# EU-DSGVO ab Mai 2018 – Lösungsansätze

Keine Angst, das beißt nicht!

Daniel Nelle
Senior Datenbank Admin und Security Spezialist
merlin.zwo InfoDesign GmbH & Co. KG
76228 Karlsruhe


merlin2wp
InfoDesign
ศรวีย์
SORAVEE
21

merlin2wo
InfoDesign

# EU-DSGVO, was Sie garantiert schon kennen!

merlin 2wo InfoDesign

77 Tage 11 Stunden 15 Minuten

(waren es bei Vortragsbeginn)


Relevant für Unternehmen weltweit.


Jedes Unternehmen braucht ein Datenschutz-Management-System

# Informations- und Auskunftspflichten


Data Protection by Design und Default

# Risikoanalyse und Folgeabschätzung


Datenverarbeitung in Konzernen wird vereinfacht


Datenschutzverstöße müssen innerhalb von 72h gemeldet werden


Bußgeld soll „in jedem Einzelfall wirksam, verhältnismäßig und abschreckend sein“

# Darum geht es: EU-DSGVO Artikel 32 Absatz 1

„(1) **Unter Berücksichtigung des Stands der Technik**, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die **Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche** und der Auftragsverarbeiter **geeignete technische und organisatorische Maßnahmen**, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.“

# Darum geht es: EU-DSGVO Artikel 32 Absatz 1

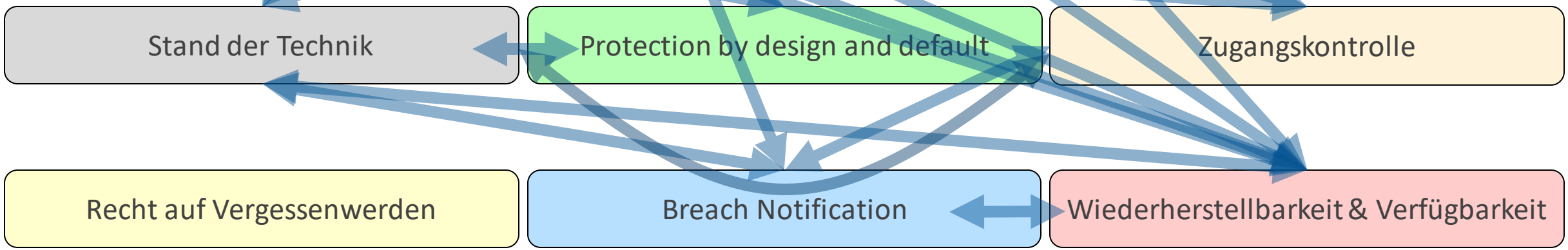
„(1) Unter Berücksichtigung des **Stands der Technik**, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

a) die **Pseudonymisierung** und **Verschlüsselung** personenbezogener Daten;

b) die Fähigkeit, die **Vertraulichkeit**, **Integrität**, **Verfügbarkeit** und **Belastbarkeit** der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

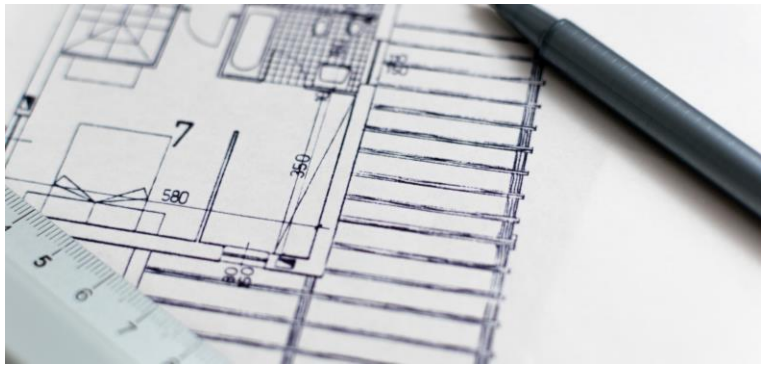
c) die Fähigkeit, die **Verfügbarkeit** der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall **rasch wiederherzustellen**;

d) ein Verfahren zur **regelmäßigen Überprüfung**, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.“



# Inhalt

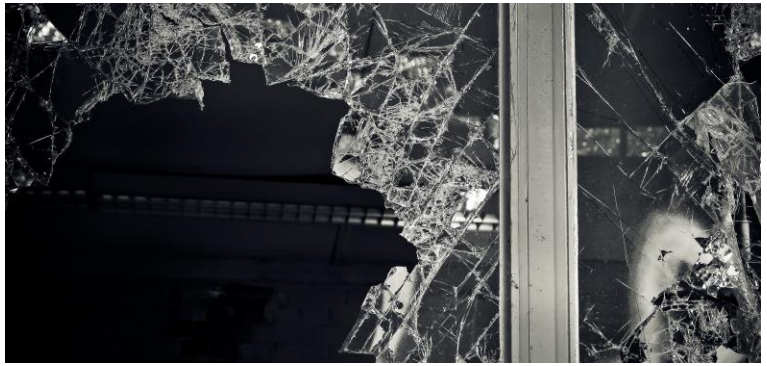
Stand der Technik



Data Protection by Design & Default

Zugangskontrolle

Recht auf Vergessenwerden



Breach Notification


Wiederherstellbarkeit & Verfügbarkeit

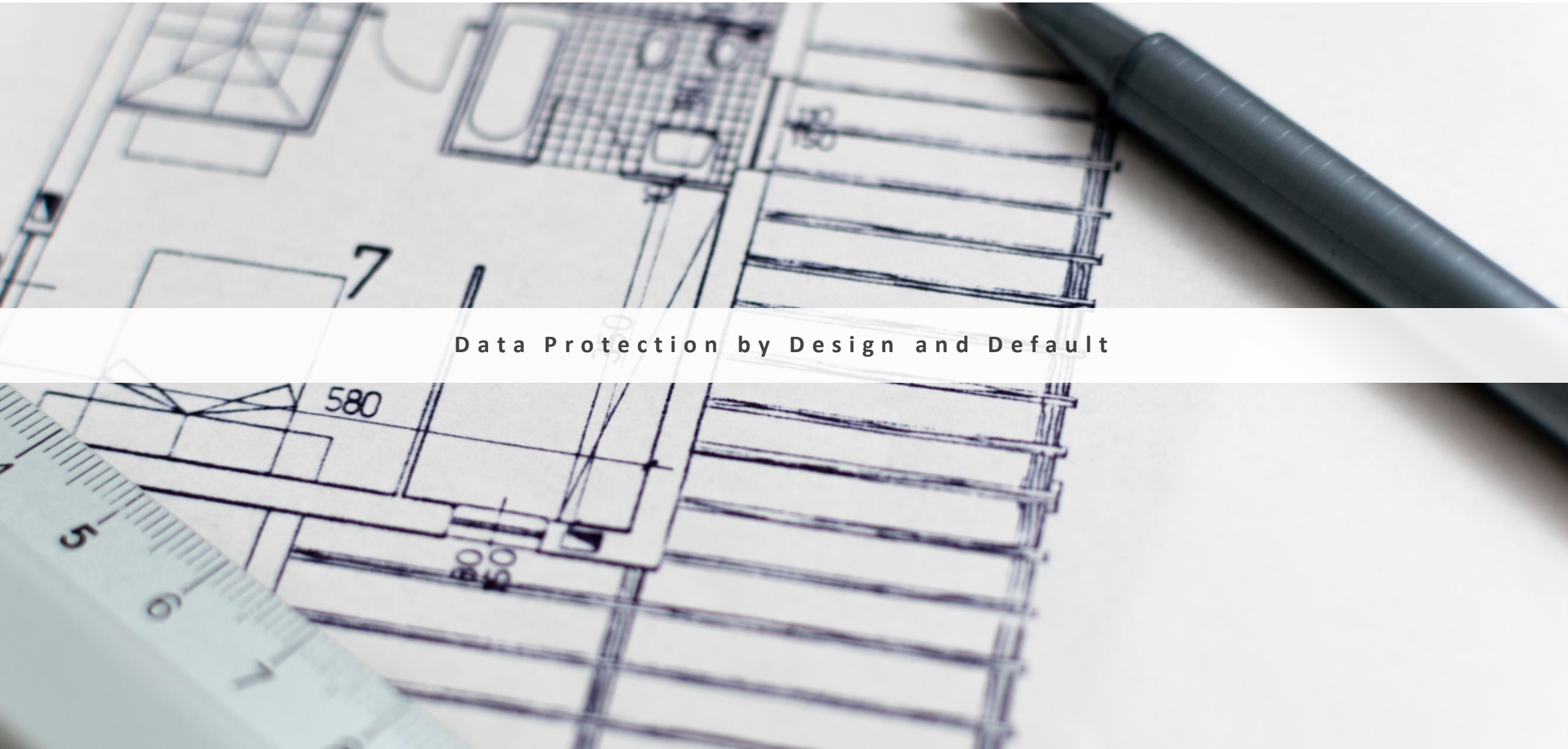

# Stand der Technik

# Stand der Technik

# Stand der Technik – Beispiel

- ~~WEP~~
- ~~WPA~~
- WPA2 ??? KRACK-Lücke von 10/2017
- WPA2 + VPN-Tunnel / SSL
- WPA2, 63-stelliger Key,
  alle *n*-Tage neuer Key
  + VPN-Tunnel / SSL

merlin 2nd
InfoDesign



# Data Protection by Design and Default

# „Data Protection by Design“ und „Data Protection by Default“

# „Data Protection by Design“ und „Data Protection by Default“

Was heißt das für die Praxis?

