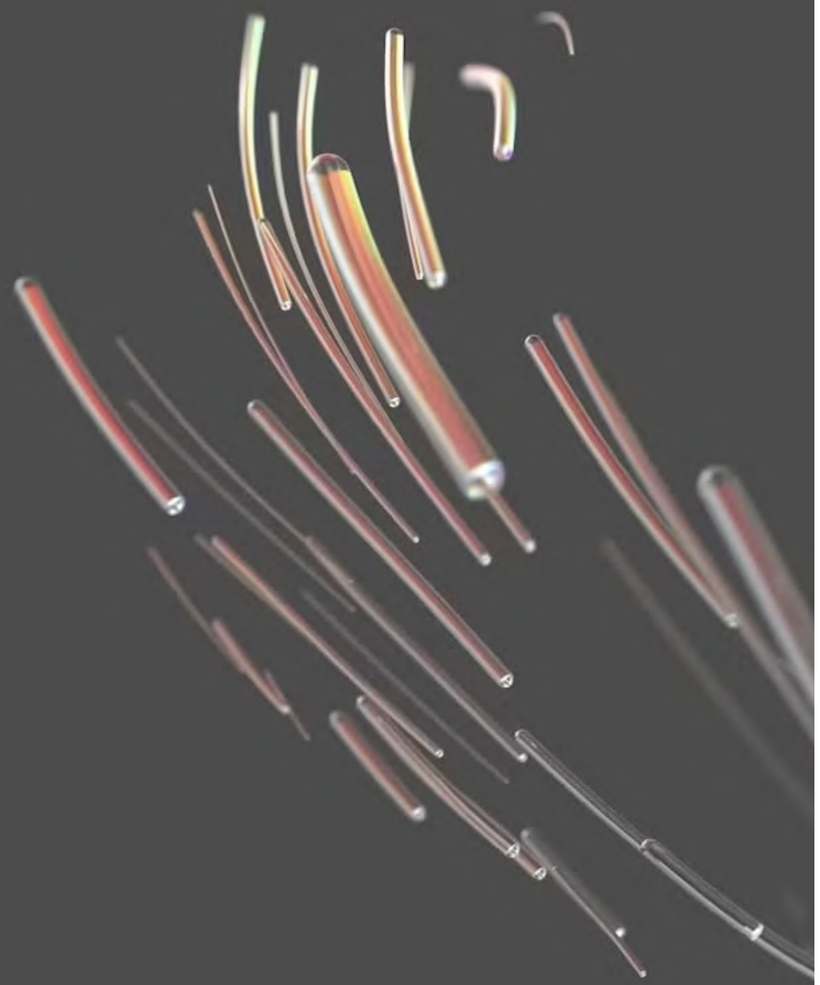


TECHNOLOGY DAY 2025

Innovativ, aber sicher!

Datensicherheit in der Produktentwicklung

INNOQ

ANJA KAMMER
SENIOR CONSULTANT

INNOQ

Anja Kammer
Senior Consultant

Agenda

Datensicherheit in der Praxis

Niemand hat Bock darauf

Beispiel: Fitness-Tracker

Realistische Herausforderungen

Soziotechnische Maßnahmen

Für soziotechnische Probleme

Datensicherheit in der Praxis

Niemand hat Bock darauf

ZEIT ONLINE

IT-Sicherheit in Gesundheitsämtern

Alle kennen die Sicherheitslücken und keiner schließt sie

In Rheinland-Pfalz setzen Gesundheitsämter eine veraltete Software voller Sicherheitsprobleme ein. Doch die Lücken werden lieber wegdiskutiert, statt geschlossen.

Von **Kai Biermann** und **Eva Wolfangel**

10. November 2023, 16:03 Uhr / 80 Kommentare /

Kai Biermann, Eva Wolfangel. (2023). IT-Sicherheit in Gesundheitsämtern: Alle kennen die Sicherheitslücken und keiner schließt sie. Retrieved from https://www.zeit.de/digital/datenschutz/2023-11/it-sicherheit-gesundheitsaemter-rheinland-pfalz-software-datenschutz

"Sicherheitsanforderungen sind komplett ***realitätsfern***."

"Feedback zur Umsetzung fehlt. Entwicklungsteams werden ***allein gelassen***."

"Sicherheitsthemen gehören ***nicht in meinen Aufgabenbereich***"

"...***möglichst restriktiv***, um auf der sicheren Seite zu sein."

"Fehlannahme: Betrieb On-Premises ist ***automatisch sicher*** ."

"Ignoranz mit voller Absicht, wenn man ***nicht zu den großen Fischen gehört***."

DSGVO-VERSTOSS

Uber soll 290 Millionen Euro Geldstrafe zahlen

Dem beliebten Fahrdienst wird vorgeworfen, mehr als zwei Jahre lang sensible Fahrerdaten bei unzureichendem Schutz in die USA übermittelt zu haben.

26. August 2024, 13:32 Uhr, Marc Stöckel

Die niederländische Datenschutzbehörde (DPA) hat eine Geldstrafe in Höhe von 290 Millionen Euro gegen Uber verhängt. Als Grund für die Strafe nennt die Behörde in einer Mitteilung den Umstand, dass der weltweit bekannte Fahrdienst unrechtmäßig und unter unzureichenden Schutzvorkehrungen personenbezogene Daten von europäischen Fahrern in die Vereinigten Staaten übermittelt und damit gegen die DSGVO verstoßen hat.

So habe Uber etwa Kontodaten, Taxilizenzen, Standortdaten, Fotos, Zahlungsinformationen, Ausweisdokumente und in einigen Fällen sogar strafrechtliche und medizinische Daten der Fahrer an Server in den USA übertragen und dort gespeichert, heißt es. Die

Marc Stöckel. golem.de (2024). Uber soll 290 Millionen Euro Geldstrafe zahlen.
https://www.golem.de/news/datenuebertragung-in-die-usa-uber-soll-290-millionen-euro-strafe-zahlen-2408-188404.html

Apple Newsroom (2023). Apple unterstreicht sein Engagement für Privatsphäre […]
https://www.apple.com/de/newsroom/2023/01/apple-builds-on-privacy-commitment-by-unveiling-new-efforts-on-data-privacy-day/

