PriS - The Privacy Safeguard

Immanuel Sims

Humboldt Universität zu Berlin
Institut für Informatik

18. November 2009

Gliederung

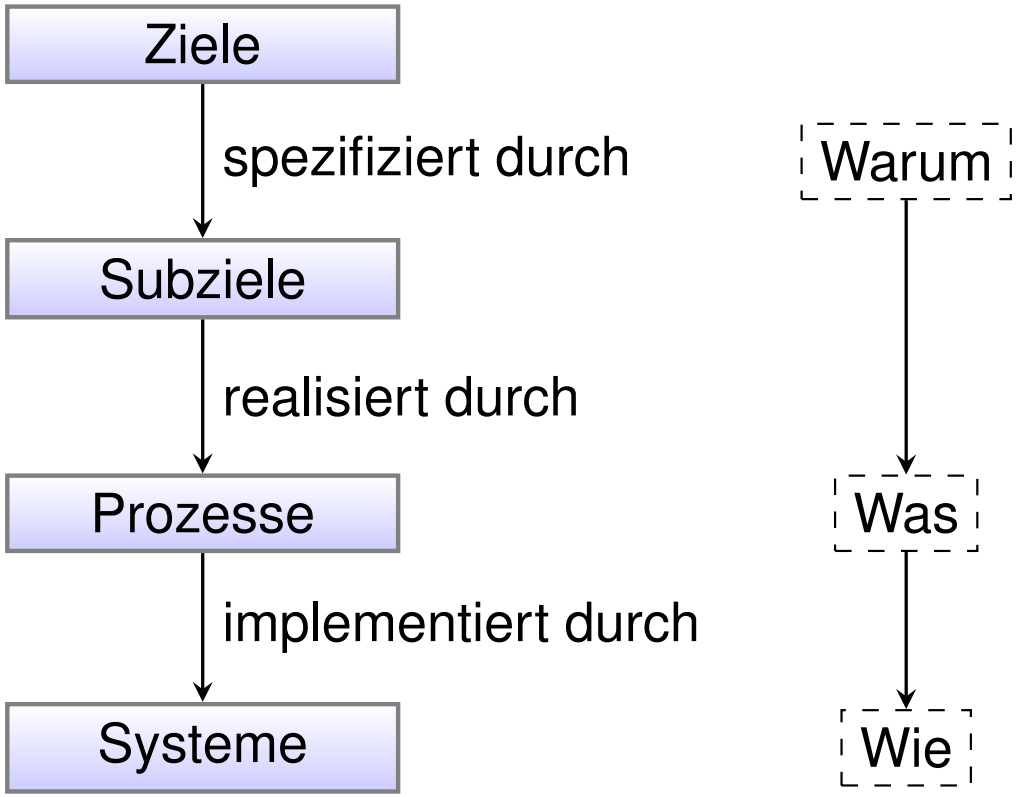
Gliederung

Was ist PriS?

Privacy **S**afeguard

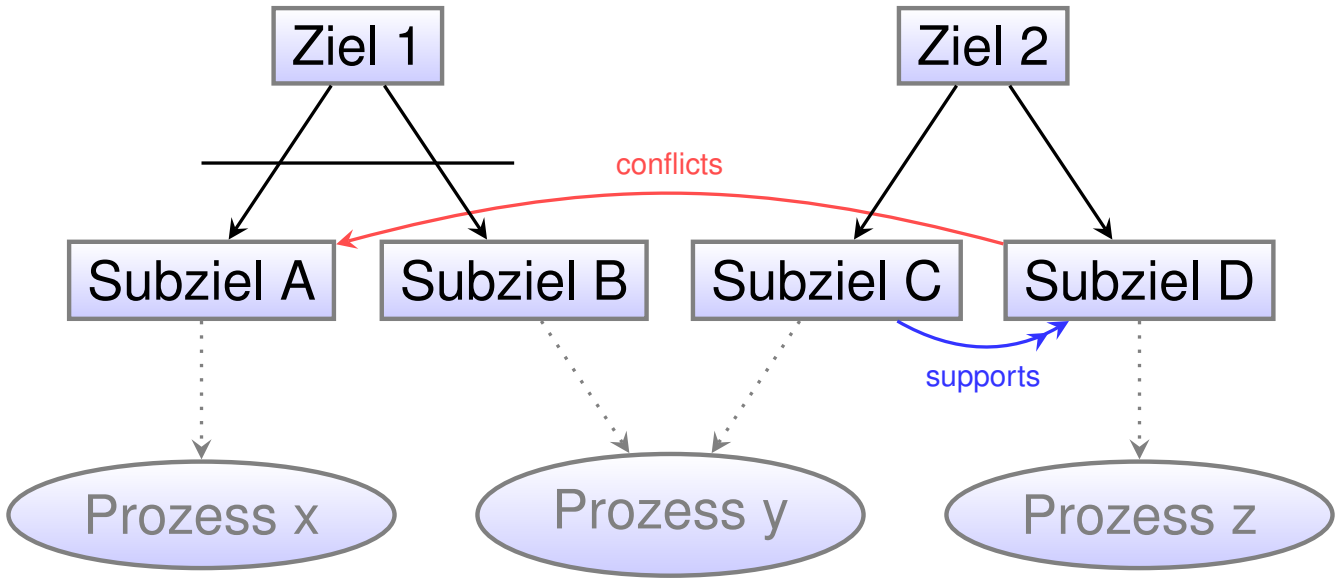
- “Planungsmethode” die Datenschutz berücksichtigt
- nicht nur für Software, auch für alles darum herum
- basiert auf einem bestehenden Framework (EKD)

Das Enterprise Knowledge Development Framework (EKD) I



Das Enterprise Knowledge Development Framework (EKD) II

(Für uns) wichtigster Diagrammtyp: Zielgraph



Datenschutzbegriff

PriS berücksichtigt folgende Prinzipien:

- Identifikation
- Authentifikation
- Authorisation
- (Daten-)Zugriffsschutz
- Anonymität
- Pseudonymität
- Nichtverbindbarkeit
- Nichtbeobachtbarkeit

Gliederung

Die Grundlegende Idee

- Datenschutzprinzipien als Ziele
- Einflussanalyse
- Designmuster zur Durchsetzung von Datenschutzprinzipien

Vier Schritte

1. Identifiziere Datenschutzrelevante Ziele
2. Analysiere den Einfluss der Datenschutzziele auf andere Ziele und Prozesse; mache dann das Modell konsistent
3. Nutze Datenschutzmuster zur Modellierung Datenschutzrelevanter Prozesse
4. Suche Implementationstechniken die die Prozesse am besten umsetzen