merlin 2.0
InfoDesign

# Zugangskontrolle

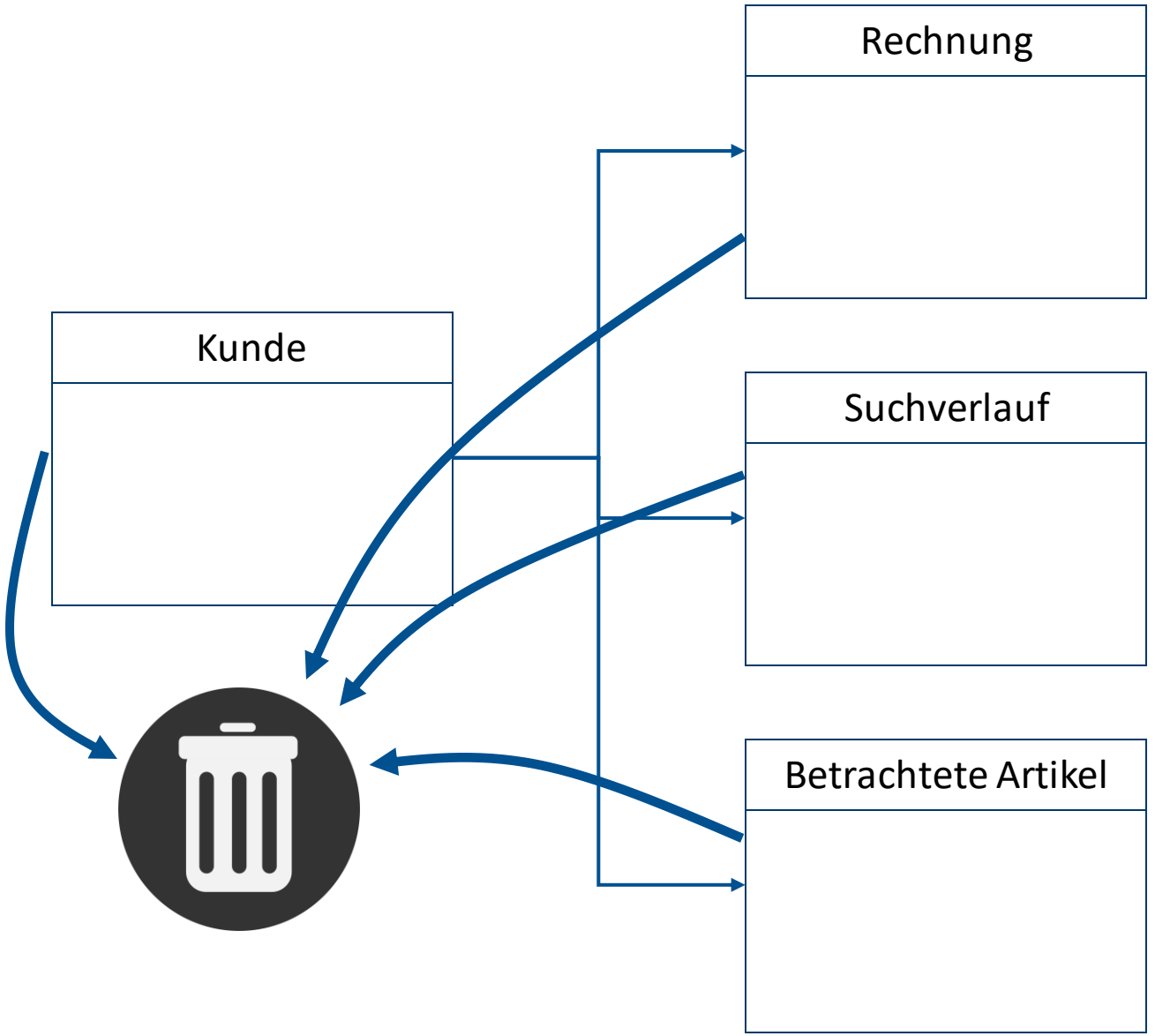

# Physischer Zugang


# Elektronischer Zugang

merlin2.0
InfoDesign

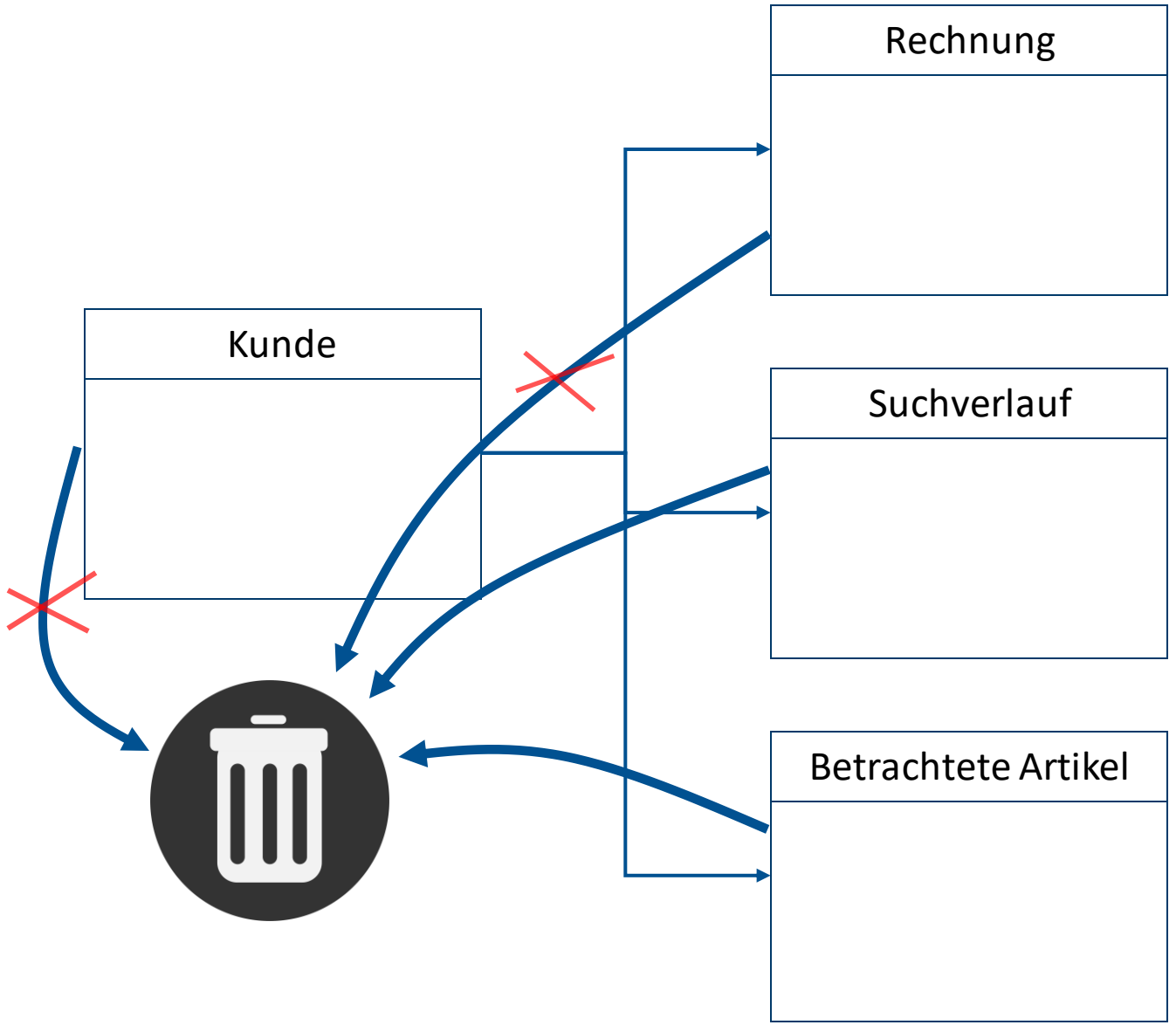
# Recht auf Vergessenwerden

# „Löschen – äääähhh, das geht nicht!“

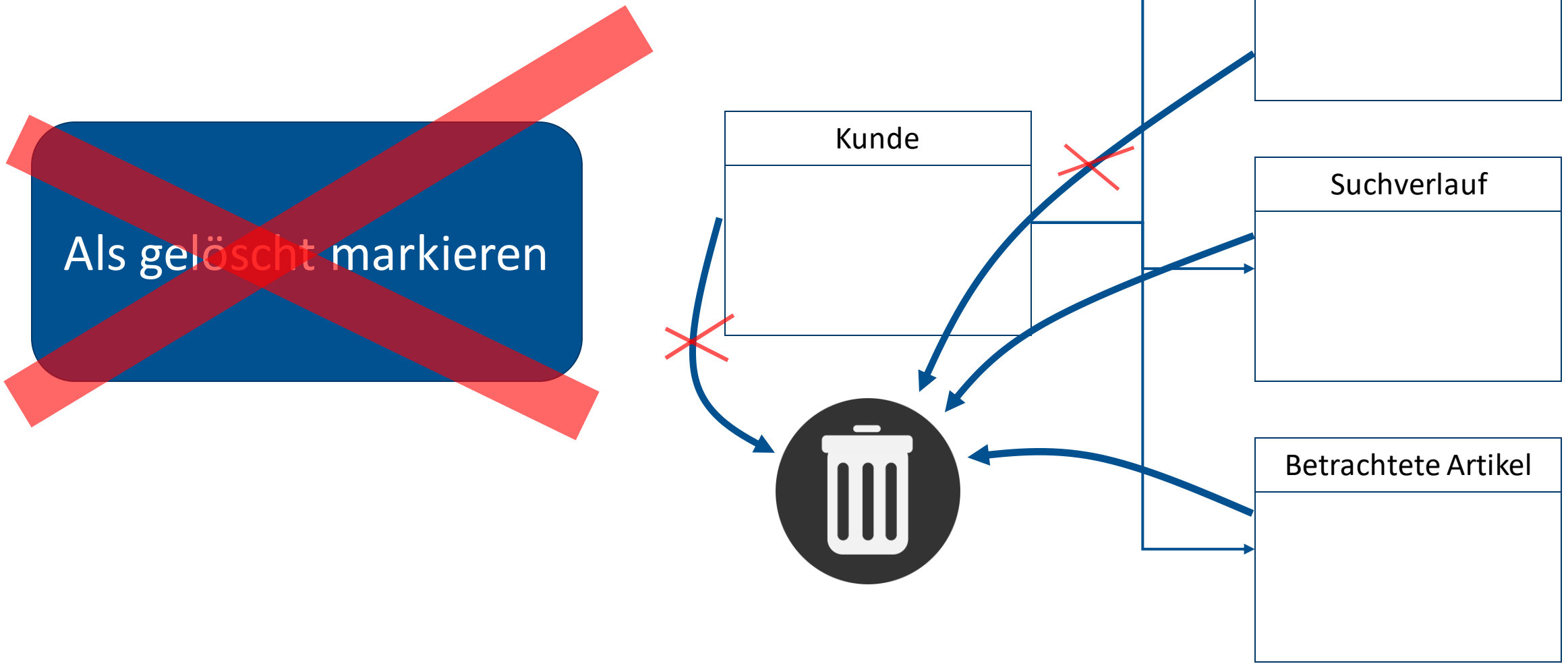


# „Löschen – äääähhh, das geht nicht!“

Jeder Datensatz muss einzeln betrachtet werden!