Beispiel

Fitness-Tracker

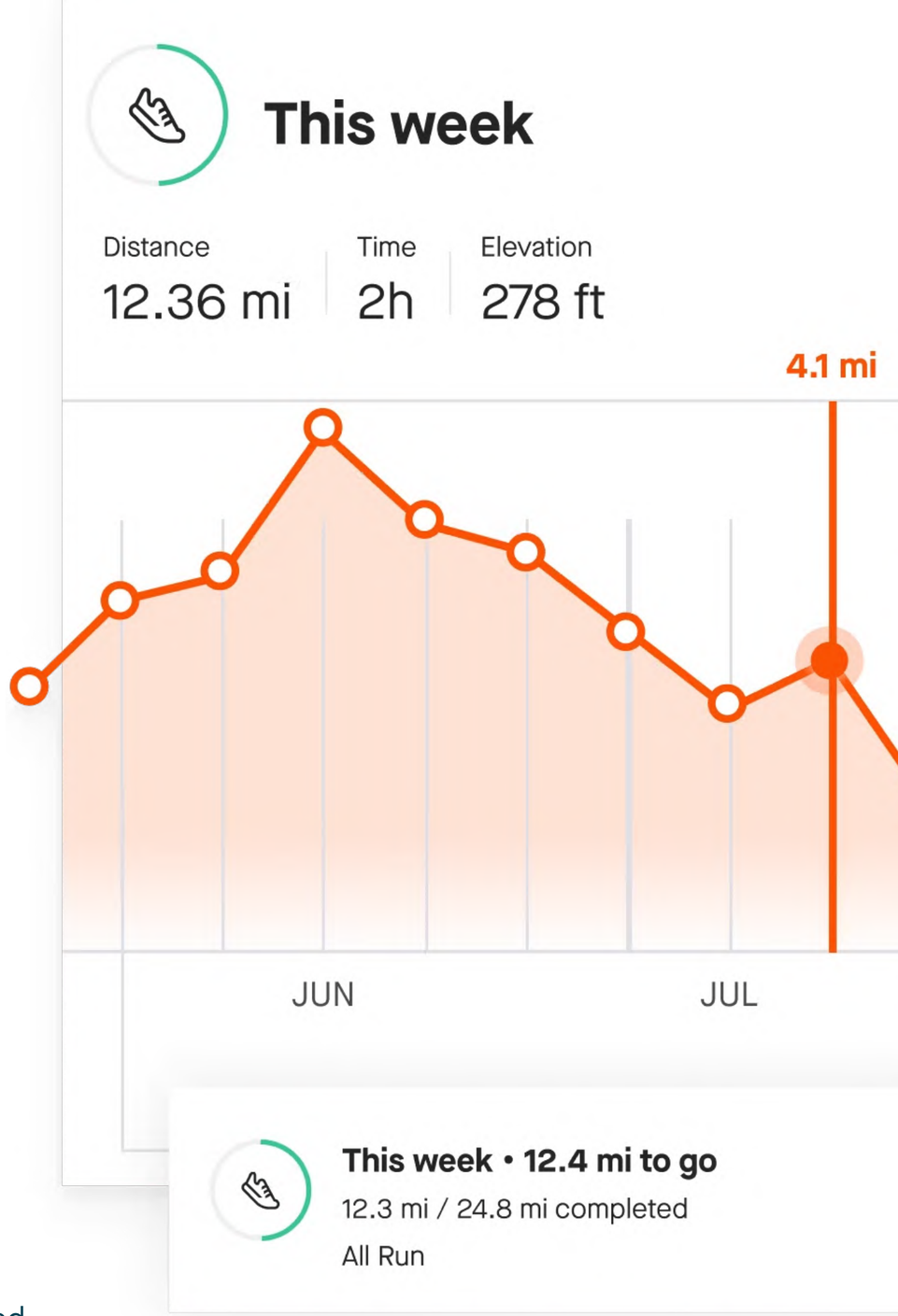
Fitness-Tracker

Gesundheitsdaten

- Schritte
- Herzfrequenz
- verbrannte Kalorien

Trainingsrouten

- Streckenverlauf
- Geschwindigkeit
- Tageszeiten



Strava (12.2024). https://www.strava.com/get-started

Fitness-Tracker

Gesundheitsdaten

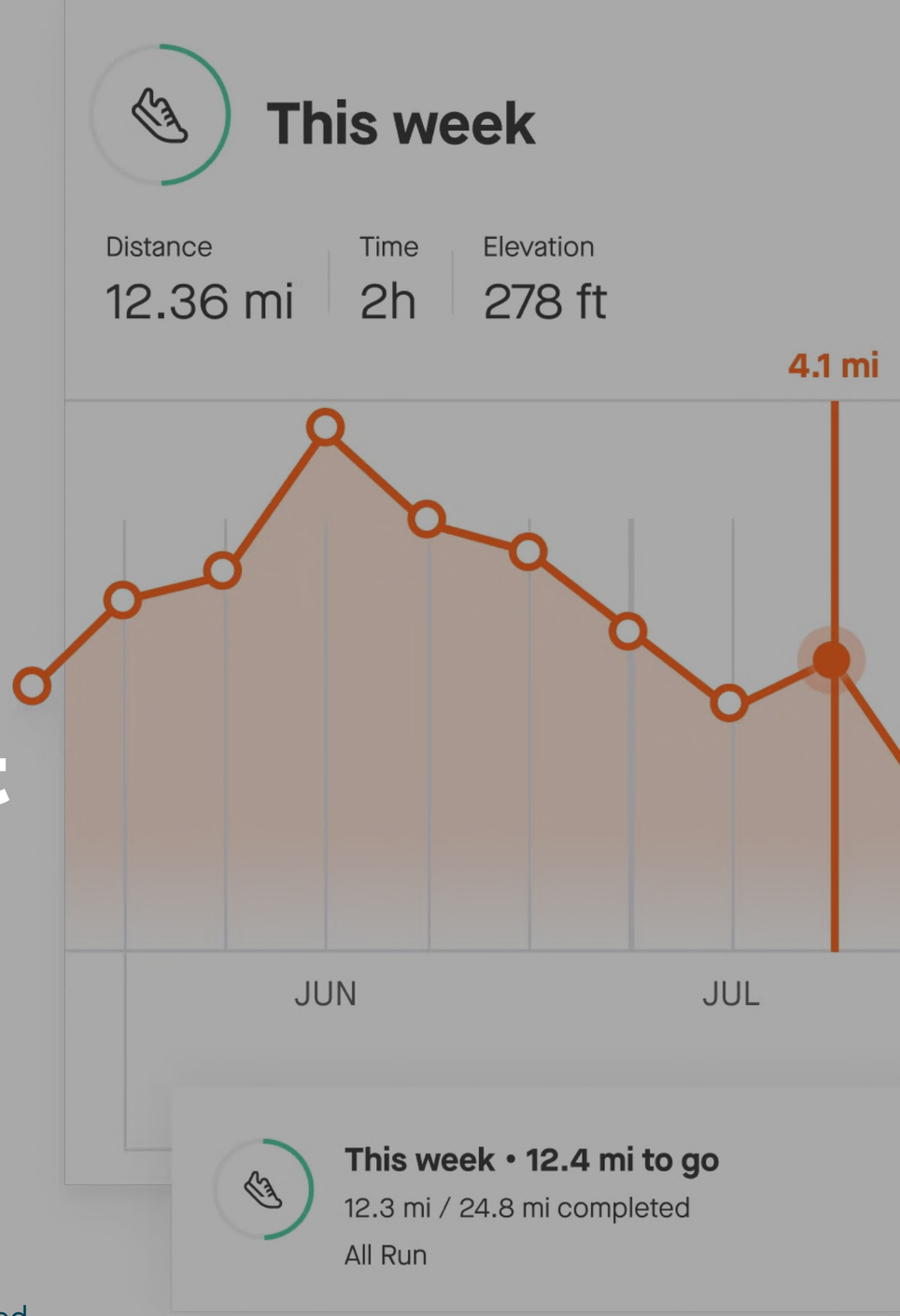
- Schritte
- Herzfrequenz
- verbrannte Kalorien

Trainingsrouten

- Streckenverlauf
- Geschwindigkeit
- Tageszeiten

Datensparsamkeit

Lokale Datenspeicherung



Strava (12.2024). https://www.strava.com/get-started

Personalisierte Trainingspläne

Personalisierte Trainingspläne

- Tageszeit und Tagesformabhängig

Standort-basierte Trainingsempfehlungen

- „Diese Strecke ist für deine Laufziele optimal“

Personalisierte Trainingspläne

Personalisierte Trainingspläne

- Tageszeit und Tagesformabhängig

Standort-basierte Trainingsempfehlungen

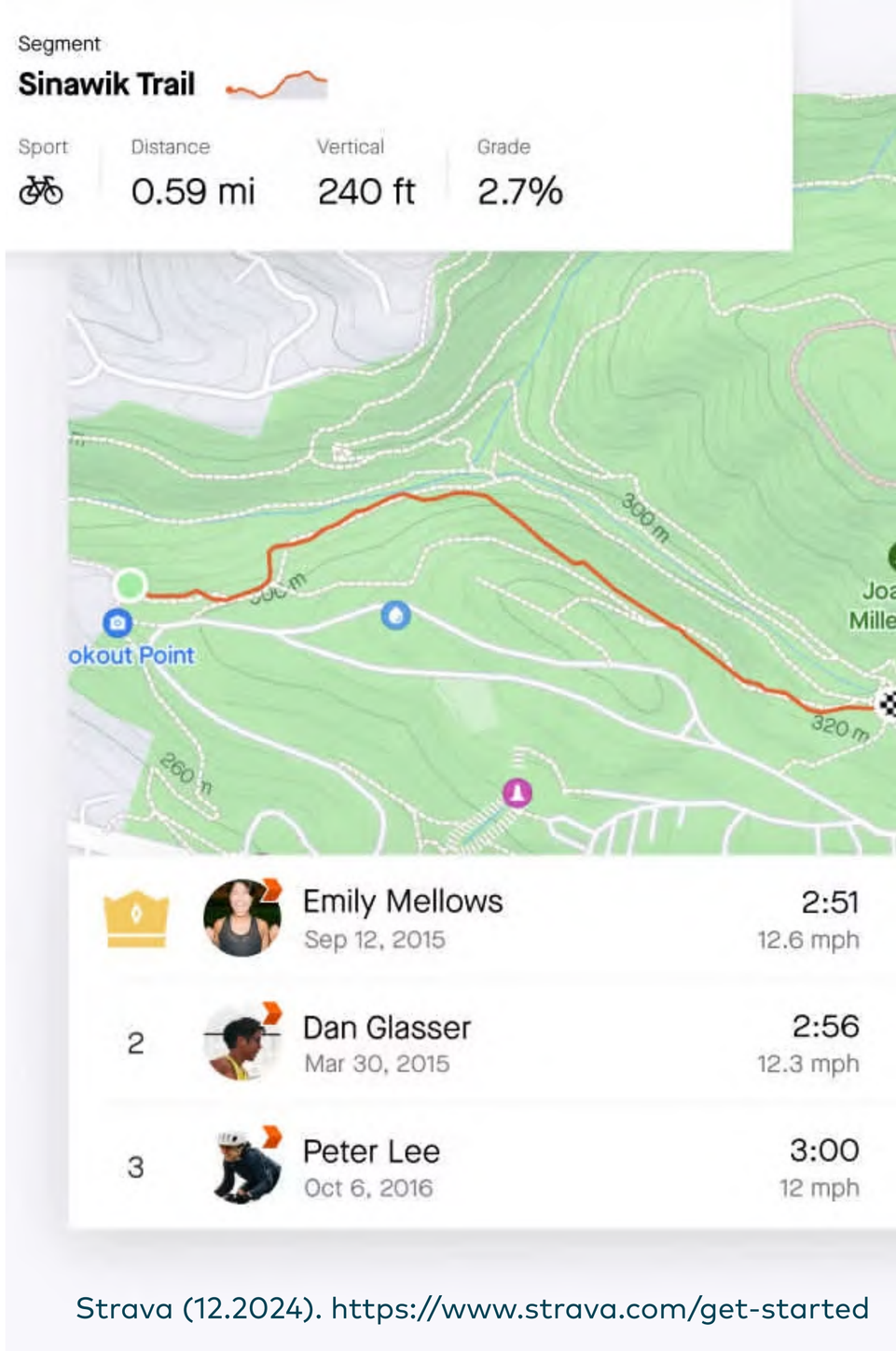
- „Diese Strecke ist für deine Laufziele optimal“