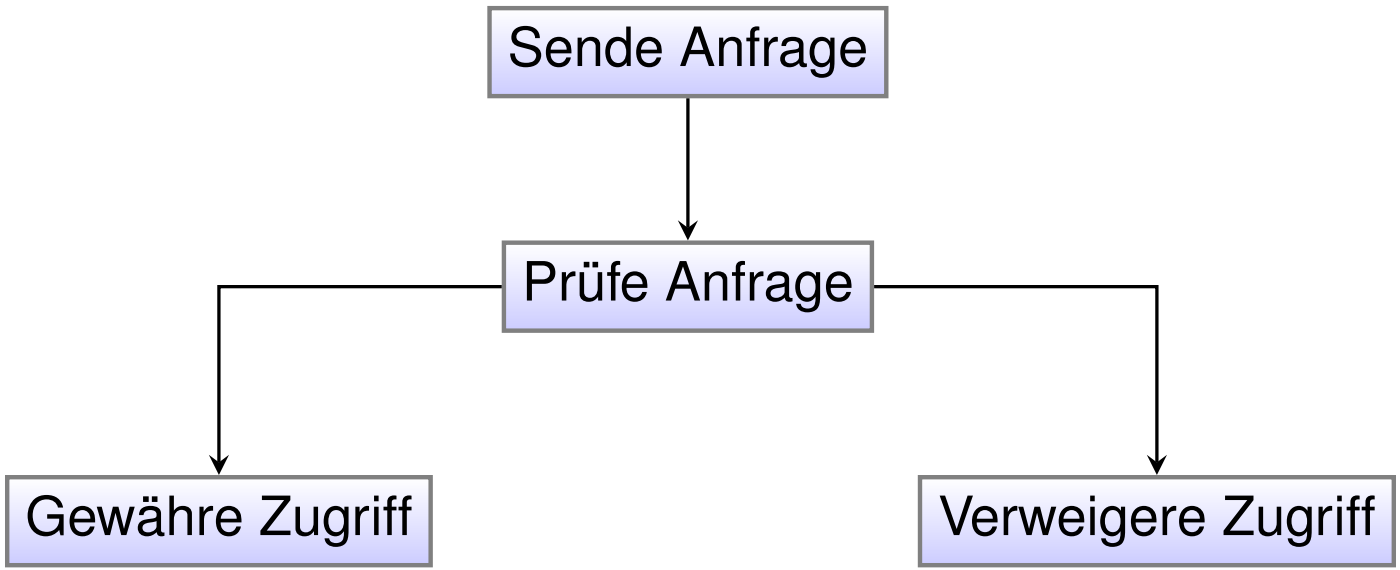
Datenschutzmuster

Allgemein

Jedes der im folgenden erklärten Muster formt den Kasten “Datenschutzrelevanter Prozess”.