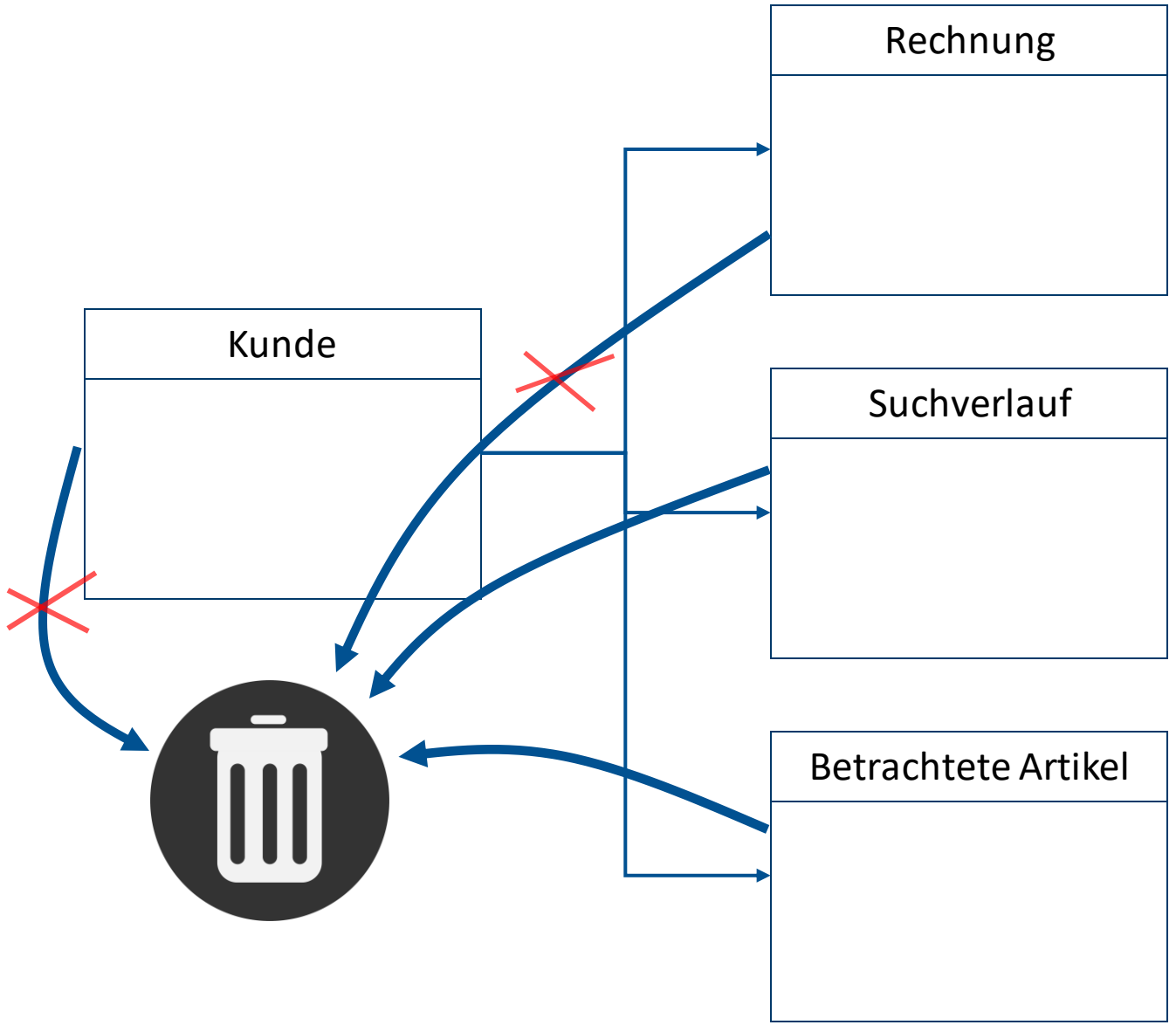


# „Löschen – äääähhh, das geht nicht!“



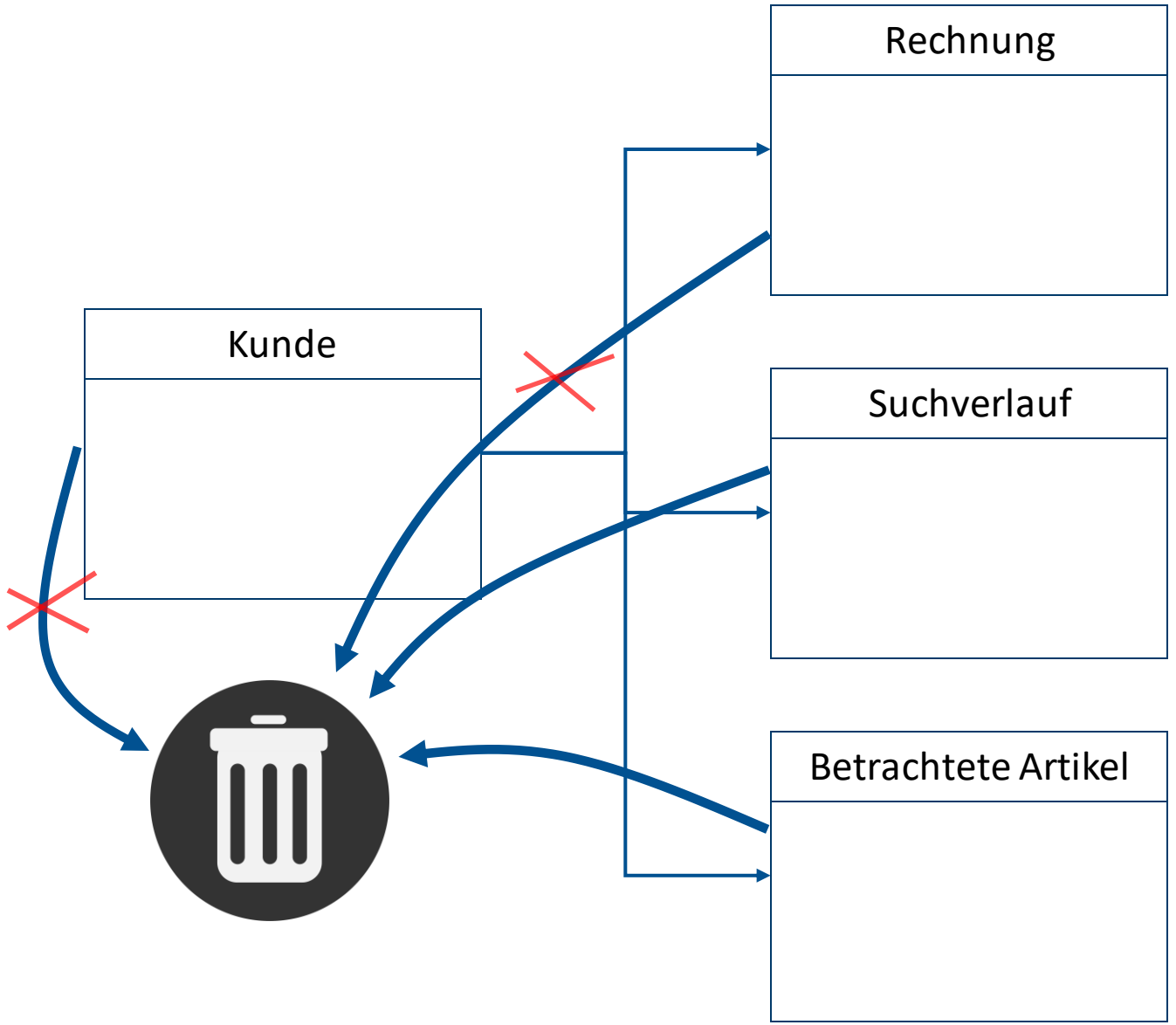
# „Löschen – äääähhh, das geht nicht!“

Nachvollziehbarkeit, Erfüllung anderer Gesetze!