Gefahr: Profiling

Soziales Netzwerk

Alleinstellungsmerkmal

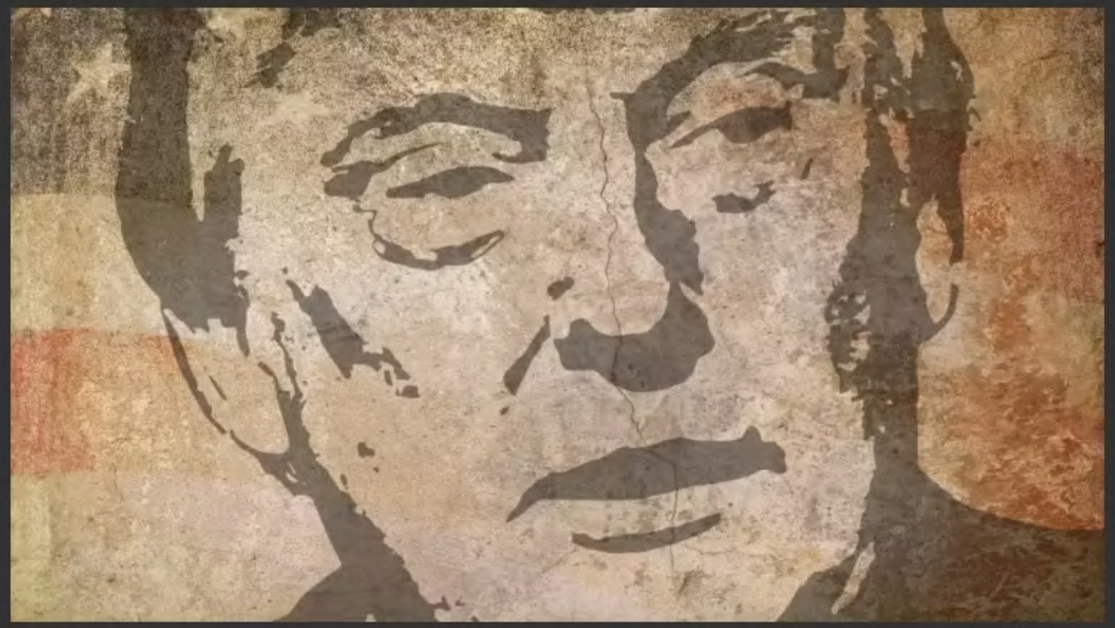
- Leistungsvergleich unter Freunden
- virtuelle Wettkämpfe
- Regionale Bestenlisten



Strava (12.2024). https://www.strava.com/get-started

Ortsinformationen geleakt: Zeitung zeichnet Trumps Bewegungsabläufe nach

Die New York Times kam an Daten von Millionen Smartphone-Nutzern. Darunter ein Secret-Service-Agent. So wurden auch die Wege von Präsident Trump öffentlich.



(Bild: pixabay.com)

Sophia Zimmermann (2019). Ortsinformationen geleakt: Zeitung zeichnet Trumps Bewegungsabläufe nach https://www.heise.de/news/Ortsinformationen-geleakt-Zeitung-zeichnet-Trumps-Bewegungsablaeufe-nach-4621820.html

Strava

Fitness-App verrät sensible militärische Geodaten

29. Januar 2018, 14:47 Uhr | Lesezeit: 4 Min.

So sieht die Strava-Heatmap von München aus. Deutlich lassen sich die Lauf- und Radstrecken erkennen, die beidseitig entlang der Isar verlaufen.
(Foto: Screenshot Strava.com)

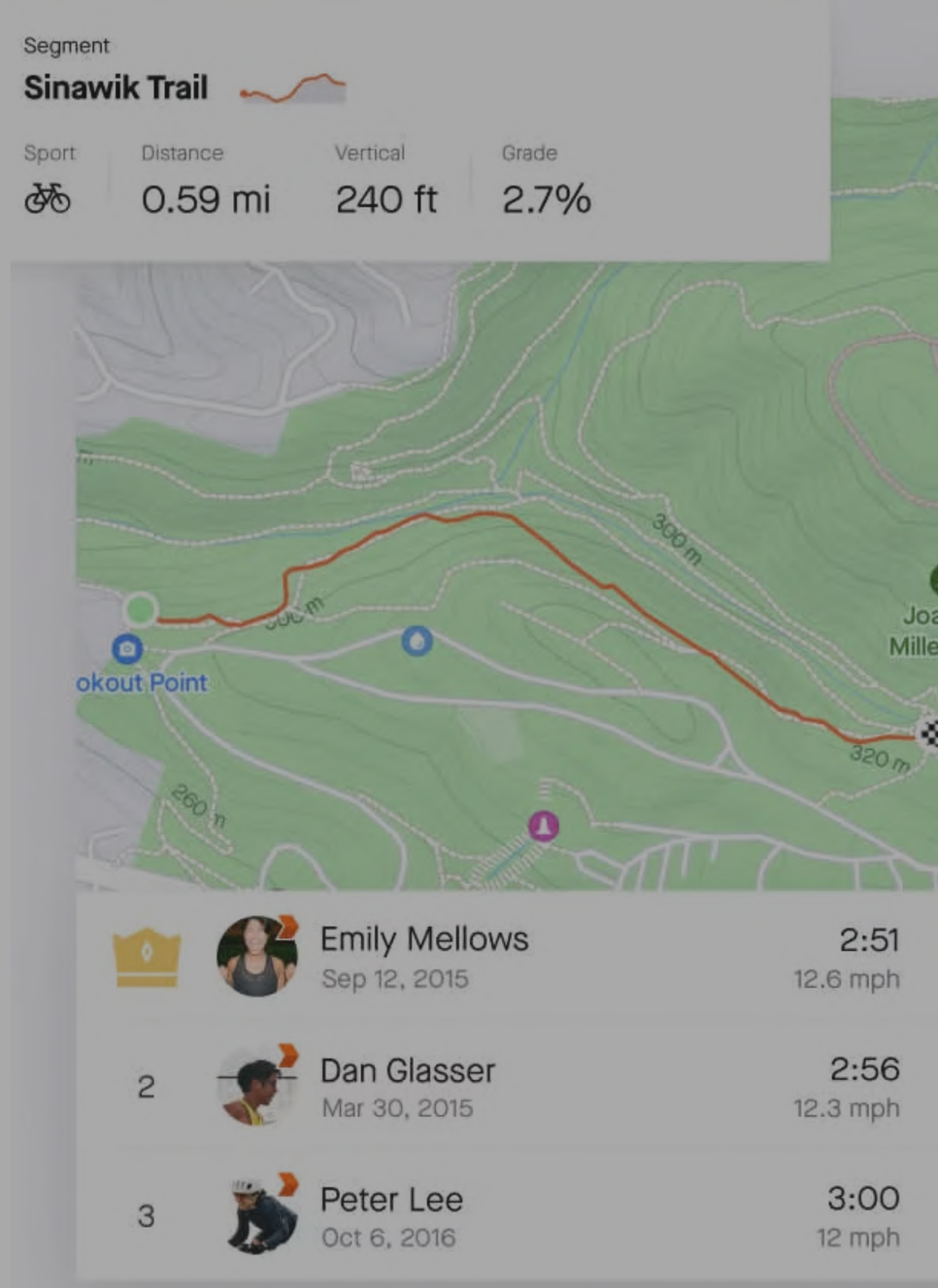
Simon Hurtz und Hakan Tanriverdi (2018). Fitness-App verrät sensible militärische Geodaten
https://www.sueddeutsche.de/wirtschaft/strava-fitness-app-verraet-sensible-militaerische-geodaten-1.3845538

Soziales Netzwerk

Alleinstellungsmerkmal

- Leistungsvergleich unter Freunden
- virtuelle Wettkämpfe
- Regionale Bestenlisten

