

# Privacy by Design

Strategien für eine datenschutzkonforme Softwarearchitektur

## Christian Seifert

Principal Software Architect  
esentri AG

[christian.seifert@esentri.com](mailto:christian.seifert@esentri.com)  
<https://team.esentri.com/christian-seifert>  
<https://linkedin.com/in/cn-seifert>



***Data protection is not just  
about protecting data but  
protecting people***

Věra Jourová (EU-Kommissarin für Justiz und Verbraucherschutz 2014-2019)

Beispiel 1 (2019)

# Deutsche Wohnen

Verhängtes Bußgeld in Höhe von

**14,5 Mio €**

*Bei Vor-Ort-Prüfungen [...] hat die Aufsichtsbehörde festgestellt, dass das Unternehmen für die Speicherung personenbezogener Daten von Mieterinnen und Mietern ein Archivsystem verwendete, das **keine Möglichkeit** vorsah, **nicht mehr erforderliche Daten zu entfernen**.*

*Personenbezogene Daten [...] wurden gespeichert, **ohne zu überprüfen**, ob eine Speicherung **zulässig** oder überhaupt **erforderlich** ist.*

[https://www.datenschutz-berlin.de/fileadmin/user\\_upload/pdf/pressemitteilungen/2019/20191105-PM-Bussgeld\\_DW.pdf](https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2019/20191105-PM-Bussgeld_DW.pdf)

**Beispiel 2 (2019)**

**1&1**

**Verhängtes Bußgeld in Höhe von**

**900 Tsd €**

**(Herabgesetzt von ursprünglich 9,5 Mio €)**

*Die Aufsichtsbehörde wirft der Firma vor, dass Unberechtigte an der Telefon-Hotline vergleichsweise einfach "**weitreichende Informationen zu weiteren personenbezogenen Kundendaten**" erhalten konnten. Die Angabe von Namen und Geburtsdatum von Betroffenen hätten ausgereicht.*

<https://www.heise.de/news/DSGVO-Verstoss-1-1-muss-knapp-10-Millionen-Euro-Strafe-zahlen-4608676.html>

Beispiel 3 (2019)

# Österreichische Post

Verhängtes Bußgeld in Höhe von

**18 Mio €**

*Die Datenschutzbehörde sah es [...] als erwiesen an,  
dass die ÖPAG durch die Verarbeitung von  
personenbezogenen Daten über die  
**vermeintliche politische Affinität**  
von Betroffenen gegen die DSGVO verstoßen hat.*

*Darüber hinaus wurde u.a. eine Rechtsverletzung  
wegen der **Weiterverarbeitung** von Daten über die  
**Paketfrequenz** und die **Häufigkeit von Umzügen** zum  
Zweck des Direktmarketings festgestellt, weil dies  
**keine Deckung in der DSGVO** findet.*

[https://www.ots.at/presseaussendung/OTS\\_20191029\\_OTS0095/strafverfahren-gegen-oesterreichische-post-ag](https://www.ots.at/presseaussendung/OTS_20191029_OTS0095/strafverfahren-gegen-oesterreichische-post-ag)

Was hat das alles mit  
**Softwarearchitektur**  
zu tun?

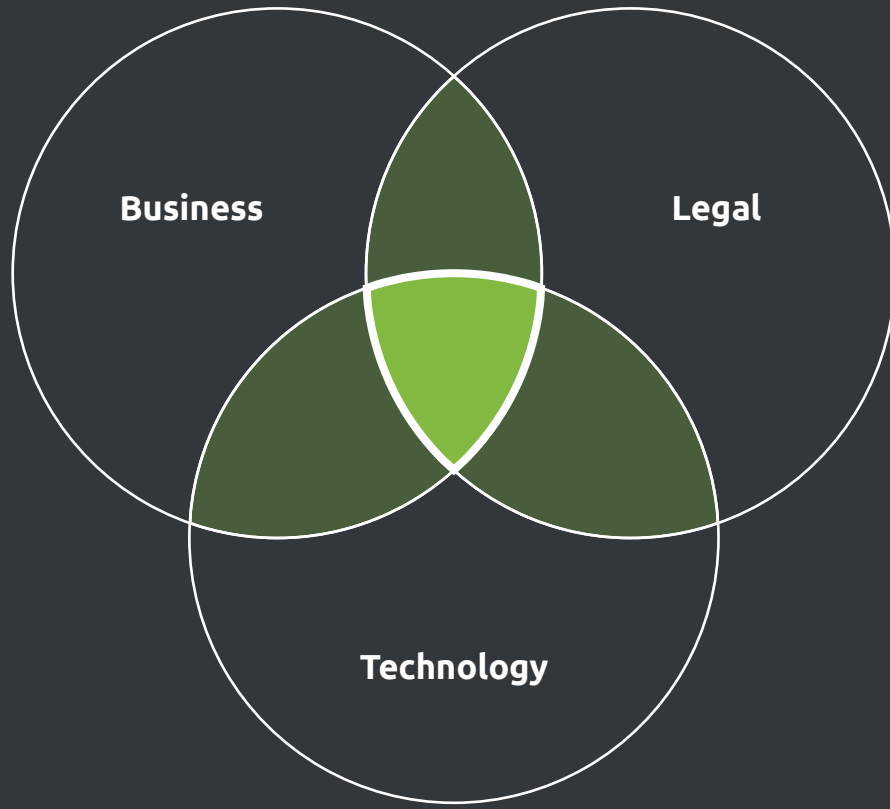


Ist das überhaupt  
**unsere** Aufgabe?