# „Löschen – äääähhh, das geht nicht!“

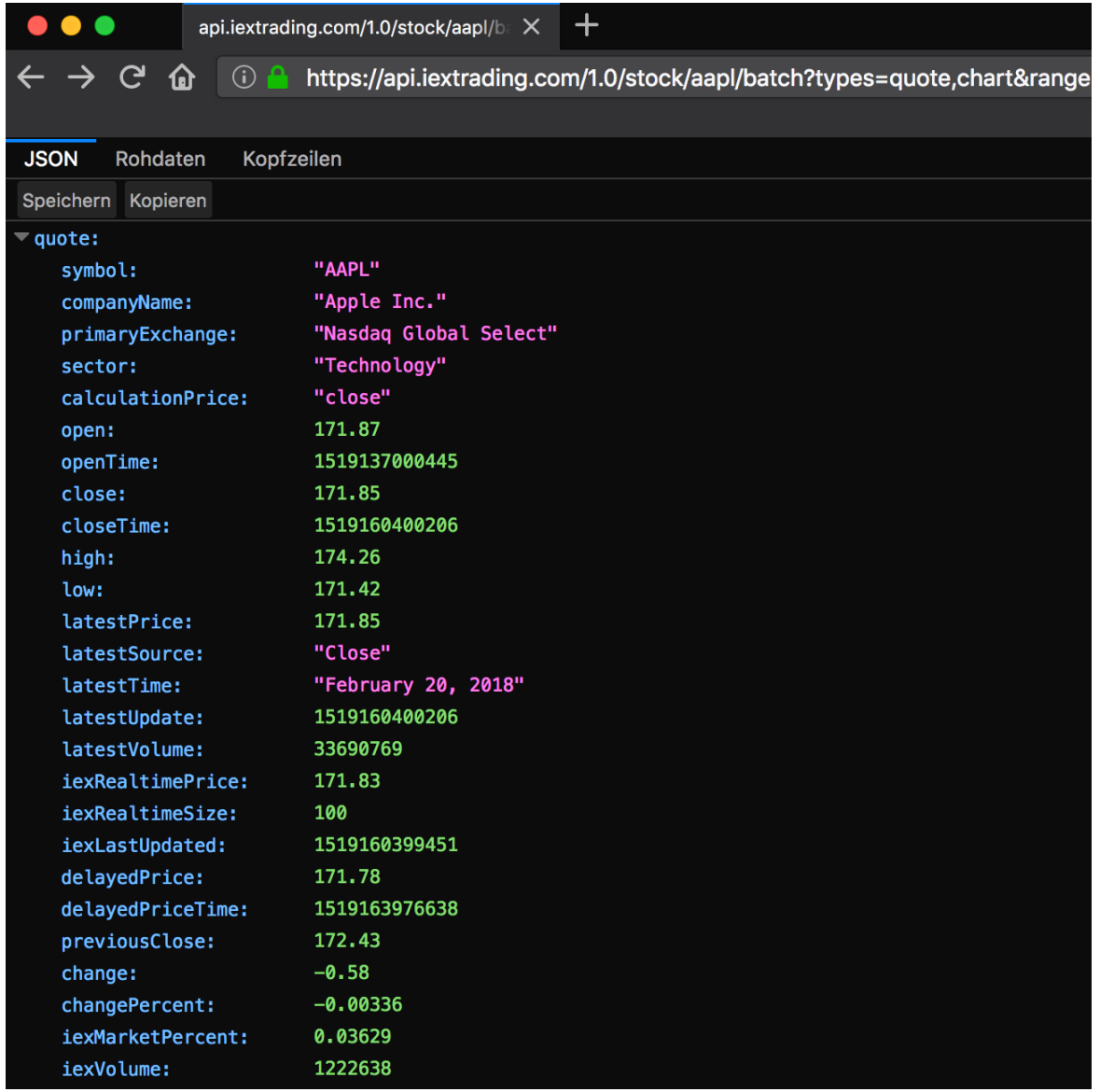
Daten aus Backups löschen ist technisch (fast) unmöglich!



# „Löschen – äääähhh, das geht nicht!“

merlin2 InfoDesign

Unstrukturierte Daten müssen ebenfalls „durchkämmt“ werden.