Einschränkbare Sichtbarkeit

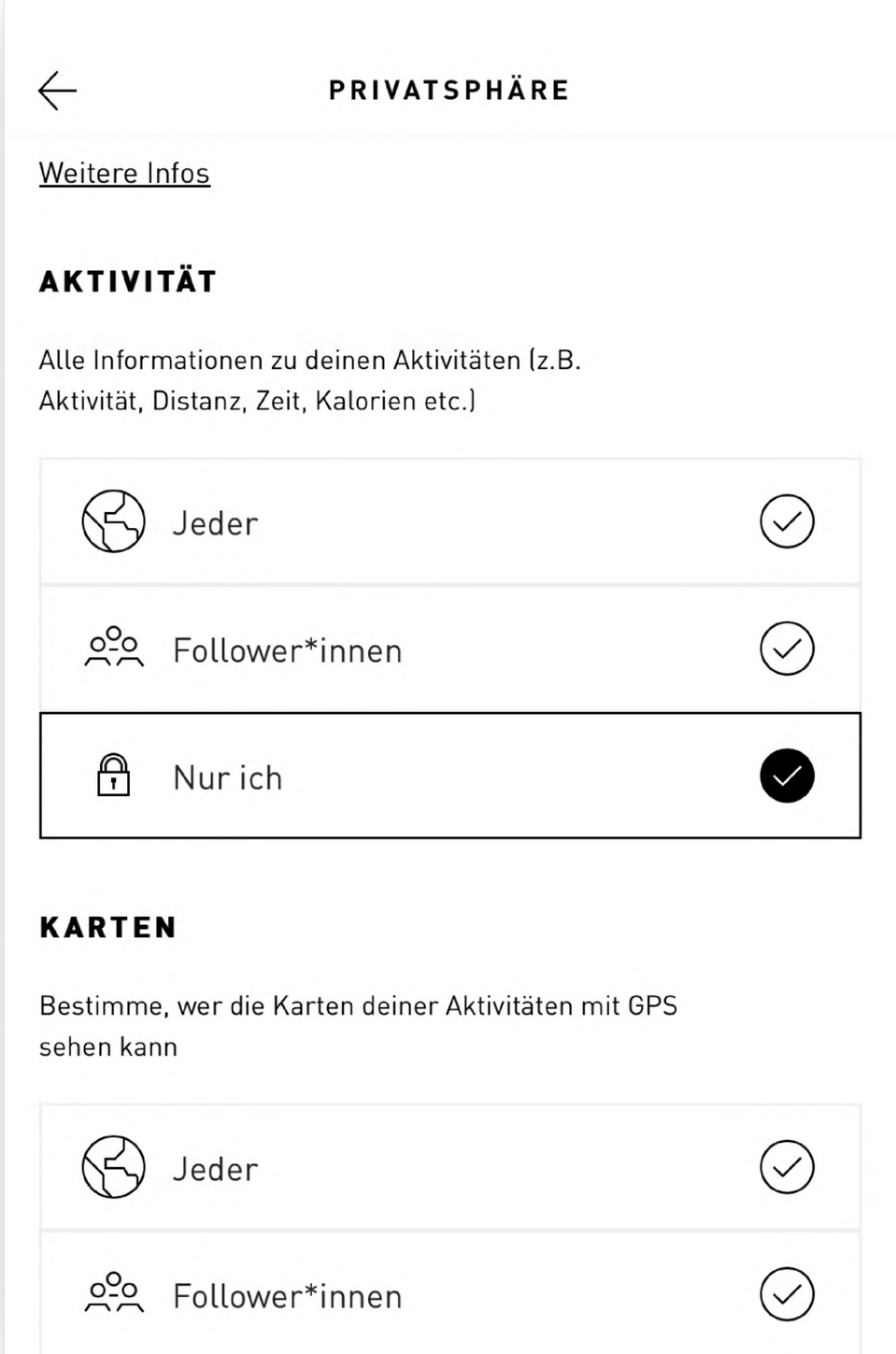


Strava (12.2024). https://www.strava.com/get-started

Privatsphäre

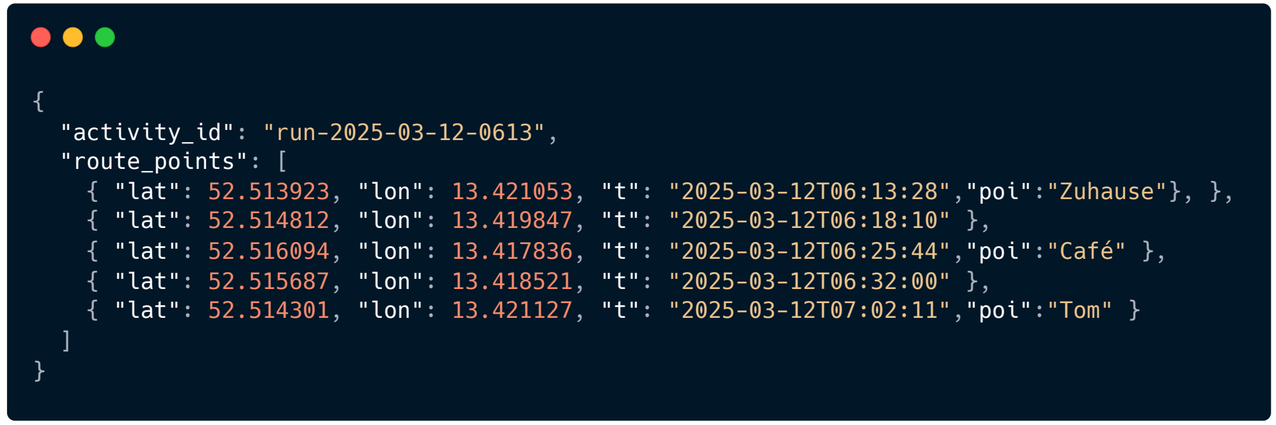
Privacy by Default

- Restriktive Standardeinstellungen
- Einschränkbare Sichtbarkeit
- Bestätigung von Freundschaftsanfragen
- Rohdaten nur lokal abspeichern



adidas Running: Tracking App (12.2024). https://www.runtastic.com

Verringerte Präzision & Aggregation



```
{
  "activity_id": "run-2025-03-12-0613",
  "route_points": [
    { "lat": 52.513923, "lon": 13.421053, "t": "2025-03-12T06:13:28","poi":"Zuhause"}, },
    { "lat": 52.514812, "lon": 13.419847, "t": "2025-03-12T06:18:10" },
    { "lat": 52.516094, "lon": 13.417836, "t": "2025-03-12T06:25:44","poi":"Café" },
    { "lat": 52.515687, "lon": 13.418521, "t": "2025-03-12T06:32:00" },
    { "lat": 52.514301, "lon": 13.421127, "t": "2025-03-12T07:02:11","poi":"Tom" }
  ]
}
```

Private Daten

- Hohe Geo-Koordinaten-Präzision
- POI markiert
- Zeitstempel pro Geo-Punkt

Geteilte Daten

- Verringerte Geo-Koordinaten-Präzision
- Start/Ende und andere POI entfernt
- Aggregation der Zeit (Gesamtdauer)

```
{
  "activity_id": "run-2025-03-12-0613",
  "route_points_public": [
    { "lat": 52.515, "lon": 13.420 },
    { "lat": 52.516, "lon": 13.418 },
    { "lat": 52.515, "lon": 13.419 }
  ],
  "start_masked": true,
  "end_masked": true,
  "time_bucket": "Morning",
  "duration_sec": "3438"
}
```

Produktentwicklung

- **Welche Daten** braucht das Produkt wirklich?
- Wie werden Datenerhebungen transparent kommuniziert, **Einwilligungen** eingeholt und anonymisiert?
- Wie reagiert das System auf **Datenlöschanfragen**?

Innovation mit Nutzungsdaten

"Wir brauchen einen Nutzungsreport"

- Anweisung von 'oben'
- Fehlende Einwilligung
- Fehlende Zweckbindung

Mögliche Reaktion

- Hinweis auf fehlende Einwilligung und Zweckbindung
- Einbindung Datenschutzbeauftragte

Überlastung durch Datenlöschanfragen

Szenario

- Datenlöschanfragen nie in Betracht gezogen
- Fehlende Datenklassifizierung
- Unklare Verteilung der Daten

Auswirkung

- Fehleranfällige manuelle Löschung
- Fristen können nicht eingehalten werden

Unvorhergesehene Verarbeitung

'falsch' genutztes Feature

- Bsp.: Tagebuch-Feature enthält sensible Daten (Freitextfeld)

