

EU-DSGVO ab Mai 2018 – Lösungsansätze

Keine Angst, das beißt nicht!

Daniel Nelle

Senior Datenbank Admin und Security Spezialist

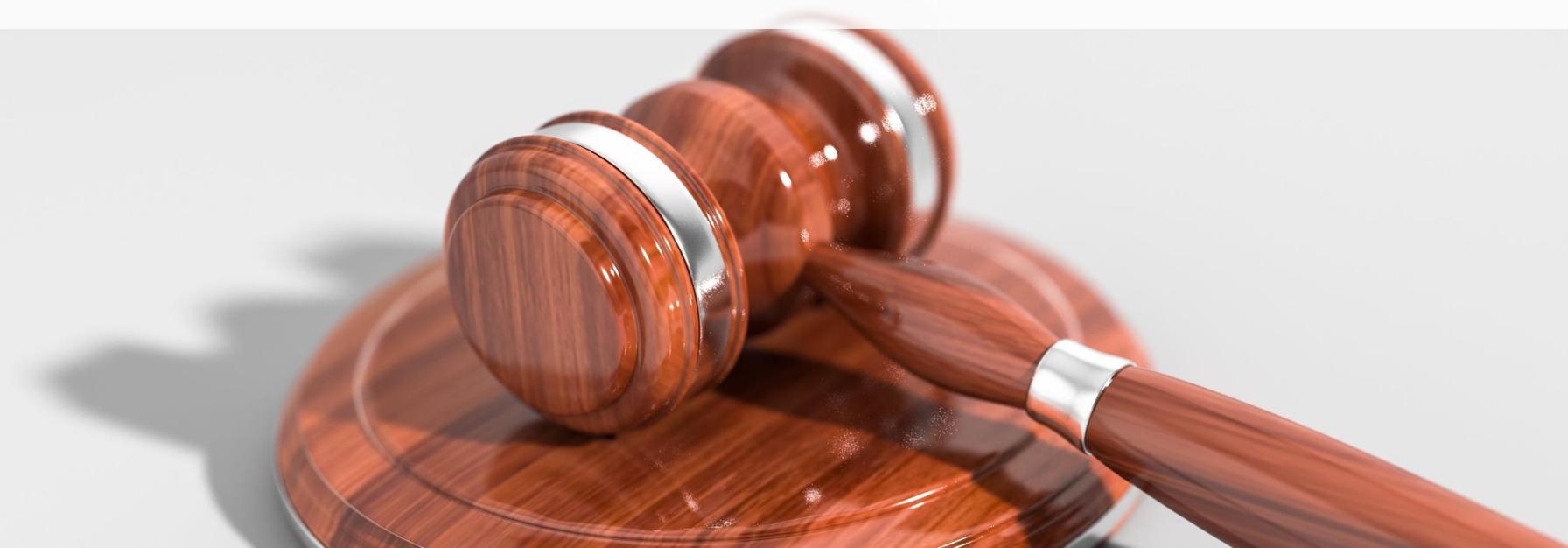
merlin.zwo InfoDesign GmbH & Co. KG

76228 Karlsruhe





EU-DSGVO, was Sie garantiert schon kennen!



77 Tage 11 Stunden 15 Minuten

(waren es bei Vortragsbeginn)

EU-DSGVO, was Sie garantiert schon wissen!



Relevant für Unternehmen weltweit.

Jedes Unternehmen braucht ein Datenschutz-Management-System



Informations- und Auskunftspflichten

EU-DSGVO, was Sie garantiert schon wissen!



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“

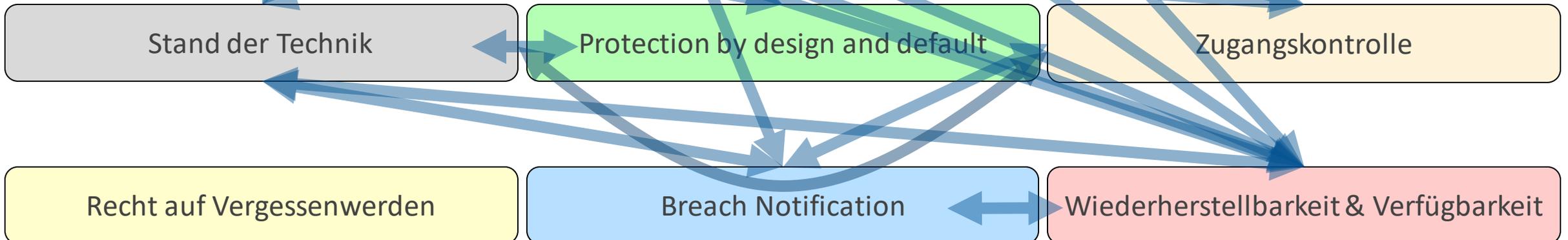
„(1) **Unter Berücksichtigung des Stands der Technik**, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die **Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche** 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 **Standes 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:

- die **Pseudonymisierung** und **Verschlüsselung** personenbezogener Daten;
- die Fähigkeit, die **Vertraulichkeit, Integrität, Verfügbarkeit** und **Belastbarkeit** der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- die Fähigkeit, die **Verfügbarkeit** der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall **rasch wiederherzustellen**;
- ein Verfahren zur **regelmäßigen Überprüfung**, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.“





