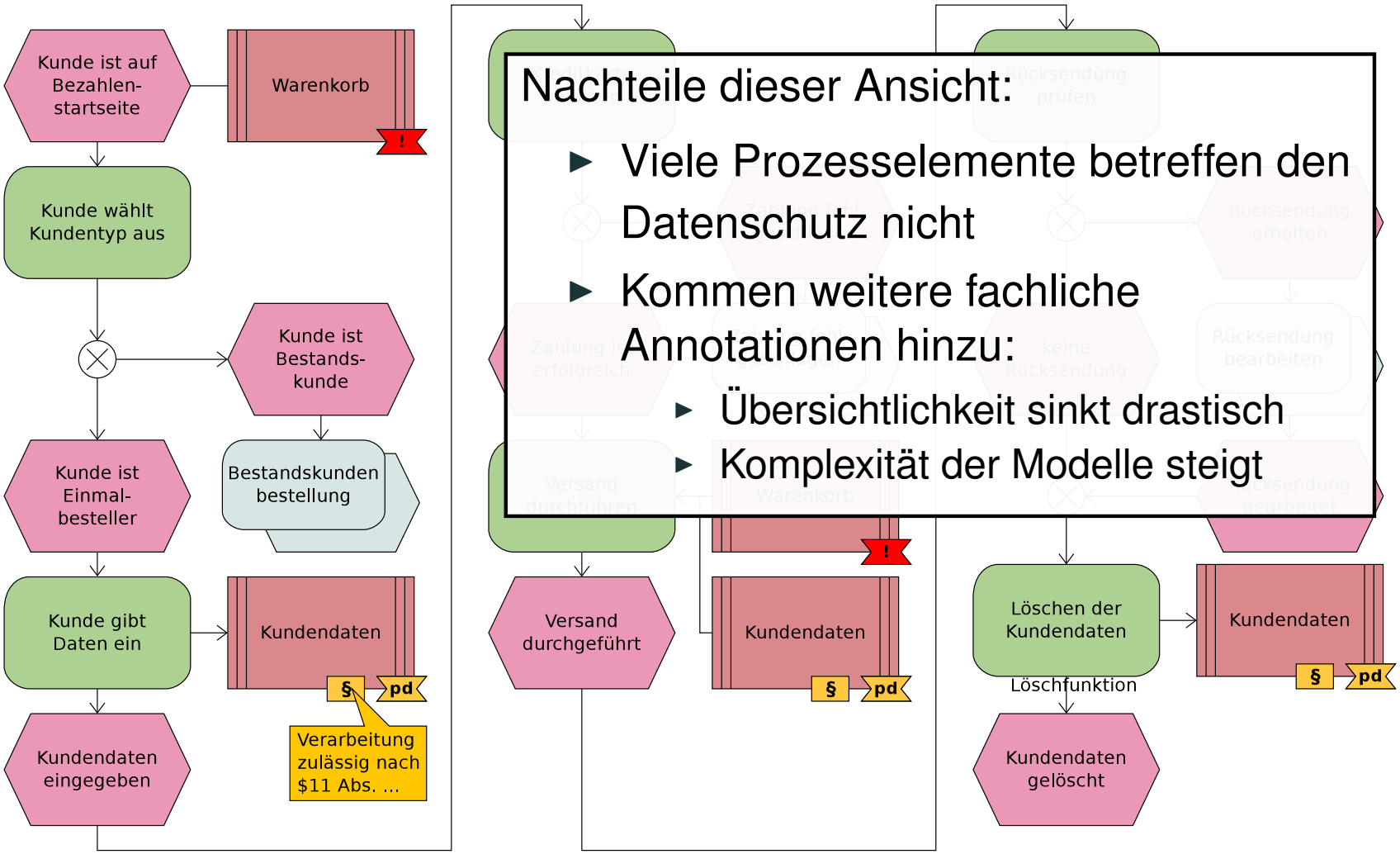
Datenschutz-Annotation im Prozess

Ansicht im Beispielprozess



Datenschutz-Annotation im Prozess

Ansicht im Beispielprozess



Nachteile dieser Ansicht:

- Viele Prozesselemente betreffen den Datenschutz nicht
- Kommen weitere fachliche Annotationen hinzu:
  - Übersichtlichkeit sinkt drastisch
  - Komplexität der Modelle steigt