Sensible Daten in Observability-Tooling

- Logging sensibler Daten
- Speicherung in Ticketsystemen
  z.B. Bugreports

Fahrlässigkeit

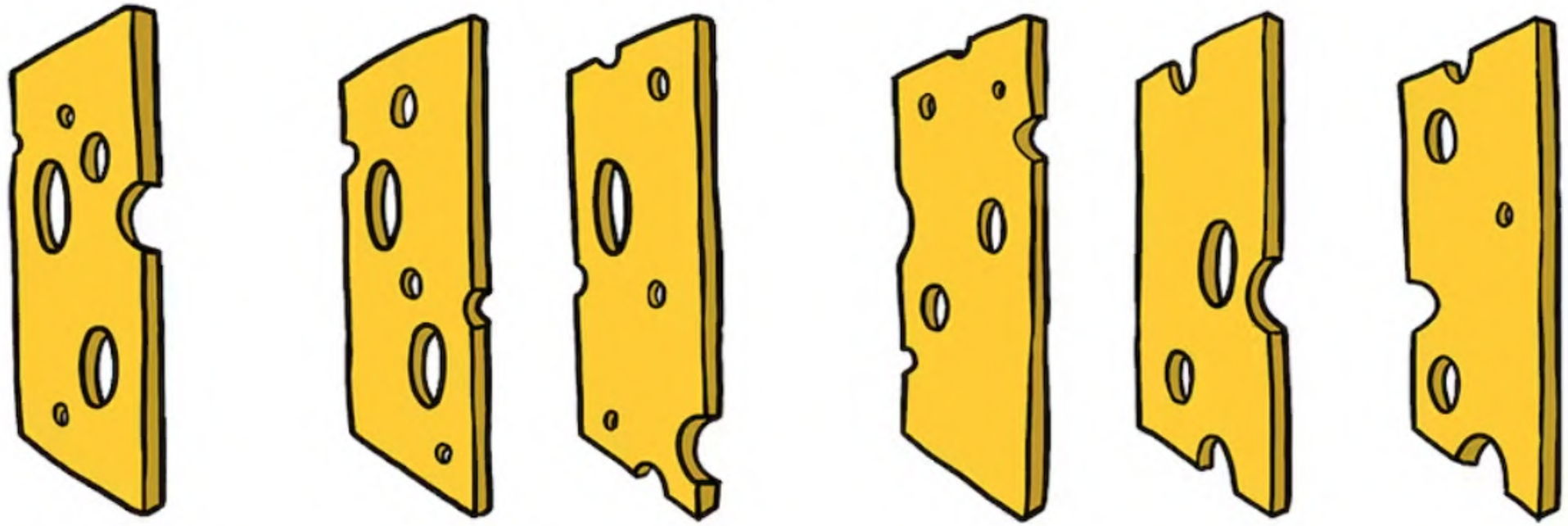
"Unsere Partner vertrauen auf uns, wir können Lücken nicht einfach zugeben."