# Recht auf Vergessen werden – Eine Herausforderung für sich!

Off Topic…

merlin 2nd
InfoDesign

# Breach Notification

# Breach Notification

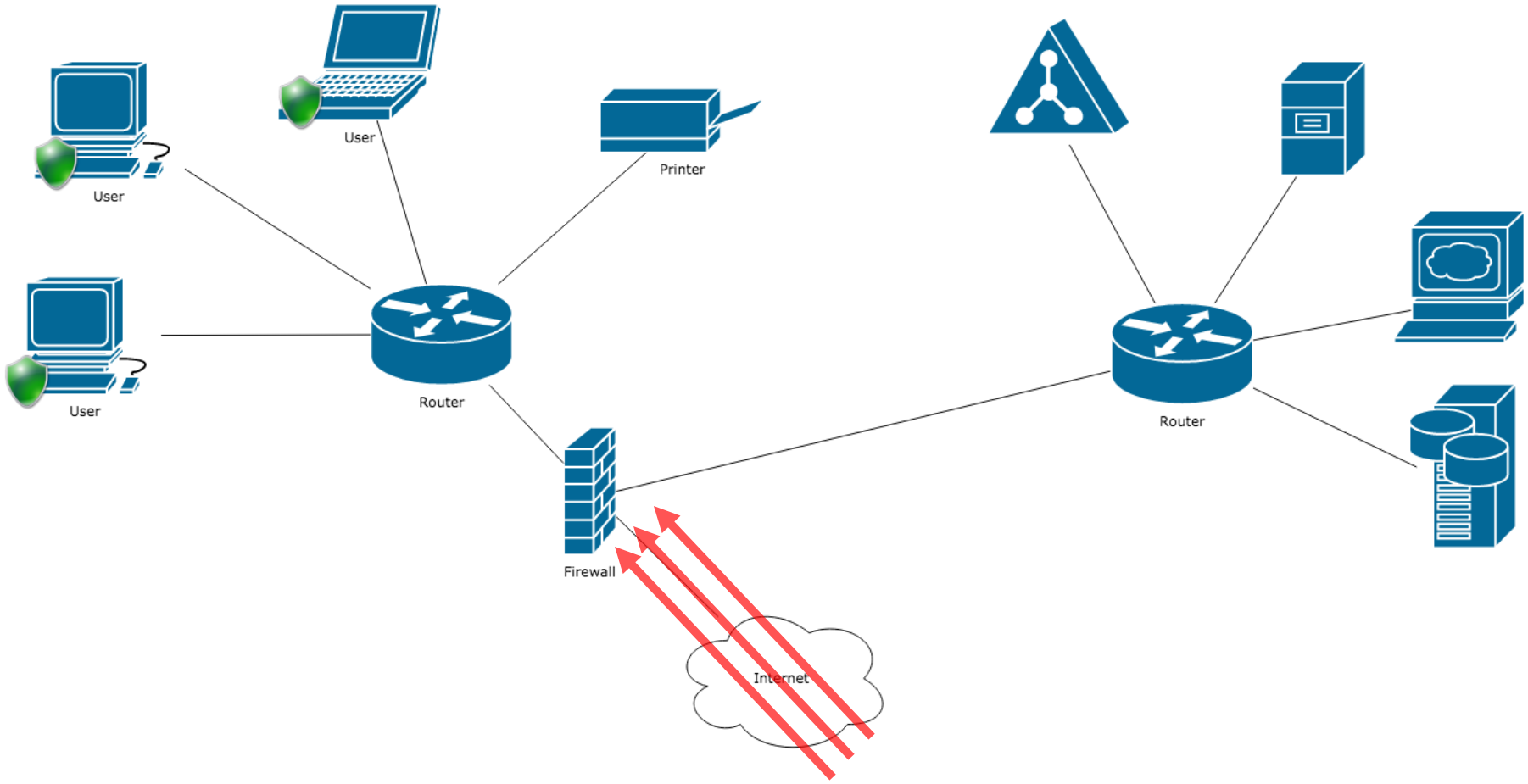
„There are only two types of companies: Those that have been hacked and those that will be hacked.“

Robert S. Mueller, Director FBI (damals)


„There are only two types of companies: Those that have been hacked and those that don’t know they have been hacked.“

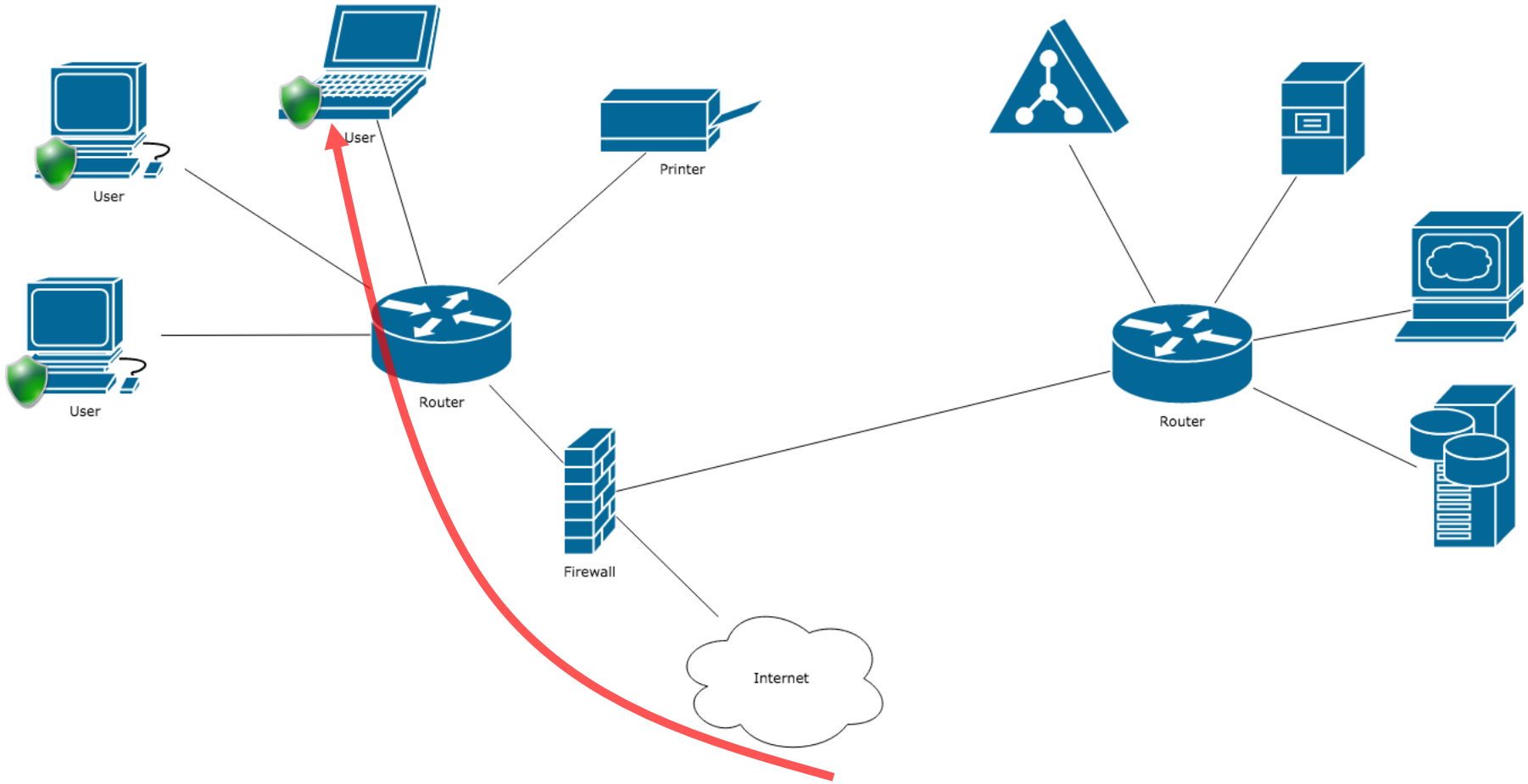
Stephen Barnes, Byron Vale Advisors

# Security Breach verteidigen



# Security Breach verteidigen

# Security Breach verteidigen



# Security Breach verteidigen – Betreff: Bitte dringend um Hilfe

Am 17.01.2018 um 12:25 schrieb F. xxxxxx:

Hallo Wxxxxx,

bitte ich will dass du eine Zahlungsverpflichtung für mich erledigst. welche Information brauchst du um eine Banküberweisung in Wert von 3.525 € vom Vereinskonto auszuführen? ich werde dir das Geld so schnell wie möglich zurückerstatten.

Ich warte auf deine Antwort

Gruß
Fxxxxx xxxxxxx

Von meinem iPhone gesendet

# Security Breach verteidigen – Betreff: Bitte dringend um Hilfe

From: Schatzmeister xxxxxx 17/1/2018 17:30:11 Subject: Re: Bitte dringend um Hilfe

hallo Fxxxxxx,
ich benötige Empfänger, IBAN, ( BIC falls verfügbar), natürlich den Betrag und Betreff.
Wir haben in Überweisungs-Limit vereinbart die genaue Höhe
weiß ich nicht aber dieser Betrag müsste durchgehen.
Schick die Daten vorbei und ich greife dann in die Tasten.
Gruß
Wxxxxxx

# Security Breach verteidigen – Betreff: Bitte dringend um Hilfe

-------- Weitergeleitete Nachricht --------
Betreff: Re: Bitte dringend um Hilfe
Datum: Wed, 17 Jan 2018 09:42:58 -0700
Von: Fxxxx xxxx <1vorsitzender@xxxx.de>
Antwort an: Fxxxx xxxx <1vorstand@inboxbear.com>
An: schatzmeister@xxxx.de

Ich werde mit der Rechnung kommen.