Überblick

Grundlagen
- Datenschutz
- Datenschutzanforderungen
- Prozessmodelle

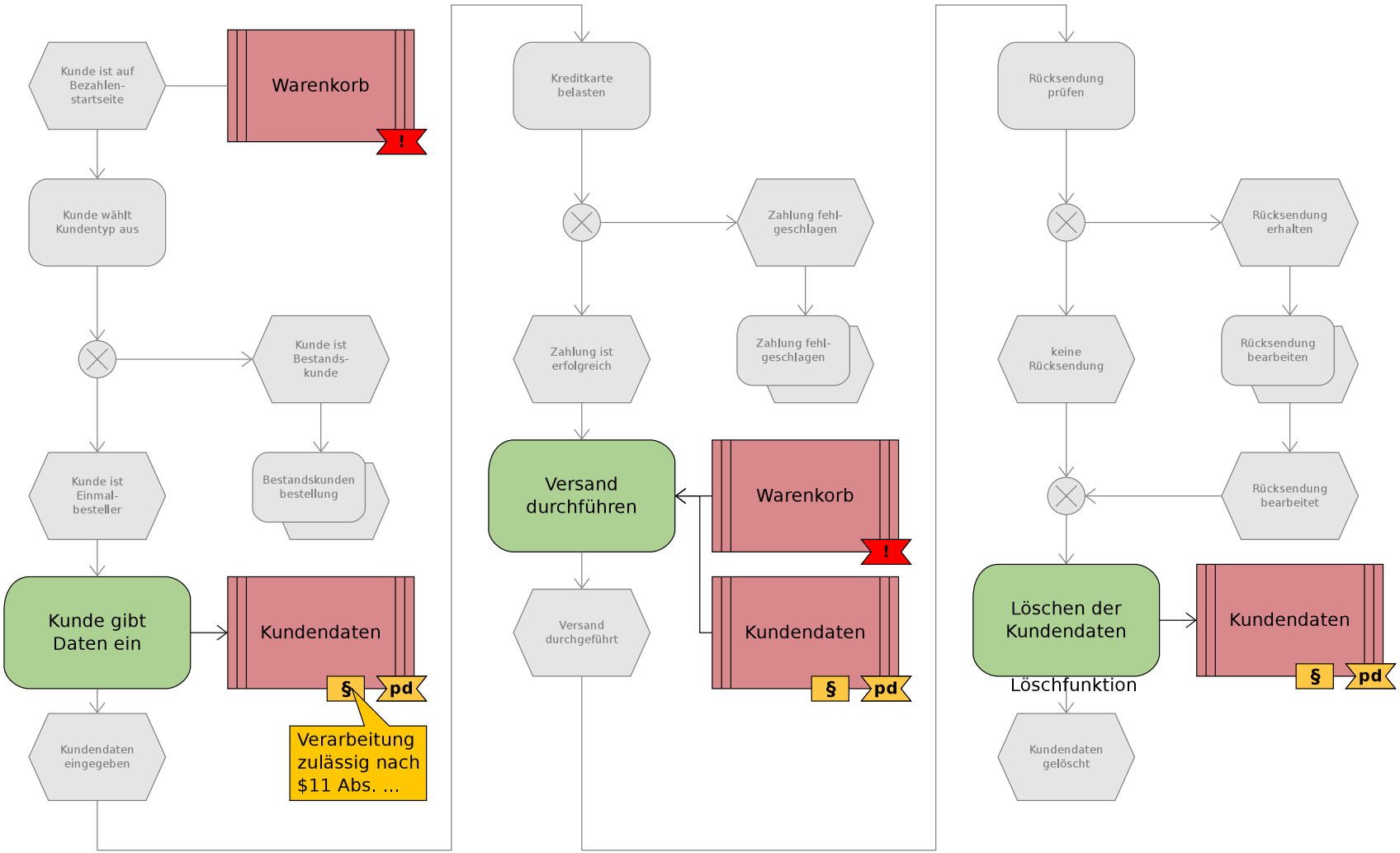
Integrierte Datenschutzmodellierung
- G-CTL – Grafische Anforderungsmodellierung
- MultiView – Komplexität in Modellen beherrschen
- Validierung

Zusammenfassung

MultiView – Komplexität in Modellen beherrschen

- Eine View bezeichnet eine fachspezifische Sicht auf einen Prozess
- Beschränkung dargestellter Elemente auf die jeweils wesentlichen
- Datenschutz ist nur eine vieler möglicher Views
- Weitere Views:
  - andere Rechtsgebiete
  - Security
  - Anforderungen spezieller Unternehmensbereiche
  - Zeitliche Betrachtungen
  - ...

Datenschutz-View für den Beispielprozess



Überblick

Grundlagen
- Datenschutz
- Datenschutzanforderungen
- Prozessmodelle

Integrierte Datenschutzmodellierung
- G-CTL – Grafische Anforderungsmodellierung
- MultiView – Komplexität in Modellen beherrschen
- Validierung

Zusammenfassung

Validierung

- Technik: Model-Checking
- Transformation des annotierten Prozesses in Kripke-Struktur
- Transformation der G-CTL-Regeln in textuelle CTL-Regeln
- Ergebnis im Fehlerfall: Gegenbeispiel

Zusammenfassung

- Datenschutz
- Vorgestellt wurde die“Integrierte Datenschutzmodellierung”
- G-CTL: Beschreibung formaler Anforderungen auf Prozessebene
- Annotation der Prozesselemente
- MultiView: Fachspezifische Sichten auf Prozesse reduzieren die Komplexität
- Datenschutz-View existiert gleichberechtigt neben anderen Views
- Validierung im Model Checker

Danke für Ihre Aufmerksamkeit!