***Security is not a  
product but a process***

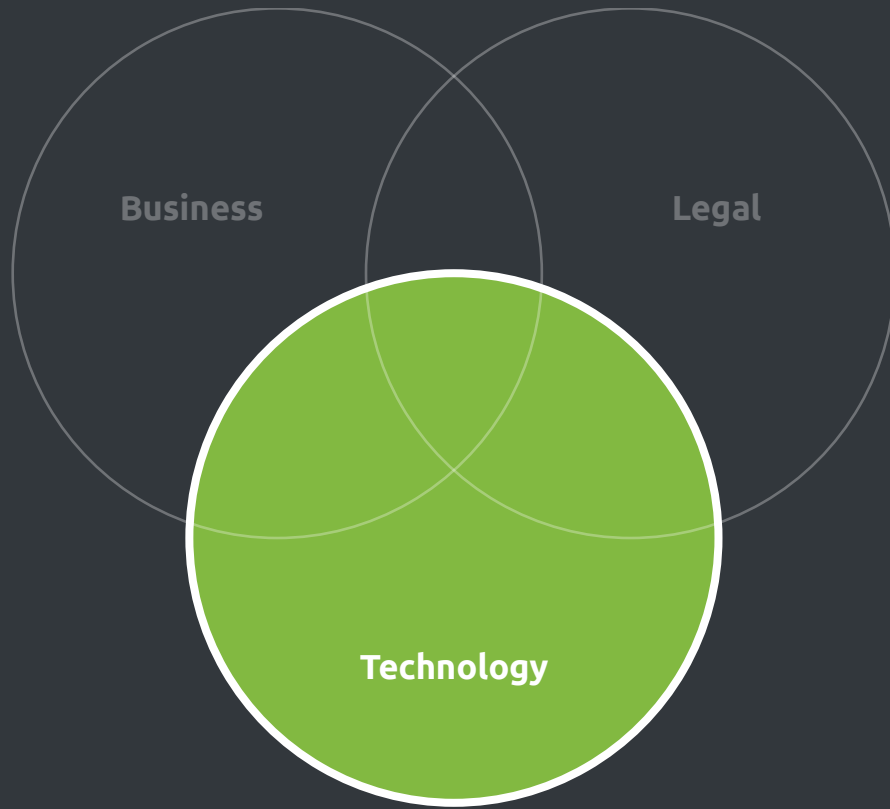
Bruce Schneier, «Elder Statesman» der Cybersecurity-Industrie

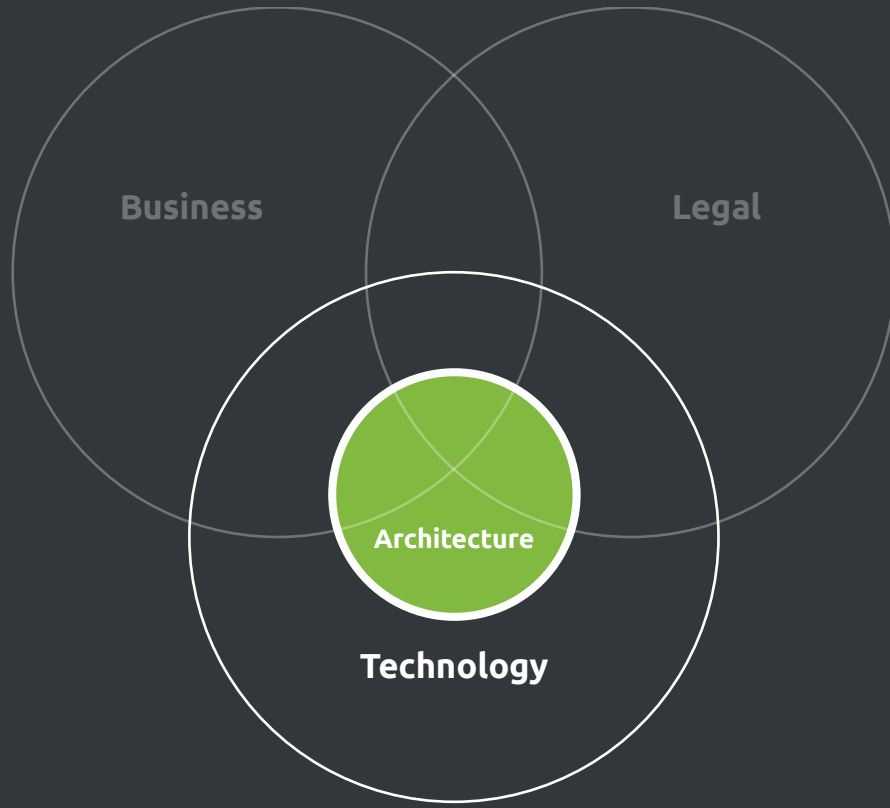


# Achtung!

Dieser Vortrag  
ist (und ersetzt)  
keine Rechtsberatung!