Empfänger
Konto Inhaber:Sule Kyeremeh
IBAN:ES2501828685650200044711
BIC:BBVAESMM
Verwendungszweck:RF/471927
Betrag:3.525 €

Ich werde auf deine E-mail mit der Überweisungsbestätigung warten weil ich der Begünstiger ein Zahlungsnachweis zeigen muss.

Gruß
Fxxxxxx xxxxxx

# Security Breach verteidigen – Betreff: Bitte dringend um Hilfe

-------- Weitergeleitete Nachricht --------
Betreff: Re: Bitte dringend um Hilfe
Datum: Wed, 17 Jan 2018 09:42:58 -0700
Von: Fxxxx xxxx <1vorsitzender@xxxx.de>
Antwort an: Fxxxx xxxx <1vorstand@inboxbear.com>
An: schatzmeister@xxxx.de

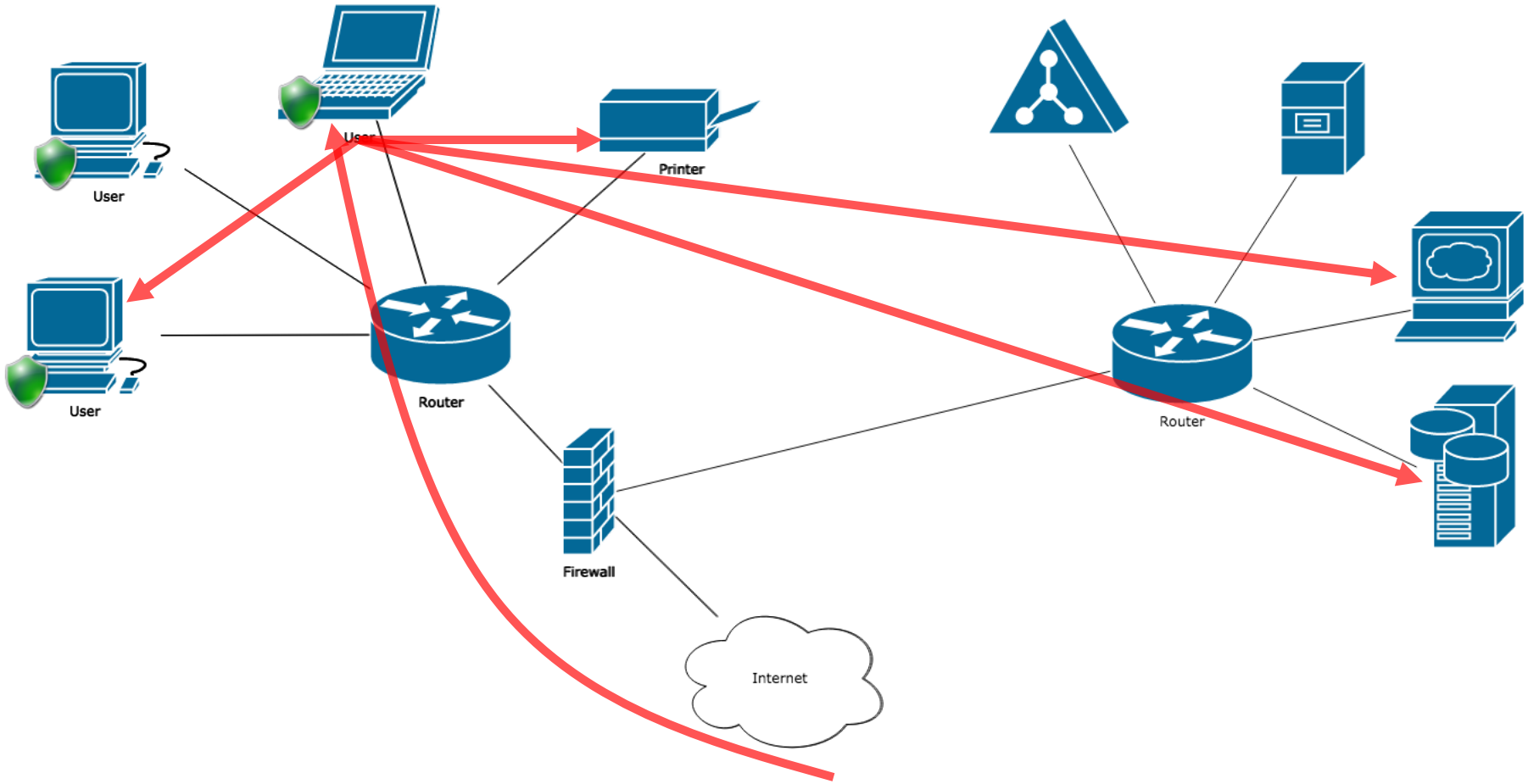
Ich werde mit der Rechnung kommen.

Empfänger
Konto Inhaber:Sule Kyeremeh
IBAN:ES2501828685650200044711
BIC:BBVAESMM
Verwendungszweck:RF/471927
Betrag:3.525 €

Ich werde auf deine E-mail mit der Überweisungsbestätigung warten weil ich der Begünstiger ein Zahlungsnachweis zeigen muss.

Gruß
Fxxxxxx xxxxxx

# Security Breach verteidigen



merlin2wo InfoDesign

# Logs

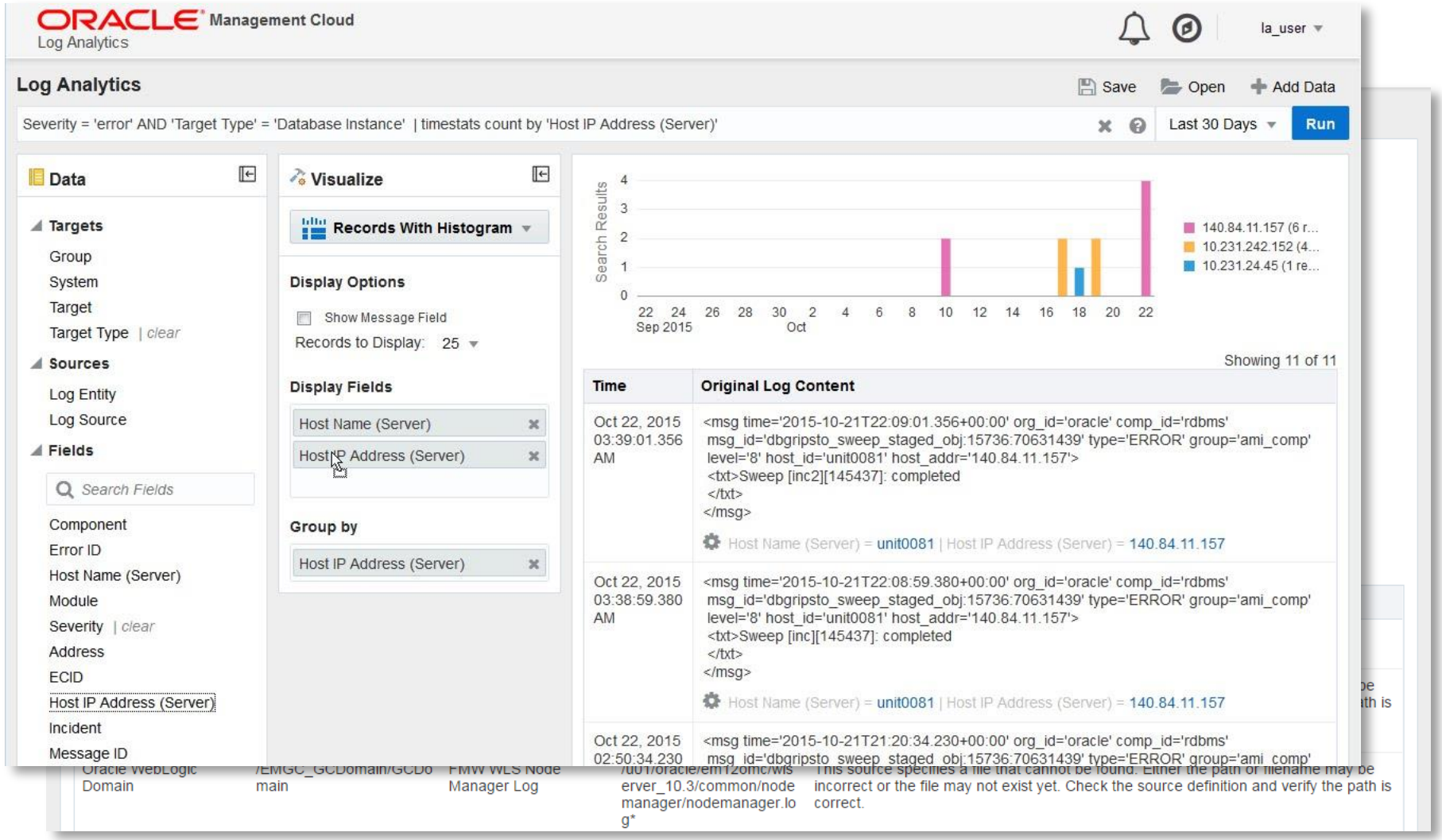
# Breach Notification – Lösungsansatz

„Die schlimmen Dinge passieren, wenn Sie gerade nicht hin schauen.“

(„The Bad Things Happen When You‘re Not Looking“)