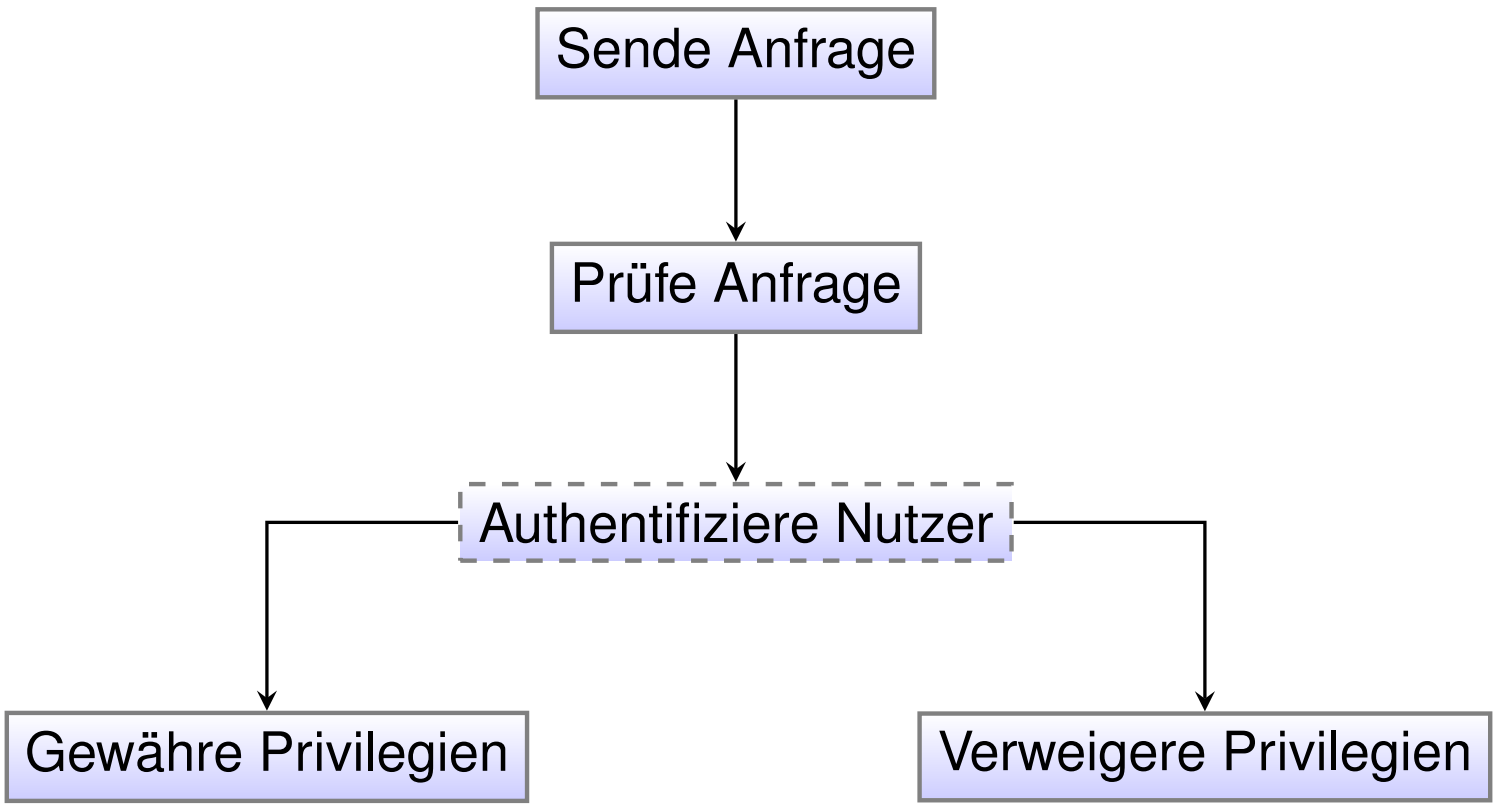
Datenschutzmuster

Authentifikation



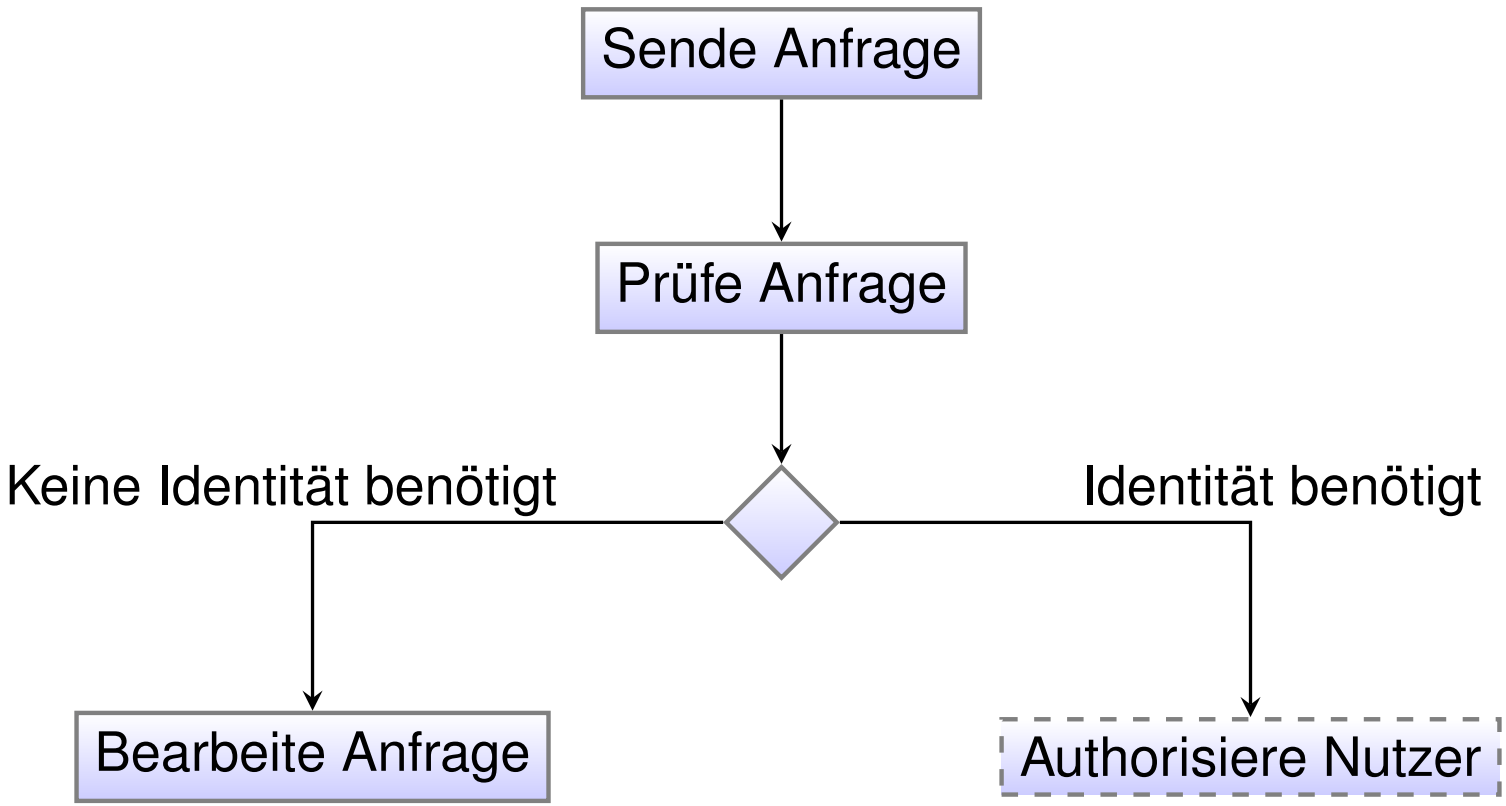
Datenschutzmuster

Authorisation



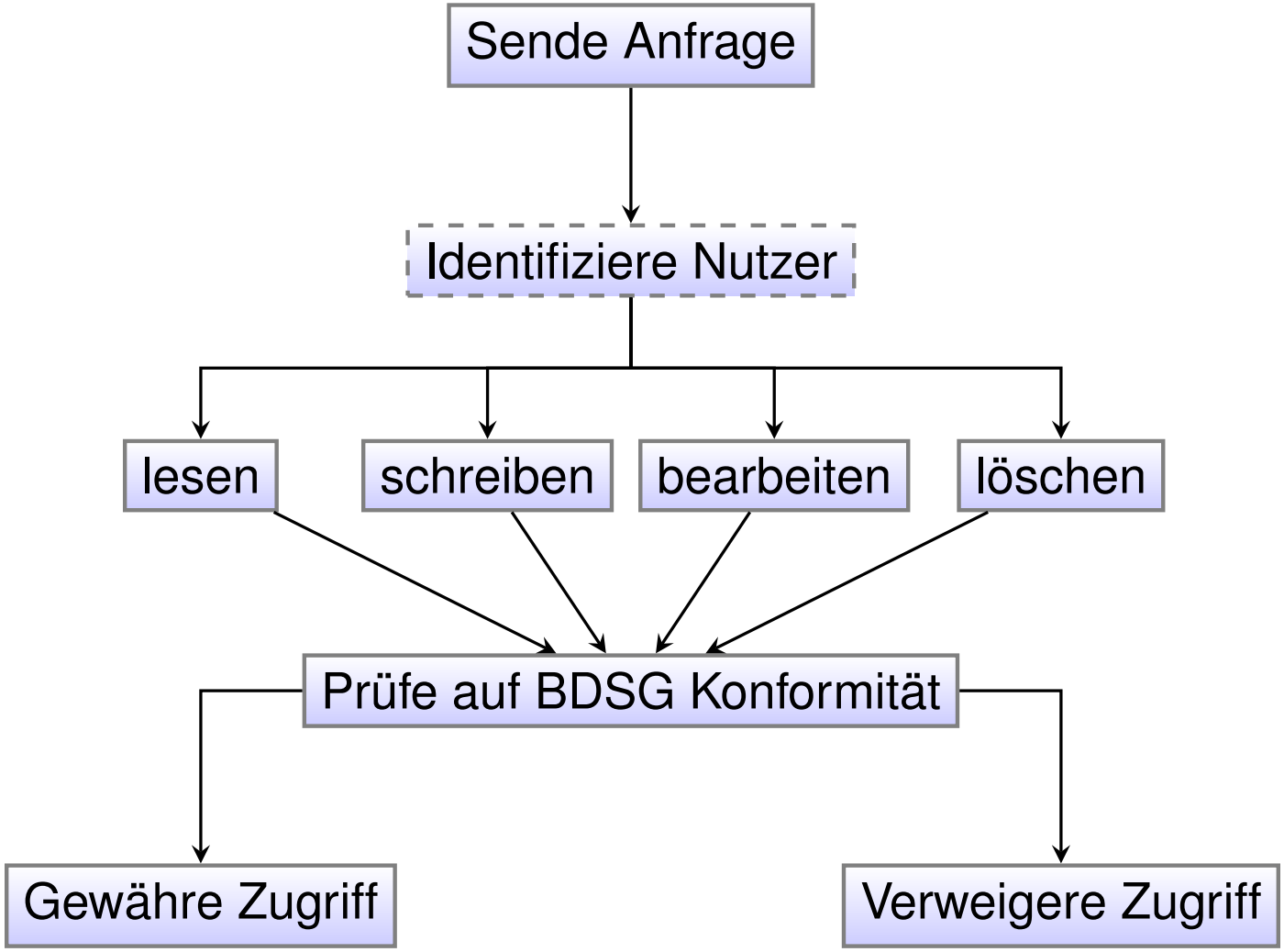
Datenschutzmuster

Identifikation



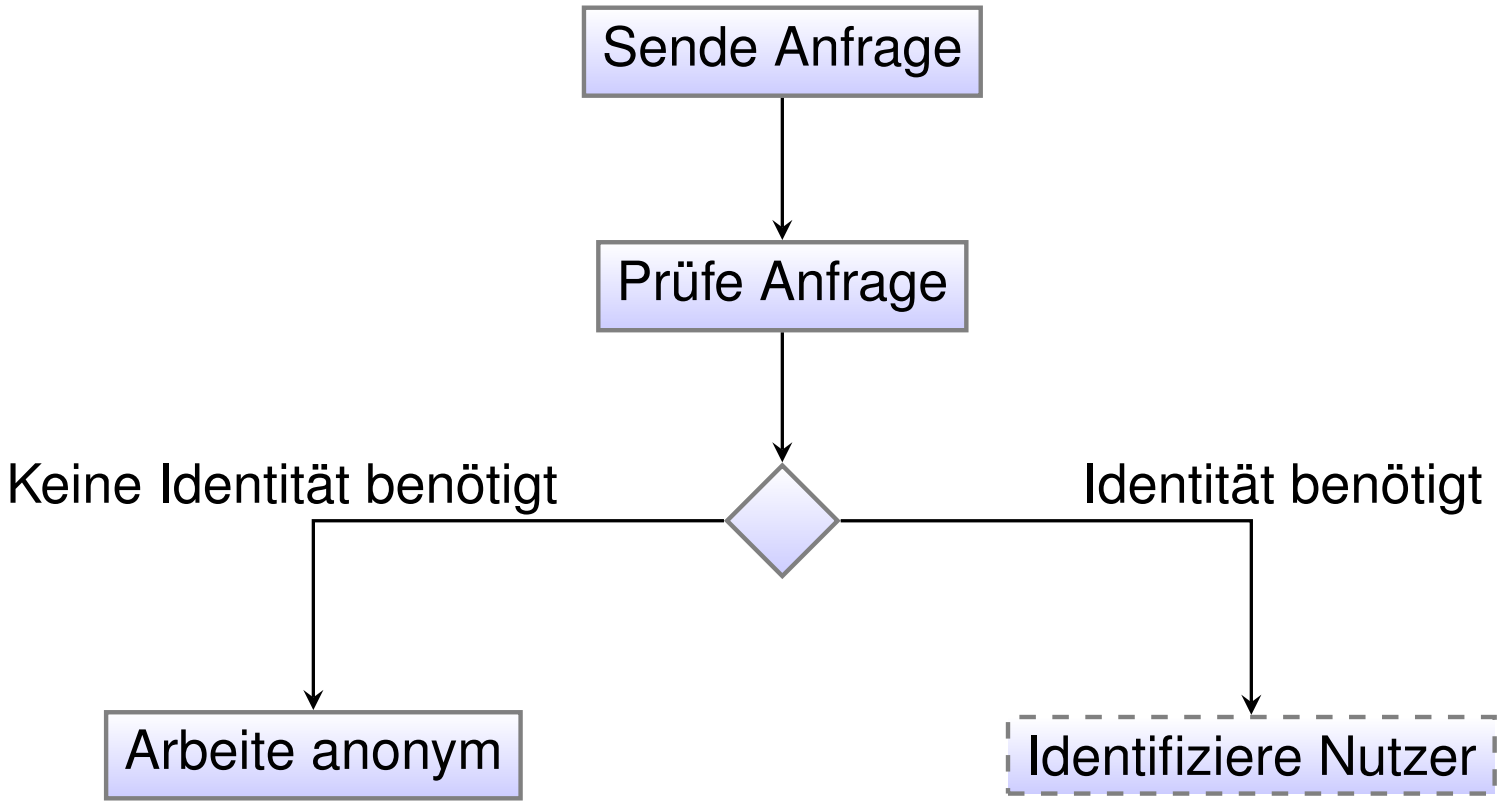
Datenschutzmuster

Zugriffsschutz



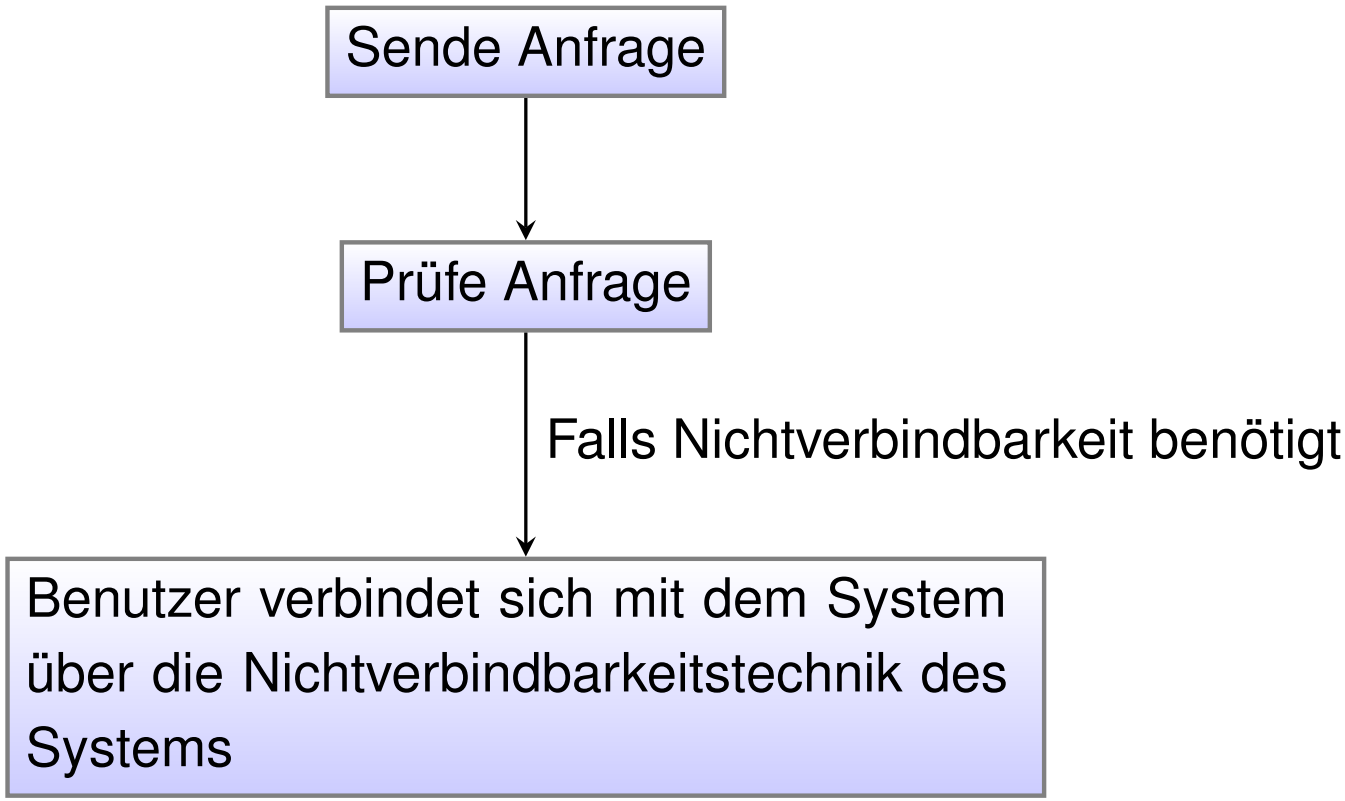
Datenschutzmuster