- Blockierende Haltung ggü. internen Audits

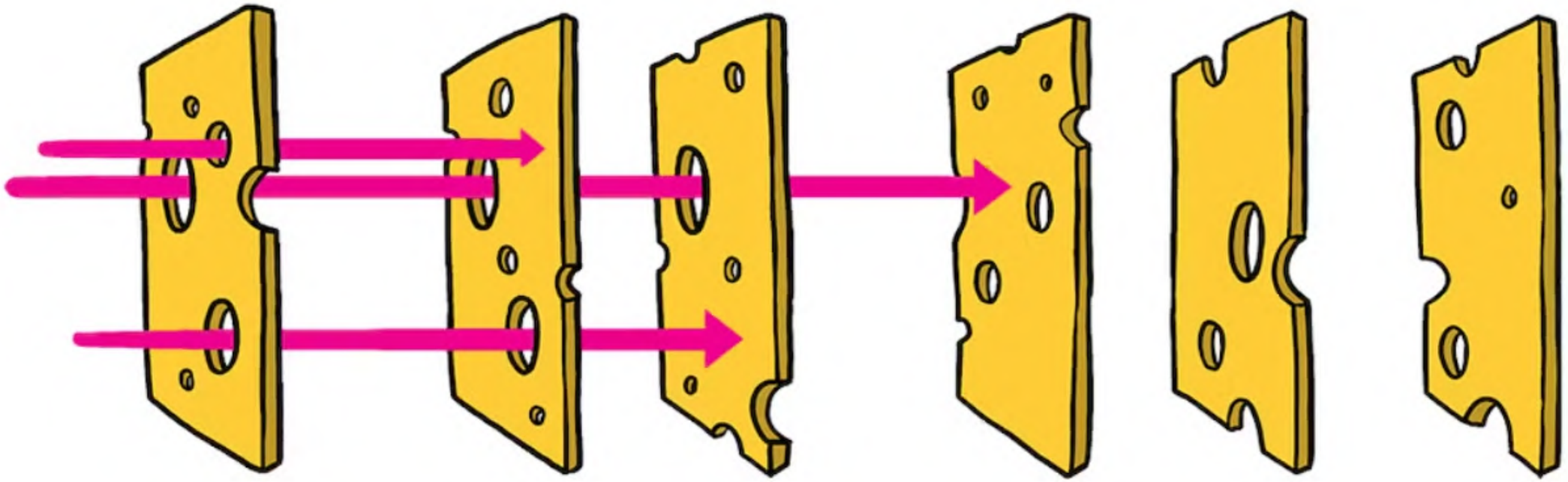
Mögliche Reaktion

- Einbindung Datenschutzbeauftragte

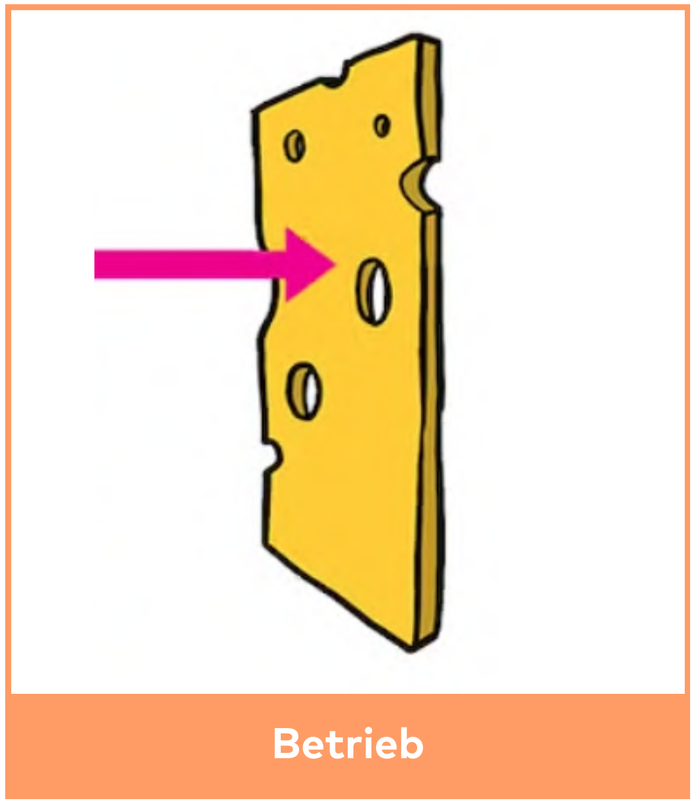
Schweizer-Käse-Modell



Schweizer-Käse-Modell

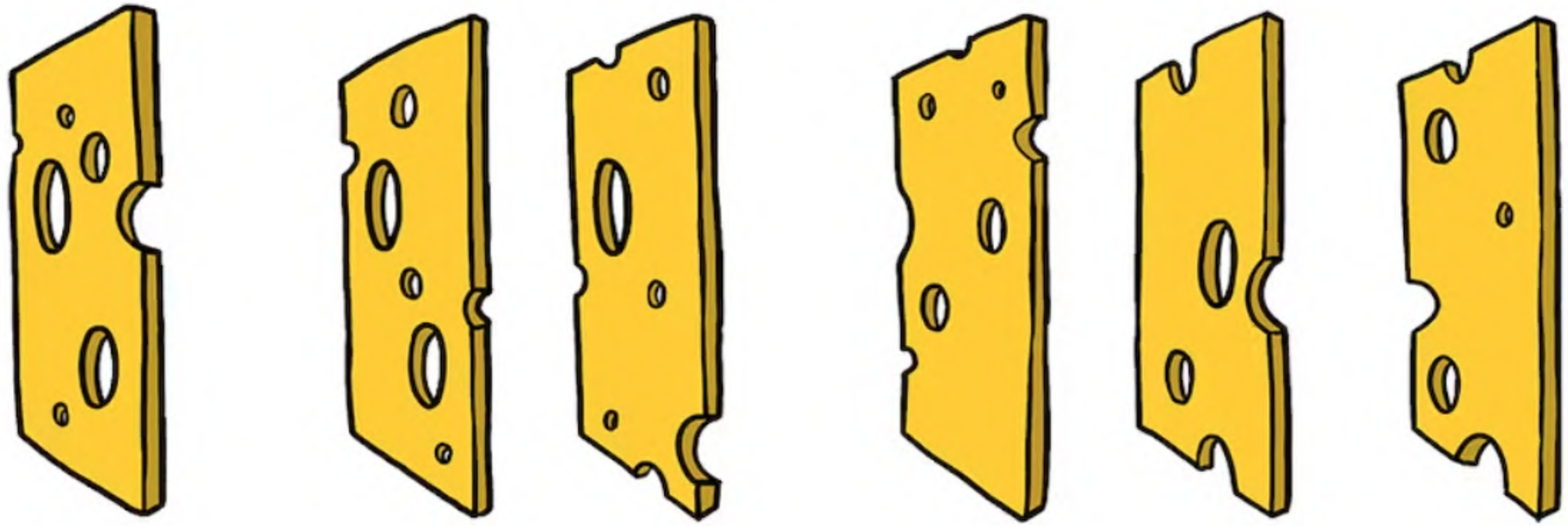


Schweizer-Käse-Modell

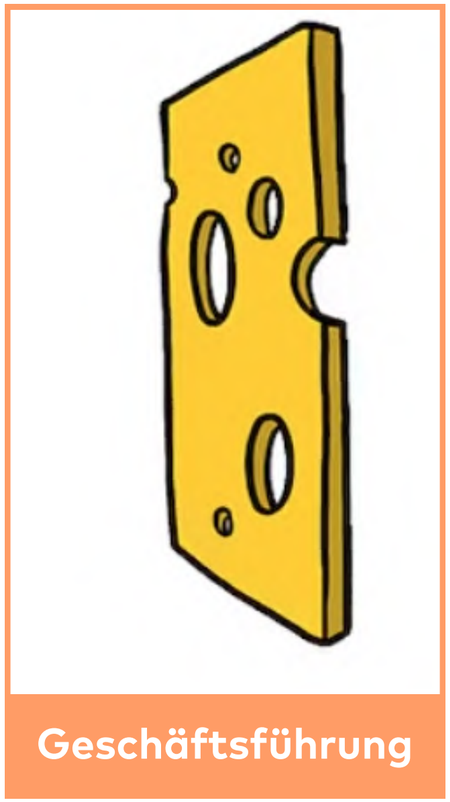


Betrieb

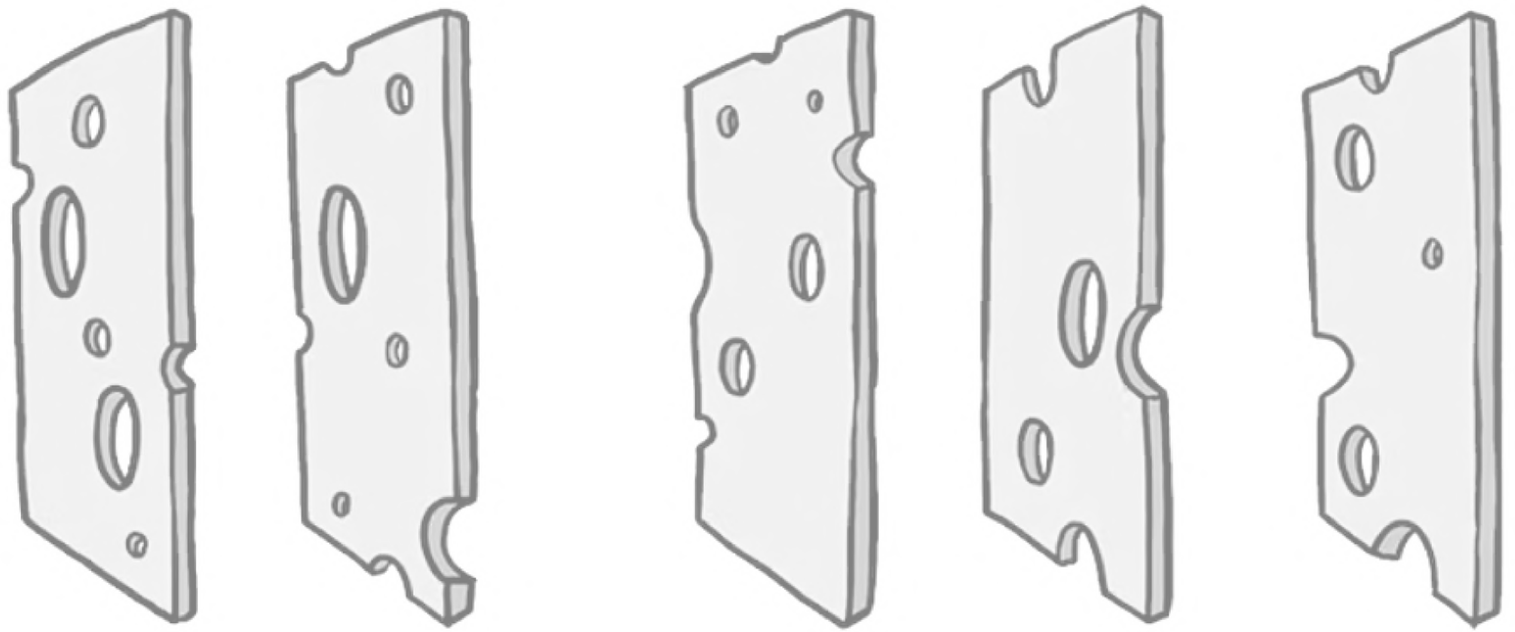
Schweizer-Käse-Modell



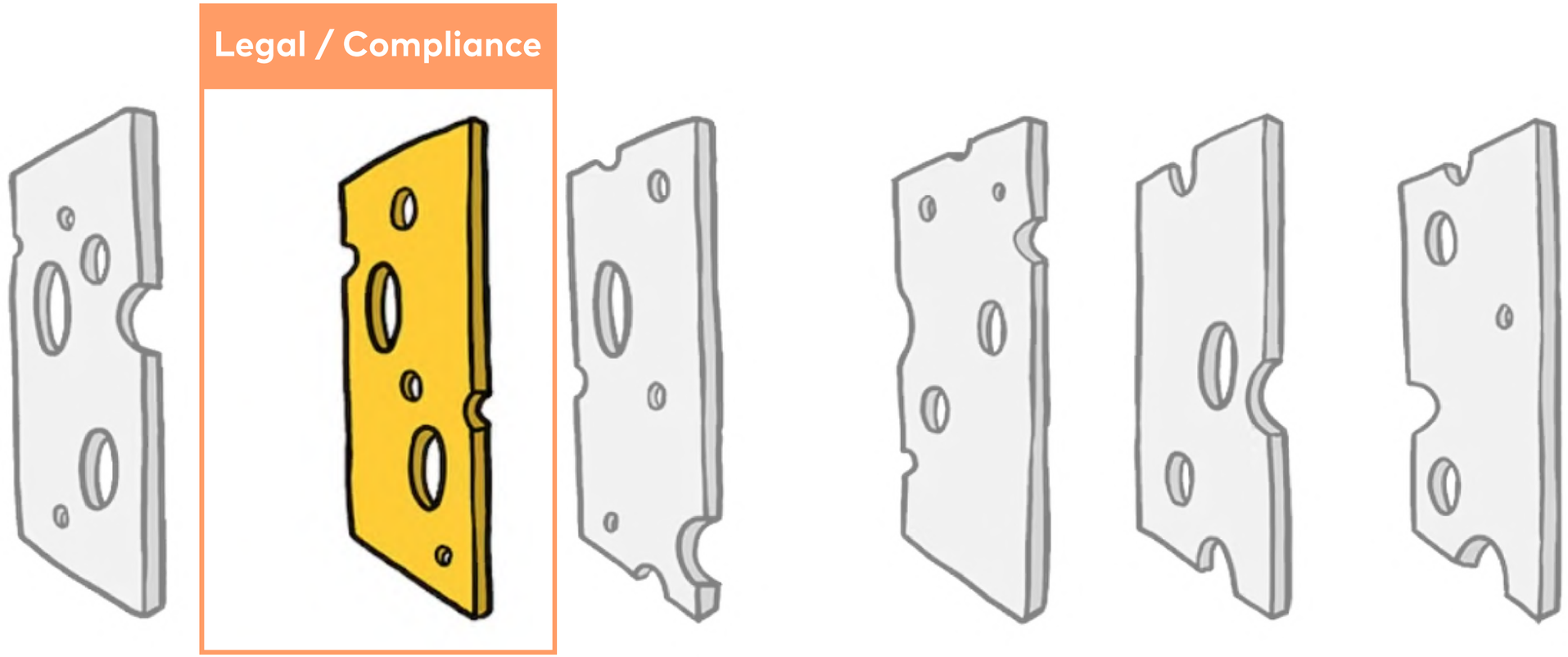
Schweizer-Käse-Modell



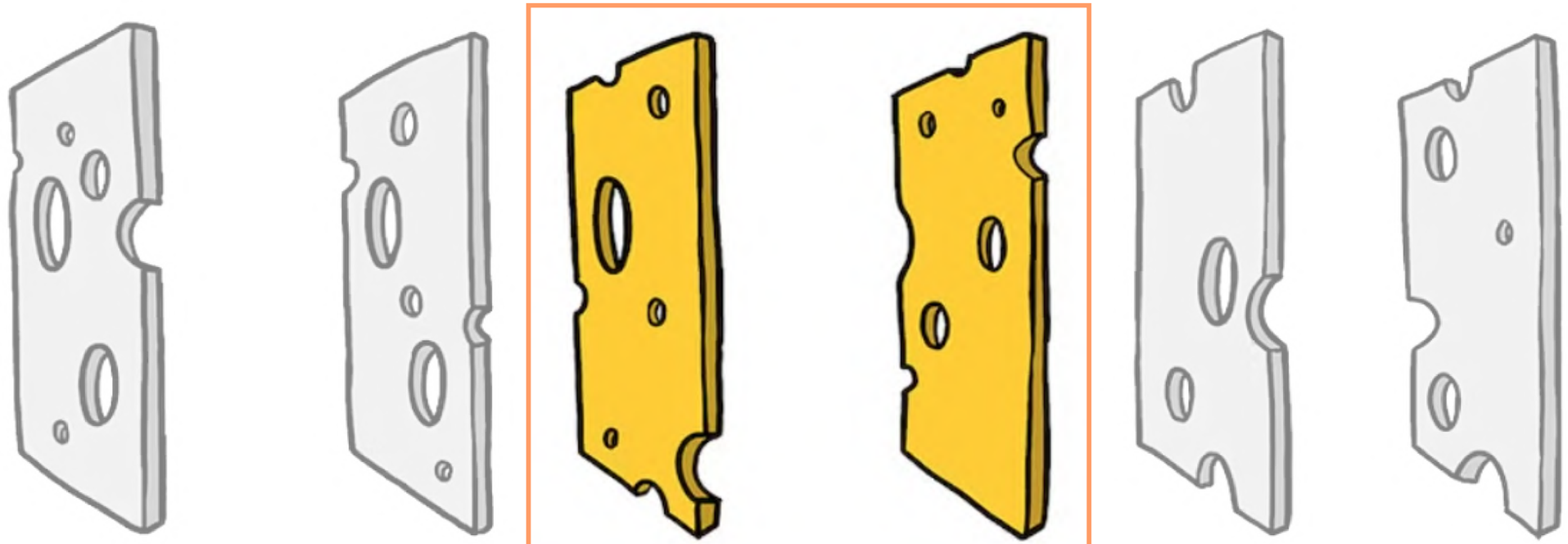
Geschäftsführung



Schweizer-Käse-Modell

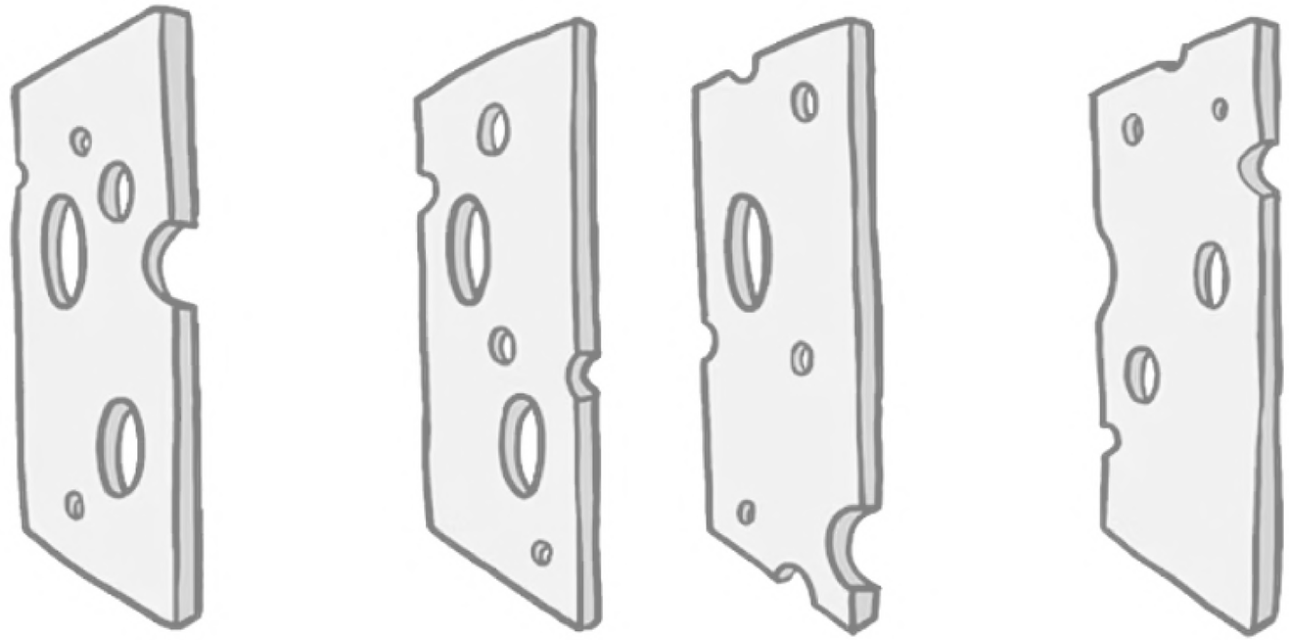


Schweizer-Käse-Modell

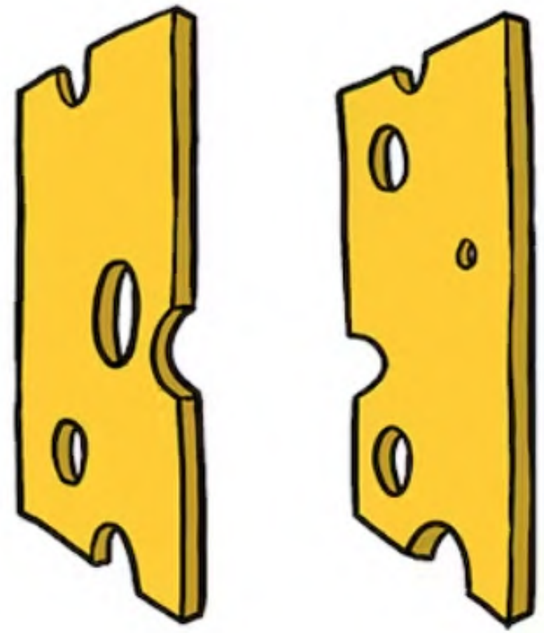