# Privacy **by** Design



»Privacy by Design« is a **development approach** that integrates privacy considerations and safeguards into the **entire software development lifecycle**, ensuring that user privacy is prioritized and protected **from the outset**.

ChatGPT

# Fünf Schlüsselprinzipien von Privacy by Design





**Proaktiv** statt reaktiv



**Jederzeit** im Design präsent



# Privacy by Default



**Kein Gegensatz  
von Privatsphäre  
und Funktionalität**



**Ende zu Ende**

# Praktische Auswirkungen auf das **Design** und die **Architektur** unserer Software



# Datensammlung und Datenverarbeitung begründen und minimieren



# Ablaufzeiten definieren und nachhalten



# Anonymisierung bzw. Pseudonymisierung



```
@Entity
@DataPrivacyRelevant
public class CustomerEntity {

    @Column
    @NotEmpty
    @DataPrivacy(
        collectionBasis=DataPrivacyCollectionBasis.LEGALLY_REQUIRED
        legalBasis="Creation of invoice"
        expiration="P10Y"
    )
    String lastName;

    @Column
    @DataPrivacy(
        collectionBasis=DataPrivacyCollectionBasis.VOLUNTARY
        expiration="P1Y"
    )
    LocalDate dateOfBirth;

}
```

```
@Entity
public class CustomerDataPrivacyTracking {

    @Column CustomerEntity customer;
    @Column String dataField;
    @Column DataPrivacyCollectionBasis collectionBasis;
    @Column LocalDate firstCollectedAt;
    @Column LocalDate lastCollectedAt;
    @Column LocalDate lastConsentedAt;
    @Column String lastConsentedThrough;
    @Column LocalDate expiresAt;

}
```

| Customer ID | Data field  | Collection basis | First collected at | Last collected at | Last consented at | Last consented through                 | Expires at |
|-------------|-------------|------------------|--------------------|-------------------|-------------------|----------------------------------------|------------|
| 4711        | firstName   | Legally required | 2023-01-01         | 2023-01-01        |                   |                                        | 2033-01-01 |
| 4711        | lastName    | Legally required | 2023-01-01         | 2023-01-01        |                   |                                        | 2033-01-01 |
| 4711        | dateOfBirth | Voluntary        | 2023-05-05         | 2023-05-05        | 2023-05-05        | Website                                | 2024-05-05 |
| 5566        | firstName   | Legally required | 2018-06-06         | 2023-05-25        |                   |                                        | 2033-05-25 |
| 5566        | dateOfBirth | Voluntary        | 2023-03-05         | 2023-03-05        | 2023-03-05        | Website                                | 2024-03-05 |
| 5566        | dateOfBirth | Legally required | 2023-05-25         | 2023-05-25        | 2023-05-25        | Order process (age restricted content) | 2033-05-25 |

**Annotiertes  
Datenmodell**

```
graph TD; A[Annotiertes Datenmodell] --> B[Dokumentation]; A --> C[Tooling];
```

**Dokumentation**

**Tooling**

# Daten **verschlüsseln**

("at rest" und "in transit")



Authentication (AuthN)

# Eindeutige Identifizierung von Akteuren

(Menschen und Maschinen)



Authorization (AuthZ)

# Berechtigungs- und Sicherheitskonzept



# Audit-Logs



# Gutes Tooling



*Das ist ja richtig **aufwändig**  
und irgendwie auch **nervig**.*

*Muss ich das wirklich  
immer machen?!*

Ein Software-Architekt, der ungenannt bleiben möchte

Der größte Feind  
von Sicherheit ist  
**Bequemlichkeit**



Nicht wegducken,  
sondern **bewusst**  
mit dem Thema  
beschäftigen



*The world is a dangerous place,  
not because of those who do  
evil, but because  
of those who look on and  
do nothing*

Albert Einstein

# Danke!

**Privacy by Design:  
Strategien für eine datenschutzkonforme Softwarearchitektur**

**Euer Feedback**



**Christian Seifert**

Principal Software Architect  
esentri AG

[christian.seifert@esentri.com](mailto:christian.seifert@esentri.com)  
<https://team.esentri.com/christian-seifert>  
<https://linkedin.com/in/cn-seifert>