Anonymität & Pseudonymität



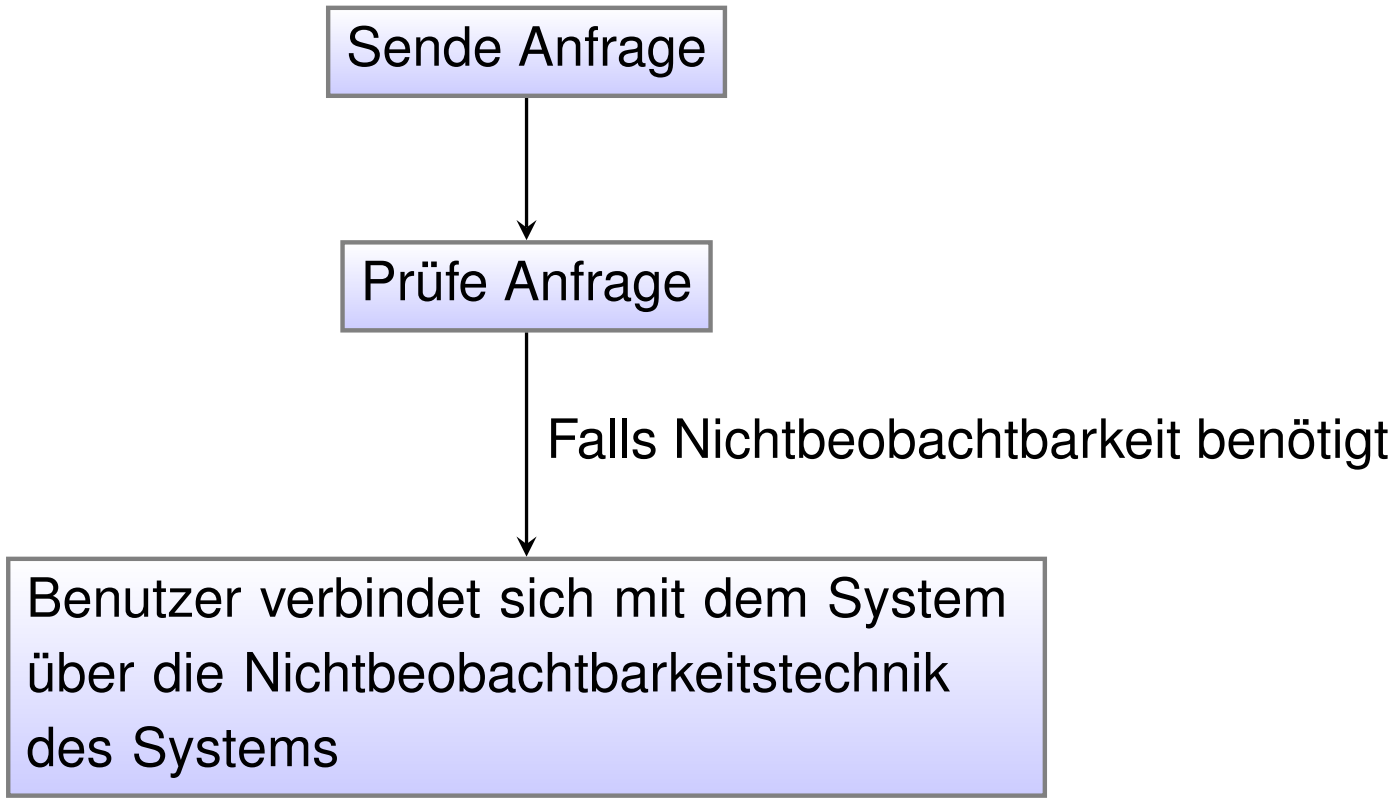
Datenschutzmuster

Nichtverbindbarkeit



Datenschutzmuster

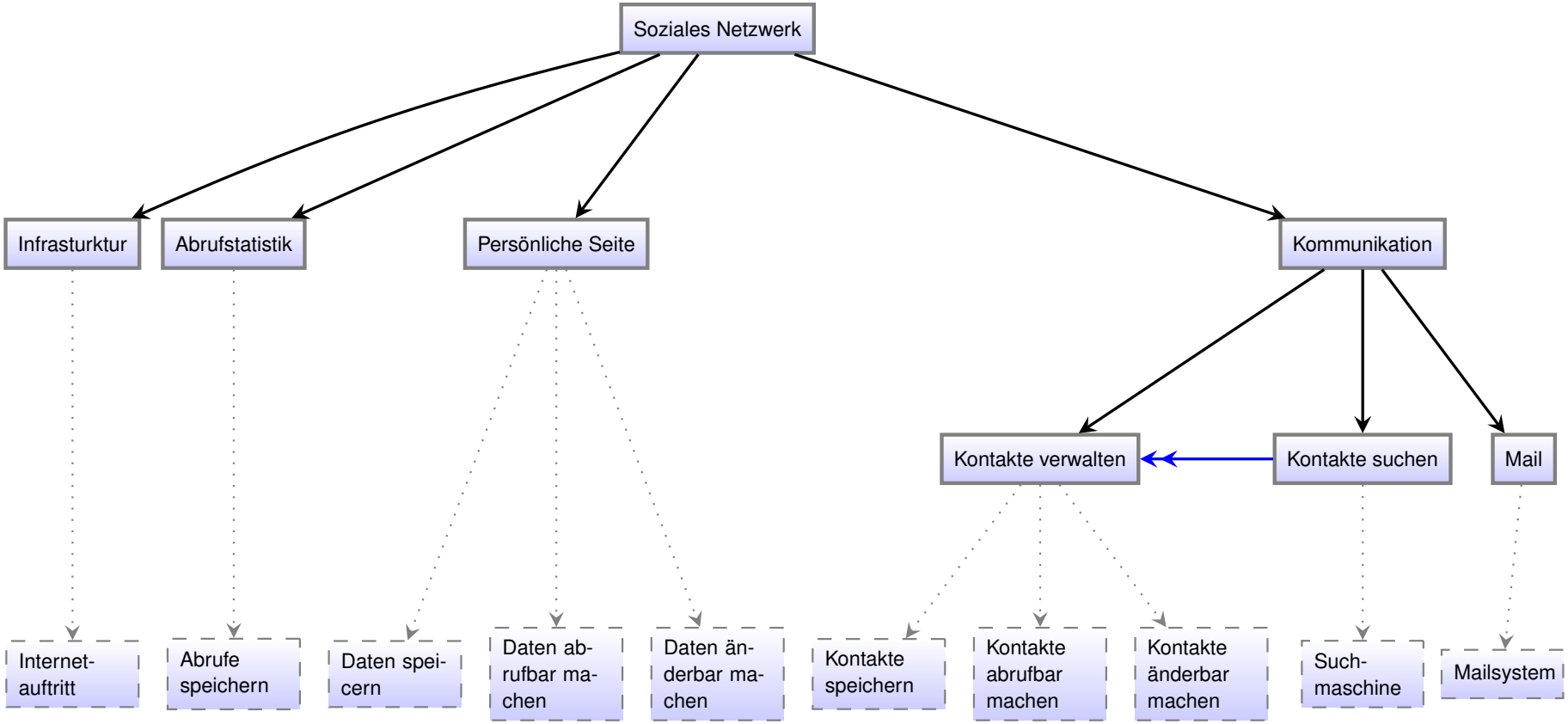
Nichtbeobachtbarkeit



Gliederung

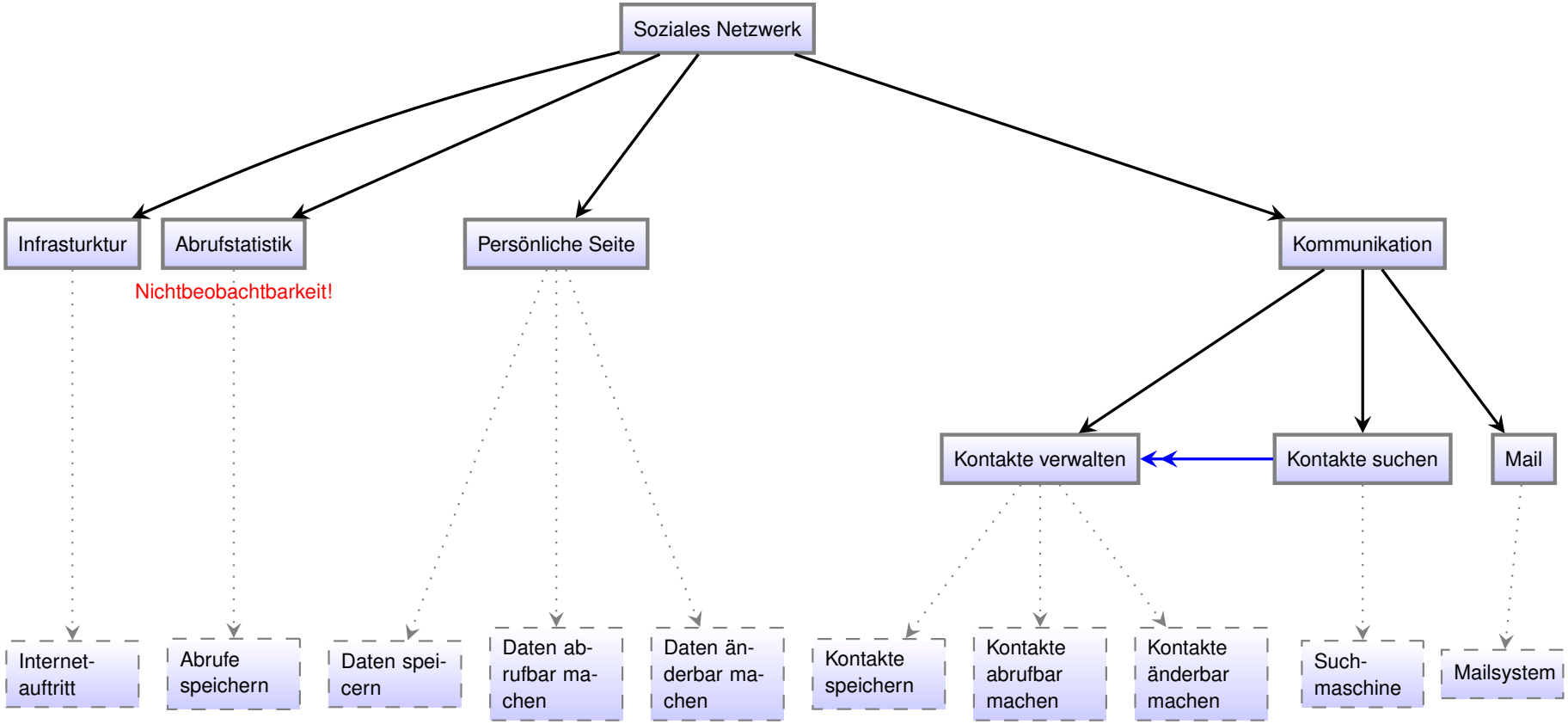
Beispiel I

Soziales Netzwerk



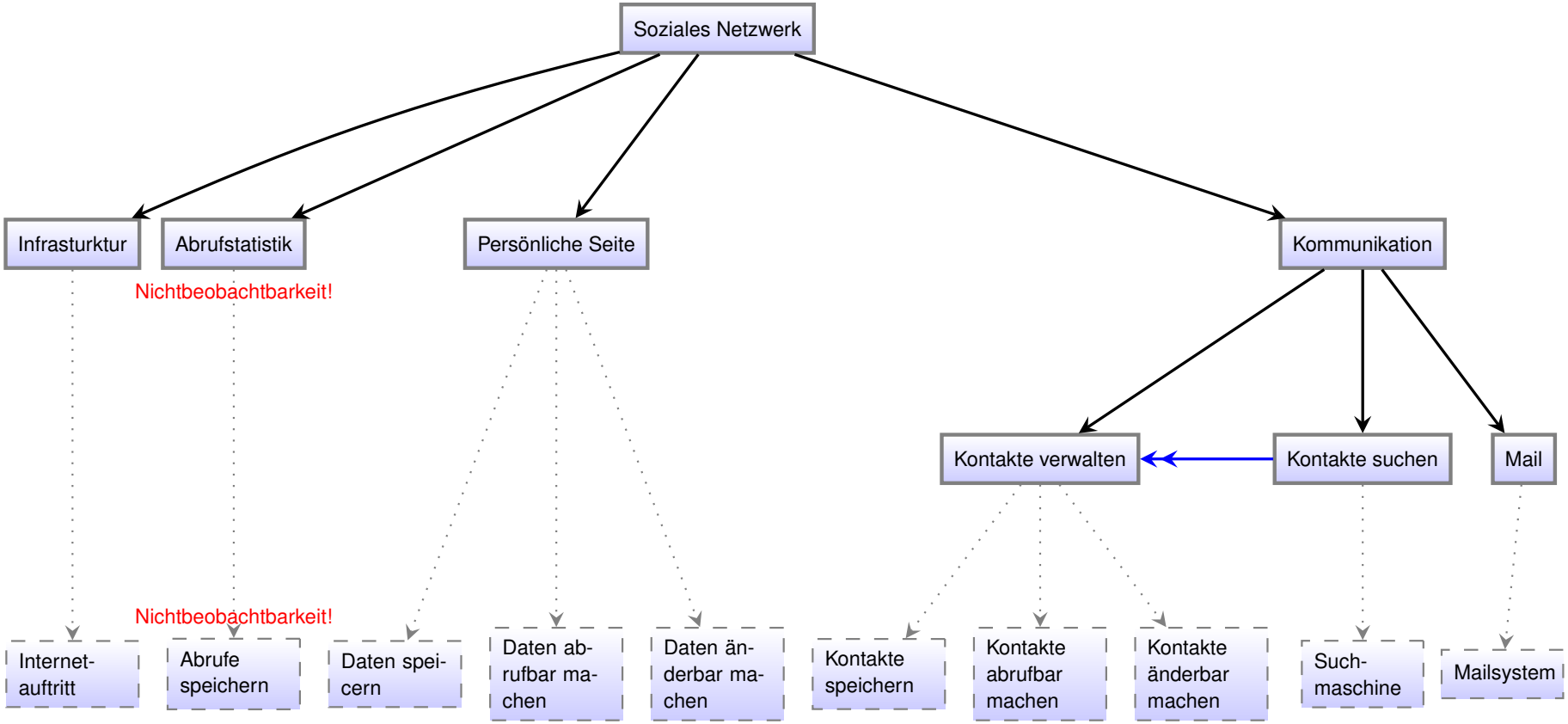
Beispiel I

Soziales Netzwerk