Produkt- und Projektsteuerung

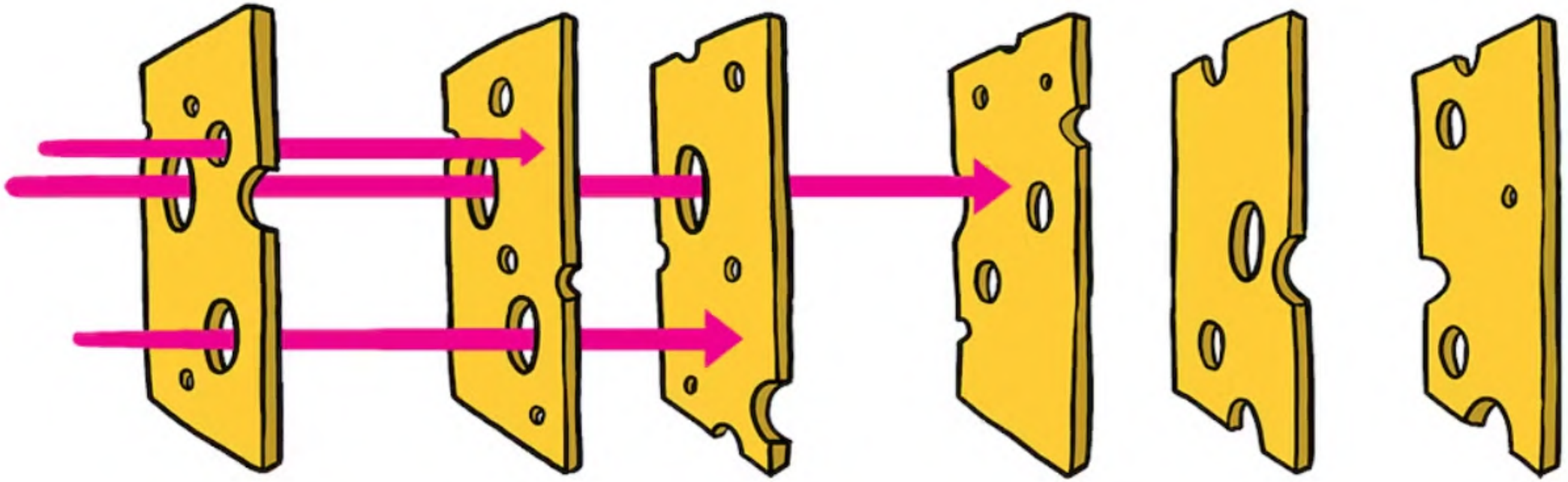
Schweizer-Käse-Modell



Operative Umsetzung



Schweizer-Käse-Modell



Soziotechnische Maßnahmen
Für soziotechnische Probleme

Top-Down-Signale

Top-Down-Signale

Datensicherheit als Unternehmensidentität

- Etablieren einer selbstverständlichen Kultur, um Datensicherheit und Weiterbildung
- Vorbild Apple als “Privacy Company”

Einbindung ins Requirements Engineering

Einbindung ins Requirements Engineering

Datensicherheit als Teil des Entwicklungsprozesses

- Privacy Impact Assessment
- Konzeption
- User Stories
- Akzeptanzkriterien
- Definition-of-Done-Kriterien
- Code-Reviews
- Quality Assurance & Testing