Ryan Huber, Manager of Security Operations at Slack

# Breach Notification – Lösungsansatz



merlin2 InfoDesign


# Wiederherstellbarkeit und Verfügbarkeit

# Wiederherstellbarkeit und Verfügbarkeit

c) „die Fähigkeit, **die Verfügbarkeit** der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall **rasch wiederherzustellen**;

EU-DSGVO Art. 32 Abs. 1

# Wiederherstellbarkeit und Verfügbarkeit

„**Verfügbarkeit bedeutet, dass** Daten und **IT-Systeme zur Verfügung stehen** und von autorisierten Personen genutzt werden können, **wenn dies benötigt wird**. Eine unbefugte Unterbrechung z.B. durch Serverausfall oder Ausfall von Kommunikationsmitteln stellt einen Angriff auf die Verfügbarkeit dar.“

https://www.datenschutzbeauftragter-info.de/unterschiede-zwischen-datenschutz-datensicherheit-informationssicherheit-oder-it-sicherheit/

d) ein Verfahren zur **regelmäßigen Überprüfung**, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.“

EU-DSGVO Art. 32 Abs. 1

# Wiederherstellbarkeit und Verfügbarkeit – Beispiel

- SLA 2h

Betrachtung, Totalverlust des DB-Servers:

- Geschätzte Downtime: 3-4h

Feuerwehrübung:

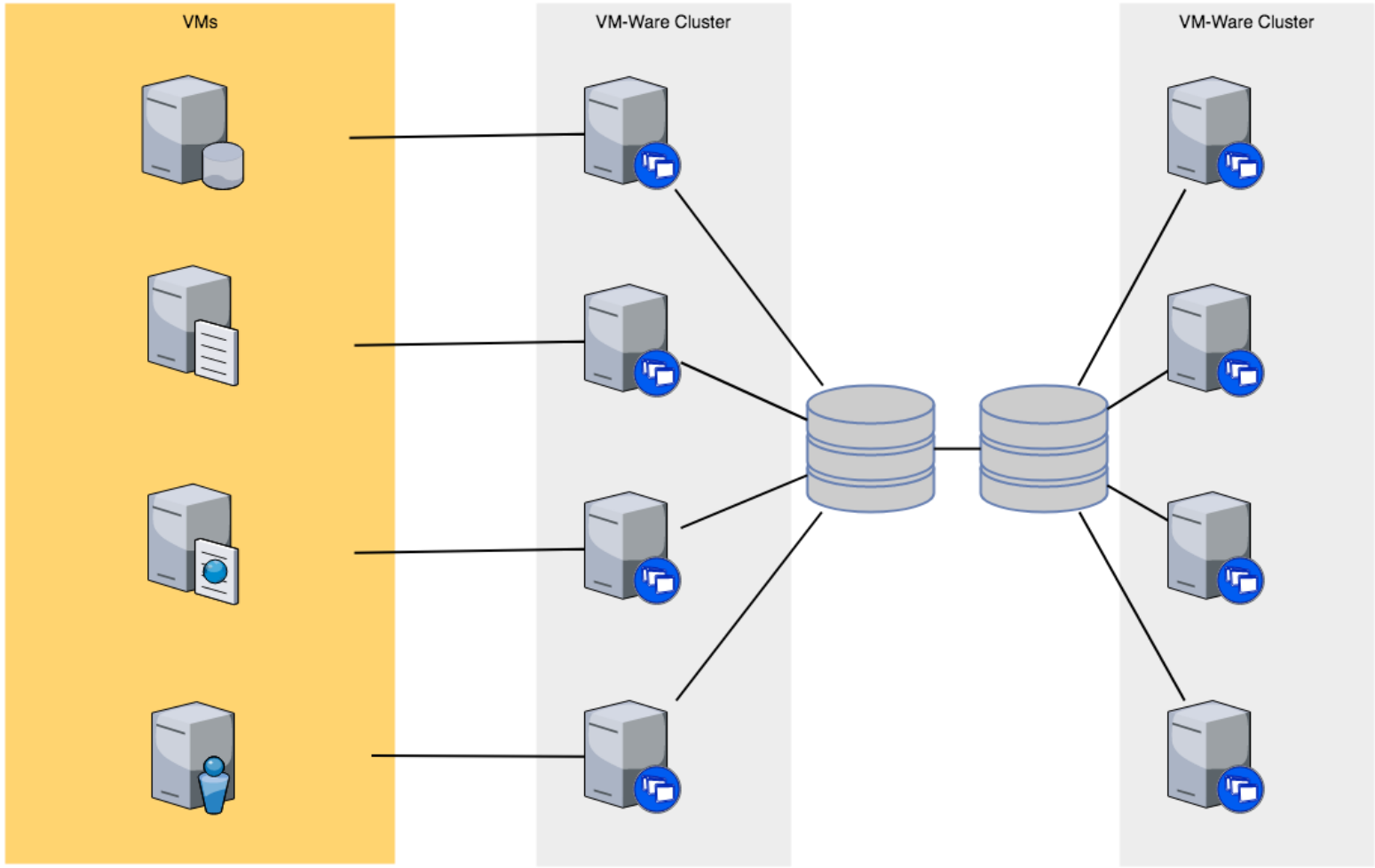
- Reine Rechenzeit: 12h
- Inkl. Arbeitszeit: 18h

Geschätzte Downtime im K-Fall:

- 24h

Vertragsstrafe bei diesem K-Fall:

- 6-Stelliger Betrag
- Vertrauen des Kunden verloren



# Wiederherstellbarkeit und Verfügbarkeit – Beispiel

- SLA 2h

Betrachtung, Totalverlust des DB-Servers:

- Geschätzte Downtime: 3-4h

Feuerwehrübung:

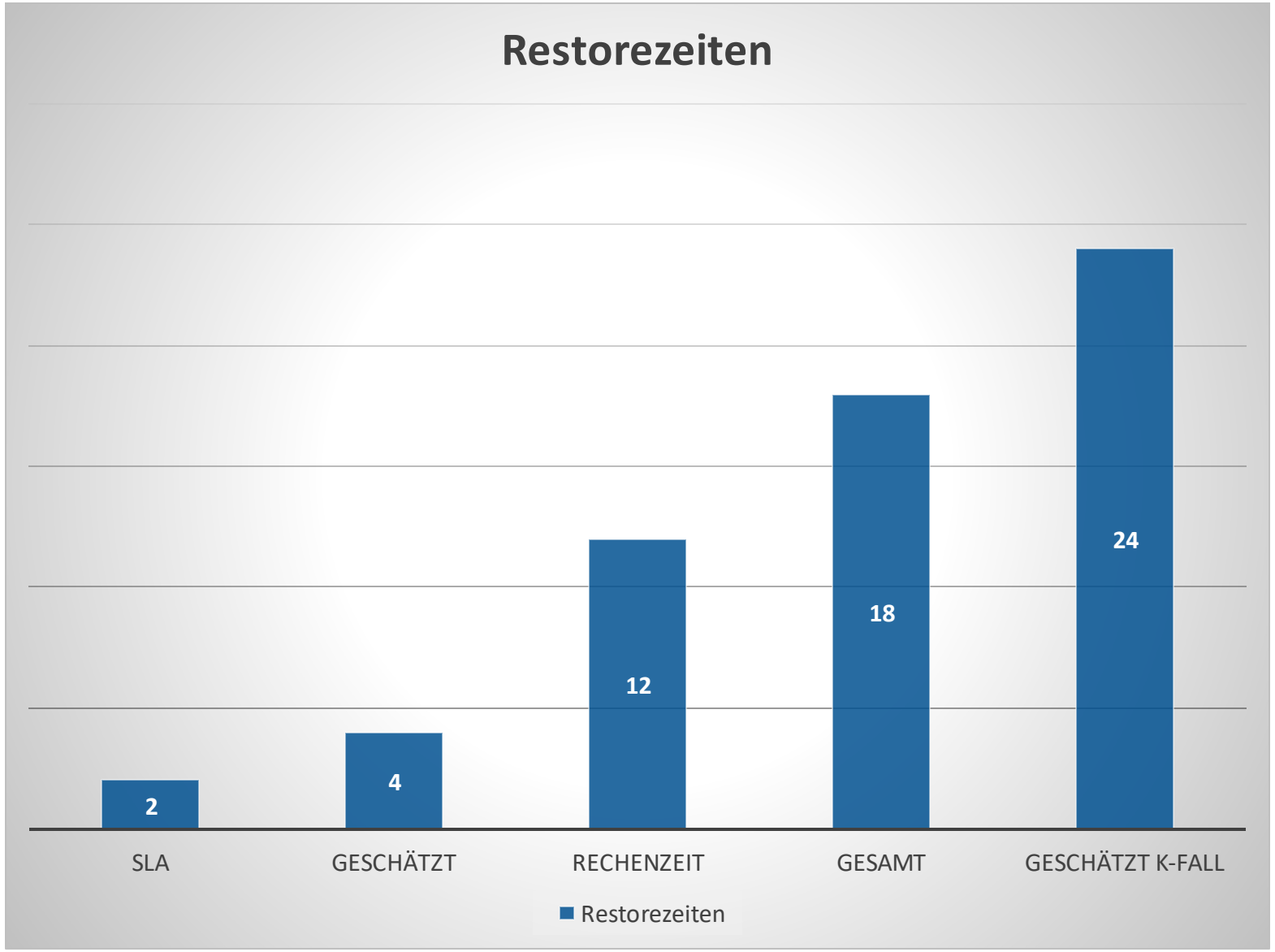
- Reine Rechenzeit: 12h
- Inkl. Arbeitszeit: 18h

Geschätzte Downtime im K-Fall:

- 24h

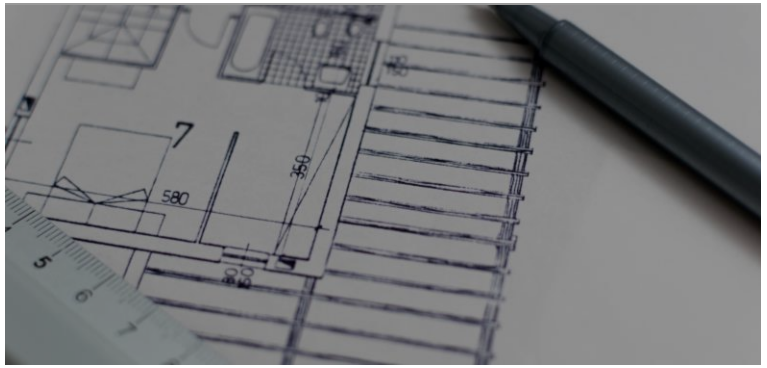
Vertragsstrafe bei diesem K-Fall:

- 6-Stelliger Betrag
- Vertrauen des Kunden verloren



# Persönliches Fazit zum Datenschutz

Stand der Technik



Data Protection by Design & Default

Zugangskontrolle

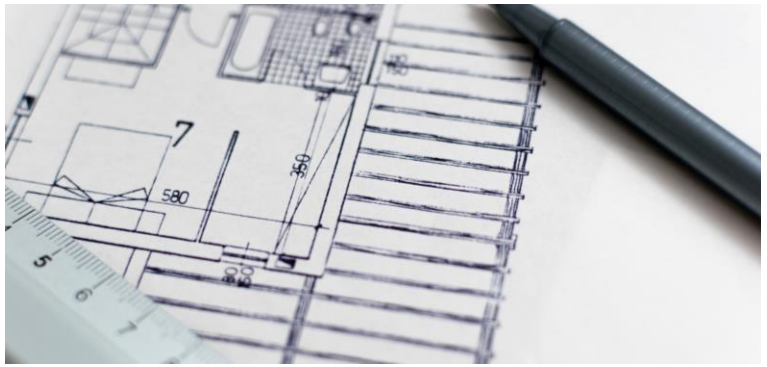
Recht auf Vergessenwerden

Breach Notification


Wiederherstellbarkeit & Verfügbarkeit

# Persönliches Fazit zum Datenschutz

Stand der Technik



Data Protection by Design & Default

Zugangskontrolle

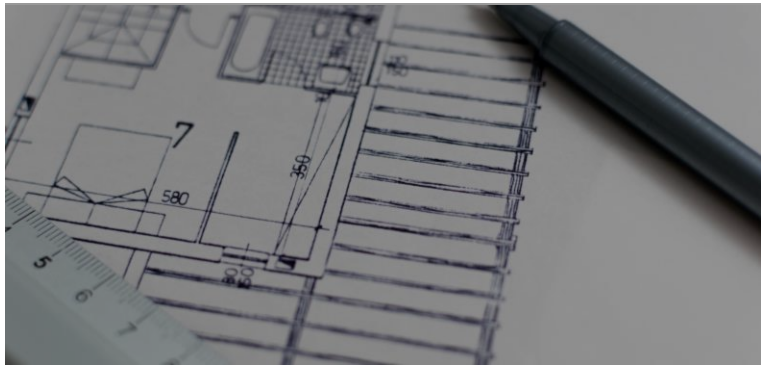
Recht auf Vergessenwerden

Breach Notification


Wiederherstellbarkeit & Verfügbarkeit

# Persönliches Fazit zum Datenschutz

Stand der Technik



Data Protection by Design & Default

Zugangskontrolle

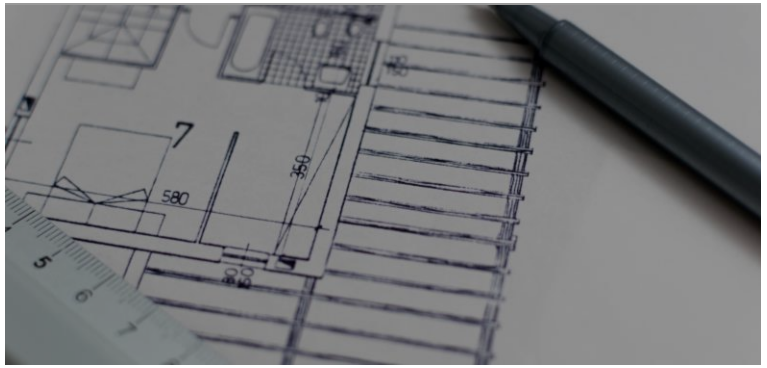
Recht auf Vergessenwerden

Breach Notification


Wiederherstellbarkeit & Verfügbarkeit

# Persönliches Fazit zum Datenschutz

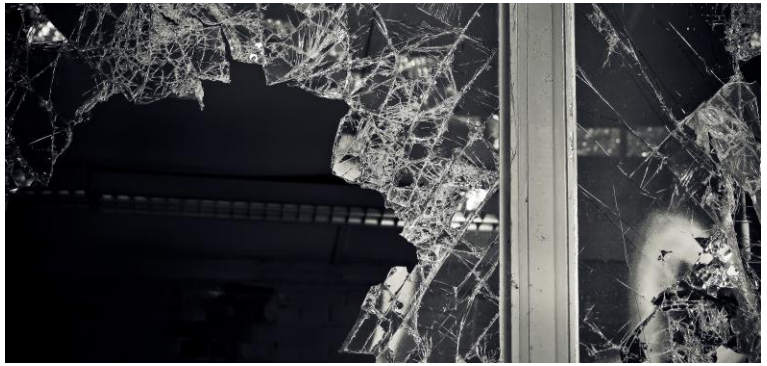
Stand der Technik



Data Protection by Design & Default

Zugangskontrolle

Recht auf Vergessenwerden



Breach Notification

Wiederherstellbarkeit & Verfügbarkeit


merlin.zwo InfoDesign GmbH & Co. KG
Daniel Nelle

# Fragen?

**merlin.zwo**
Wir kümmern uns!

**merlin.zwo InfoDesign GmbH & Co. KG**
**Daniel Nelle**

Elsa-Brändström-Straße 14
76228 Karlsruhe
Tel. 0721 – 132 096 0

Daniel.Nelle@merlin-zwo.de
http://www.merlin-zwo.de