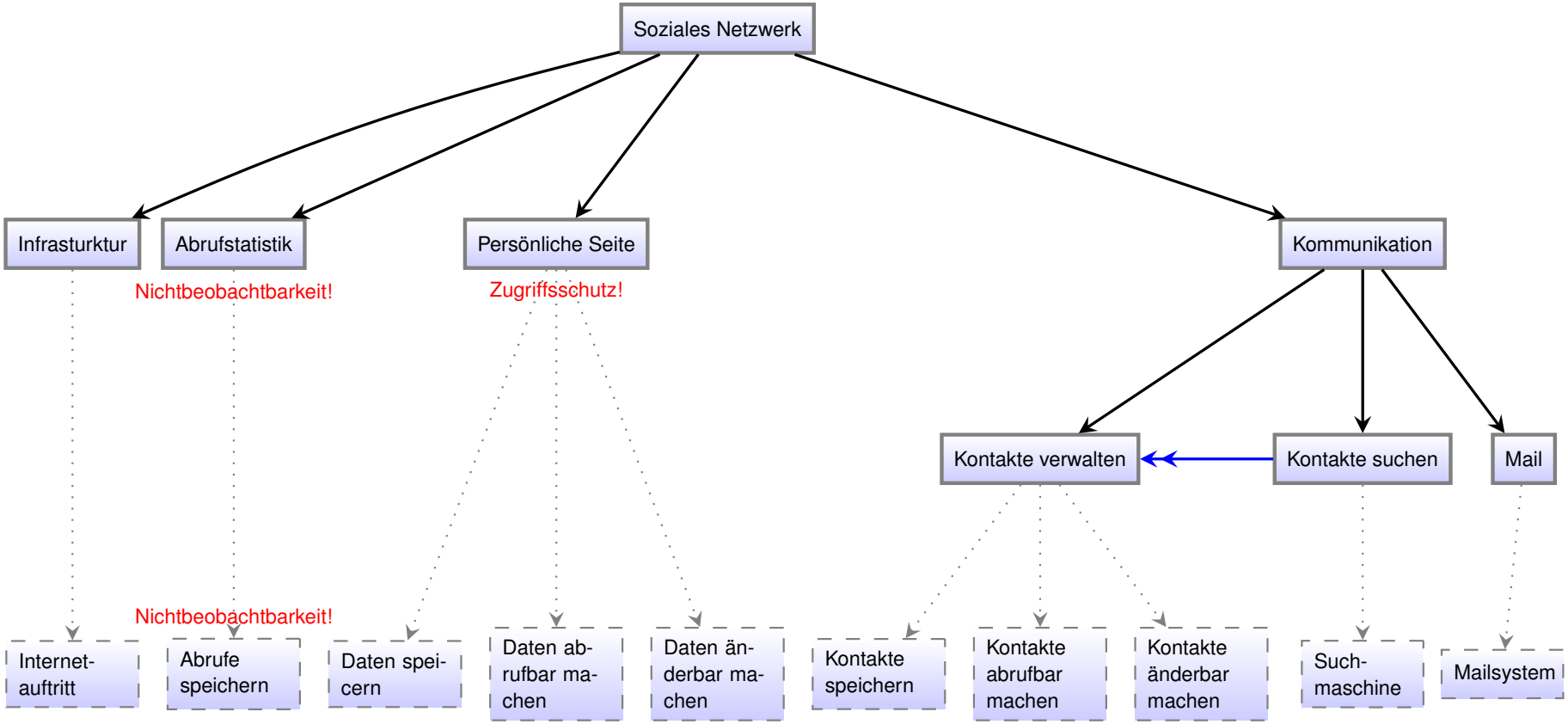
Beispiel I

Soziales Netzwerk



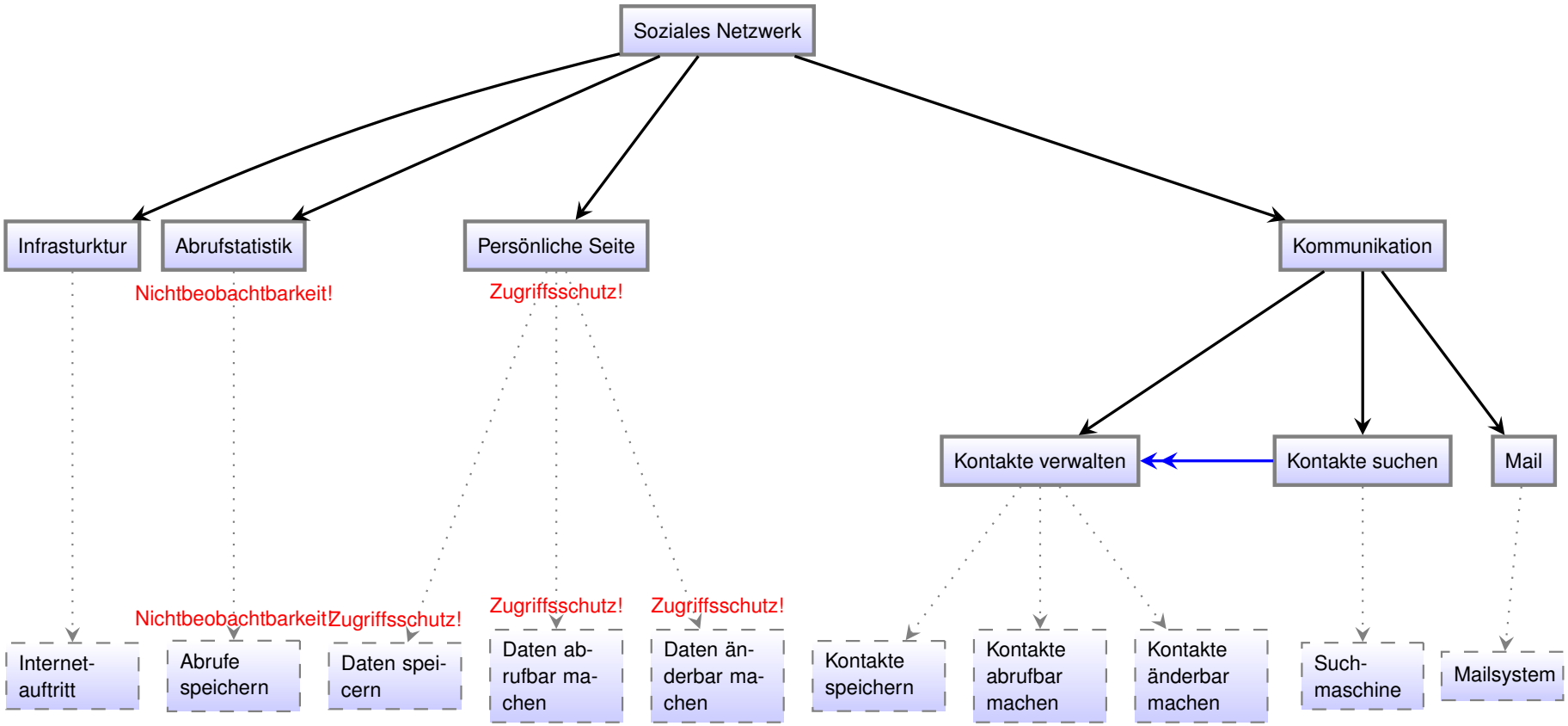
Beispiel I

Soziales Netzwerk



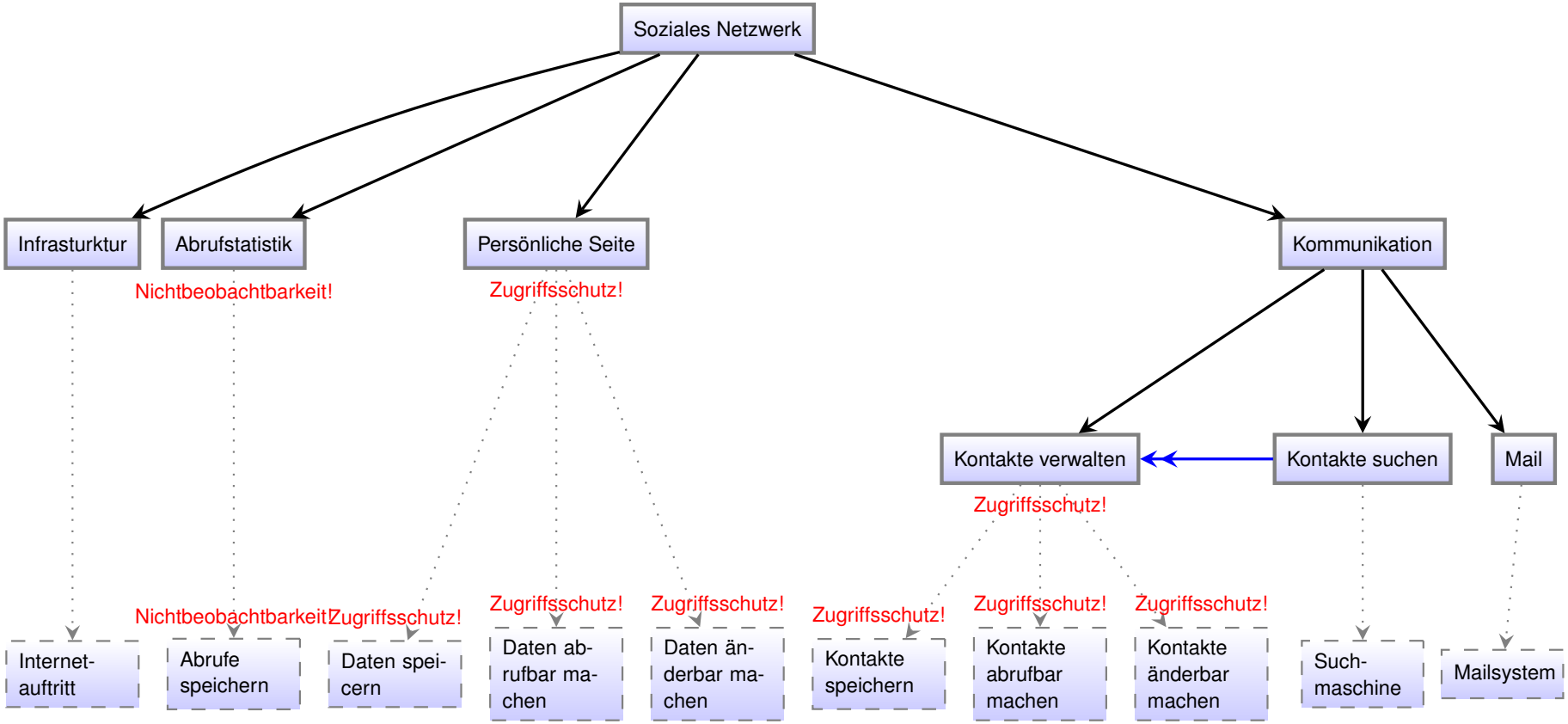
Beispiel I

Soziales Netzwerk



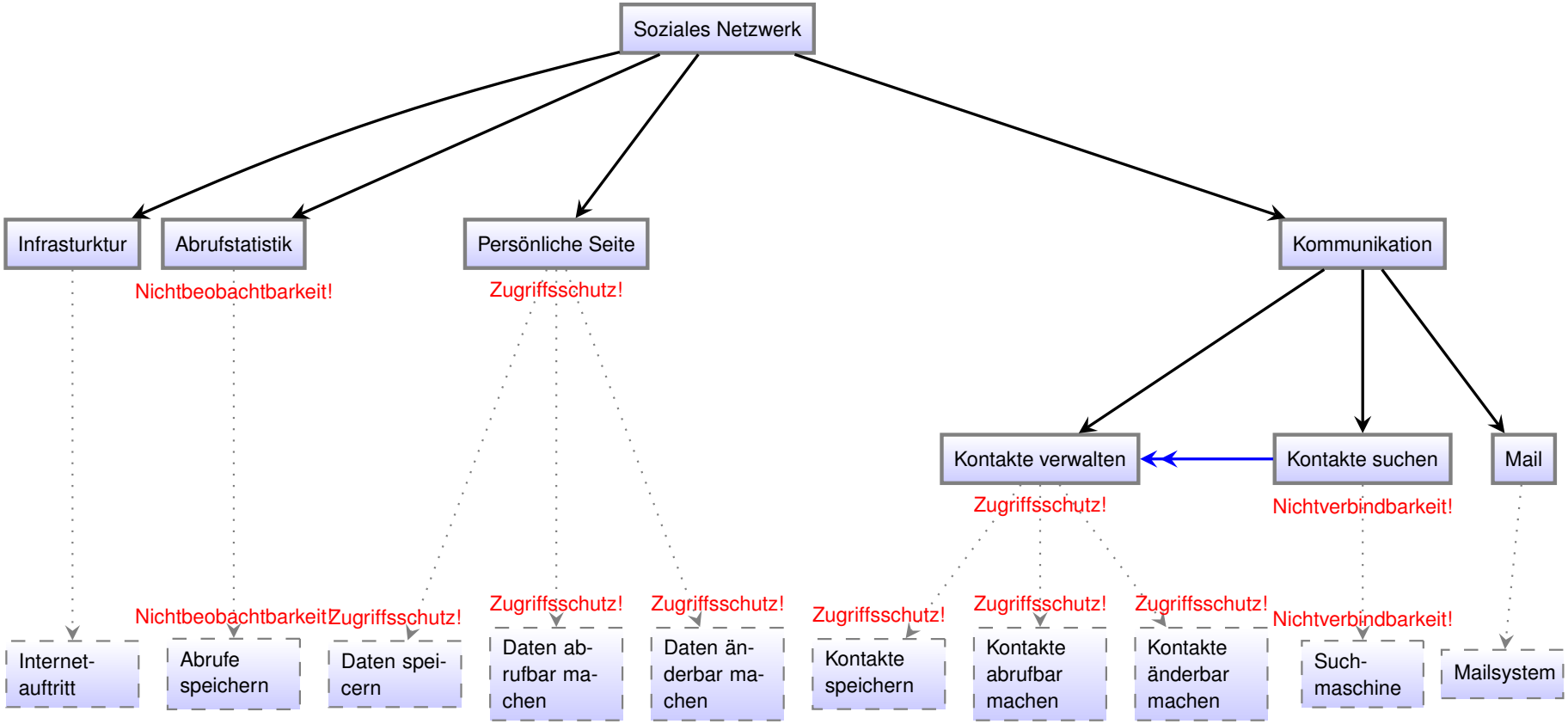
Beispiel I

Soziales Netzwerk



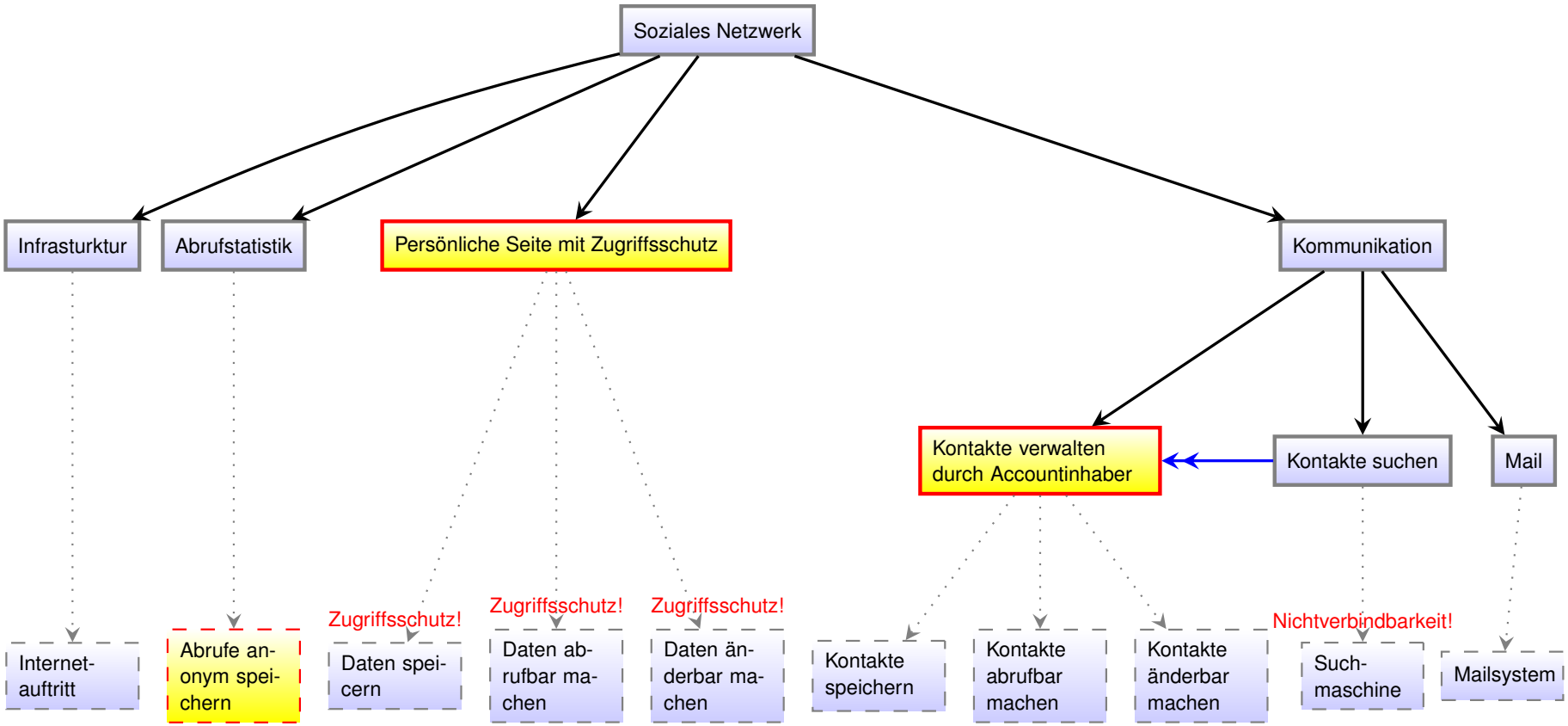
Beispiel I

Soziales Netzwerk