Tooling und Automatisierung

Tooling und Automatisierung

Automatisierte Security-Scans und Pseudonymisierungs-/ Anonymisierungswerkzeuge

- Tokenisierung
- Maskierung
- Anonymisierung
- Log-Scanning

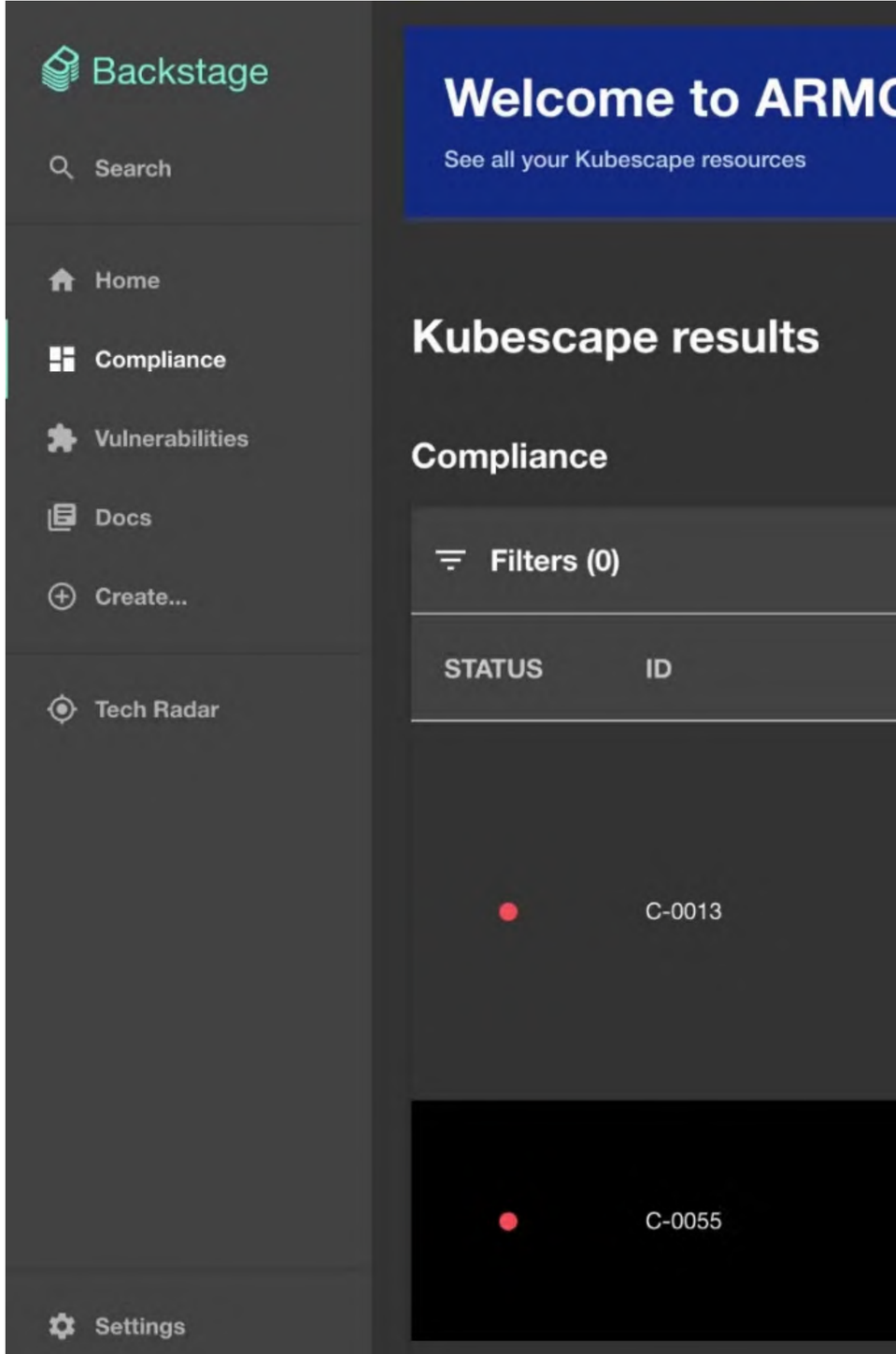
Automatisierte Datenauskunft & -Löschung

Self-Service Plattform

Self-Service Plattform

'Privacy by Design' als internes Produkt

- Auth-Infrastruktur
- Automatisiertes Backup & Recovery
- Technische Grundlage für Daten-Tagging
- Templates & Dokumentation

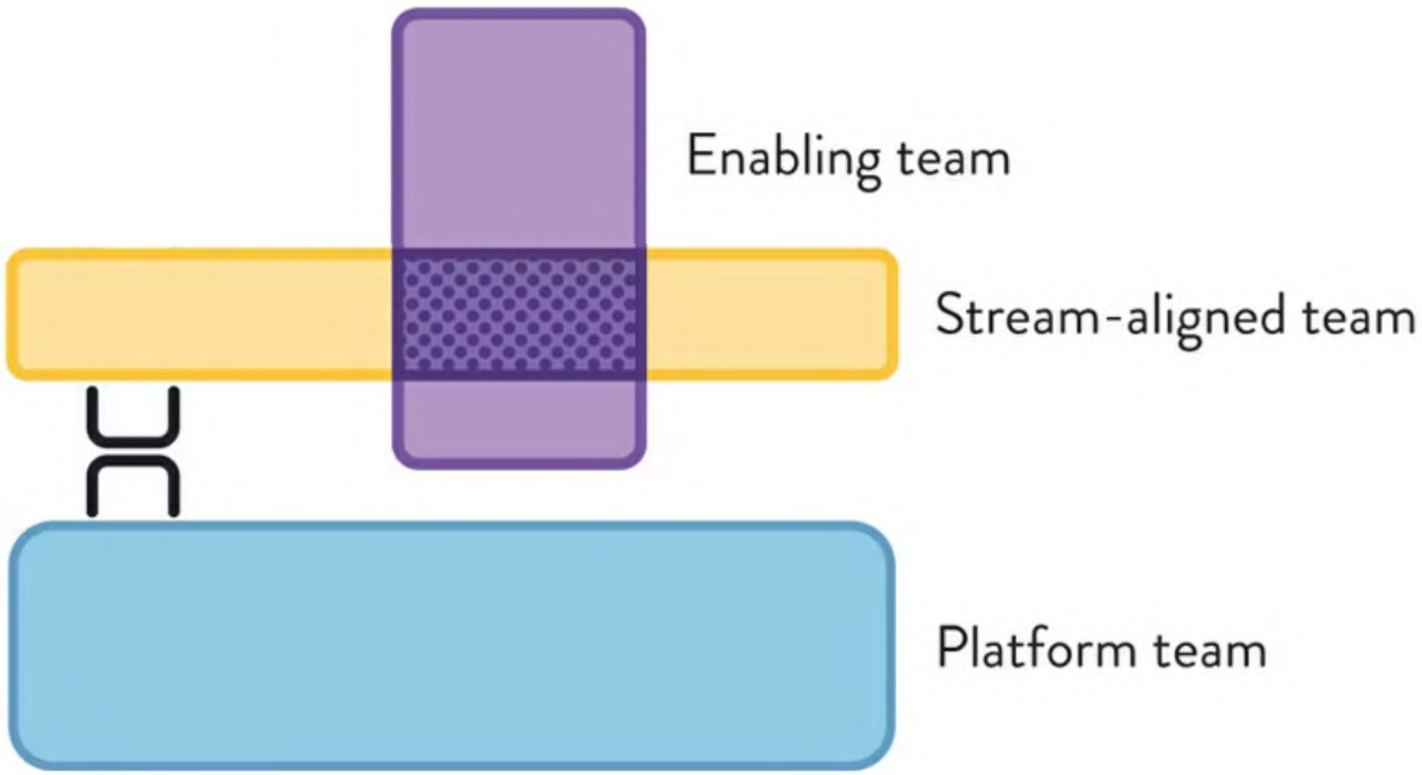


Screenshot (links):
Let's Go Backstage: IDP Security for Platform Engineers
Rotem Refael, ARMO & Suzanne Daniels, Spotify
https://kccnceu2023.sched.com/event/1HyYi/lets-go-backstage-idp-security-for-platform-engineers-rotem-refael-armo-suzanne-daniels-spotify

Dedizierter Support

Unterstützende

Teams



Team Topologies. Organizing Business and Technology Teams for fast Flow. Matthew Skelton, Manuel Pais. (2019). p. 80

Soziotechnische Maßnahmen

Top-Down-Signale

Datensicherheit als Unternehmensidentität

Einbindung ins Requirements Engineering

Datensicherheit als Teil des Entwicklungsprozesses

Tooling und Automatisierung

Automatisierte Security-Scans und Anonymisierungs-werkzeuge

Self-Service Plattform

'Privacy by Design' als internes Produkt

Schweizer Käse Modell

Trotz Lücken, trägt jede Rolle zur Sicherheit bei

Dedizierter Support

Unterstützung bei der Umsetzung

Danke!

INNOQ
www.innoq.com

Anja Kammer
anja.kammer@innoq.com

Cloud Computing | Entwicklungsprozesse | Platform Engineering

innoQ Deutschland GmbH

Krischerstr. 100
40789 Monheim
+49 2173 333660

Ohlauer Str. 43
10999 Berlin

Ludwigstr. 180E
63067 Offenbach

Kreuzstr. 16
80331 München

Wendenstr. 130
20537 Hamburg

Spichernstr. 44
50672 Köln