Beispiel II

Soziales Netzwerk



Gliederung

Gibt es Fragen?

Gibt es Fragen?

- Wie sinnvoll sind die Designmuster (insbesondere Nichtverbindbarkeit und Nichtbeobahtbarkeit)?

Gibt es Fragen?

- Wie sinnvoll sind die Designmuster (insbesondere Nichtverbindbarkeit und Nichtbeobahtbarkeit)?
- Ist das Authorisationsmuster in Ordnung?

Gibt es Fragen?

- Wie sinnvoll sind die Designmuster (insbesondere Nichtverbindbarkeit und Nichtbeobahtbarkeit)?
- Ist das Authorisationsmuster in Ordnung?
- Sind Authentifikation, Identifikation und Authorisation wirklich relevant?

Literatur

C. KALLONIATIS, E. KAVAKLI, S. GRITZALIS:
Using Privacy Process Patterns for Incorporating Privacy Requirements into the System Design Process.
In: *Second International Conference on Availability, Reliability and Security (ARES'07)*, 2007

C. KALLONIATIS, E. KAVAKLI, S. GRITZALIS:
Addressing privacy requirements in system design: the PriS method.
In: *Requirements Engineering* (2008)

E. KAVAKLI ET AL.:
Incorporating privacy requirements into the system design process.
In: *Internet Research* (2006)