Stand der Technik



Data Protection by Design & Default



Zugangskontrolle



Recht auf Vergessenwerden



Breach Notification



Wiederherstellbarkeit & Verfügbarkeit



Stand der Technik



Stand der Technik – Beispiel

- ~~WEP~~

- ~~WPA~~

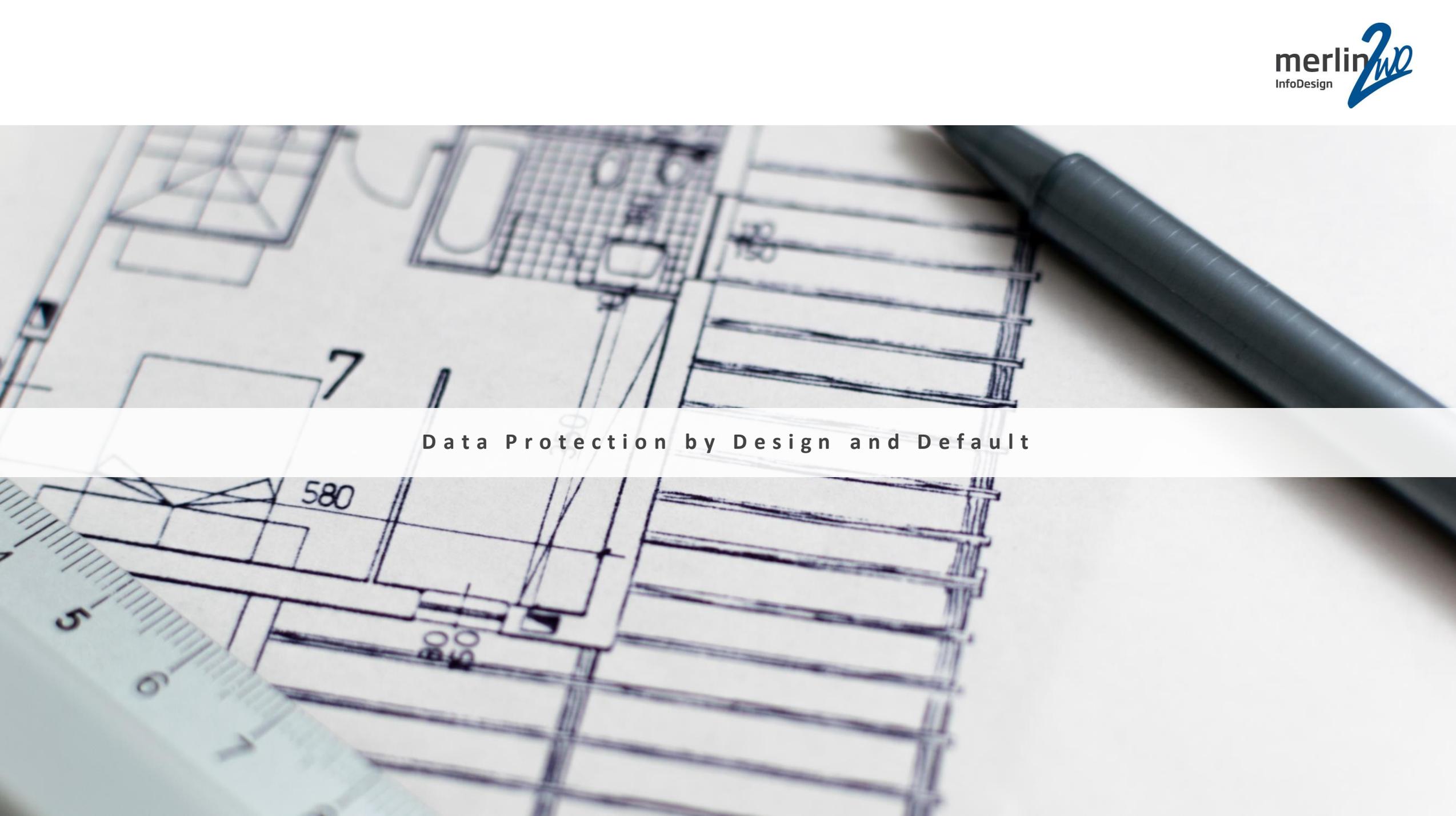
- WPA2

???
KRACK-Lücke von 10/2017

- WPA2 + VPN-Tunnel / SSL

- WPA2, 63-stelliger Key,
alle n -Tage neuer Key
+ VPN-Tunnel / SSL



A close-up photograph of an architectural drawing on a spiral-bound notebook. The drawing shows a floor plan with various rooms, walls, and furniture. A ruler is placed at the bottom left, and a pen lies diagonally across the top right. The drawing includes numerical labels such as '7', '580', '150', and '300'. The text 'Data Protection by Design and Default' is overlaid in the center of the image.

Data Protection by Design and Default



Was heißt das?



Der Aufwärm-Paragraph!



Was heißt das für die Praxis?



Zugangskontrolle



Physischer Zugang

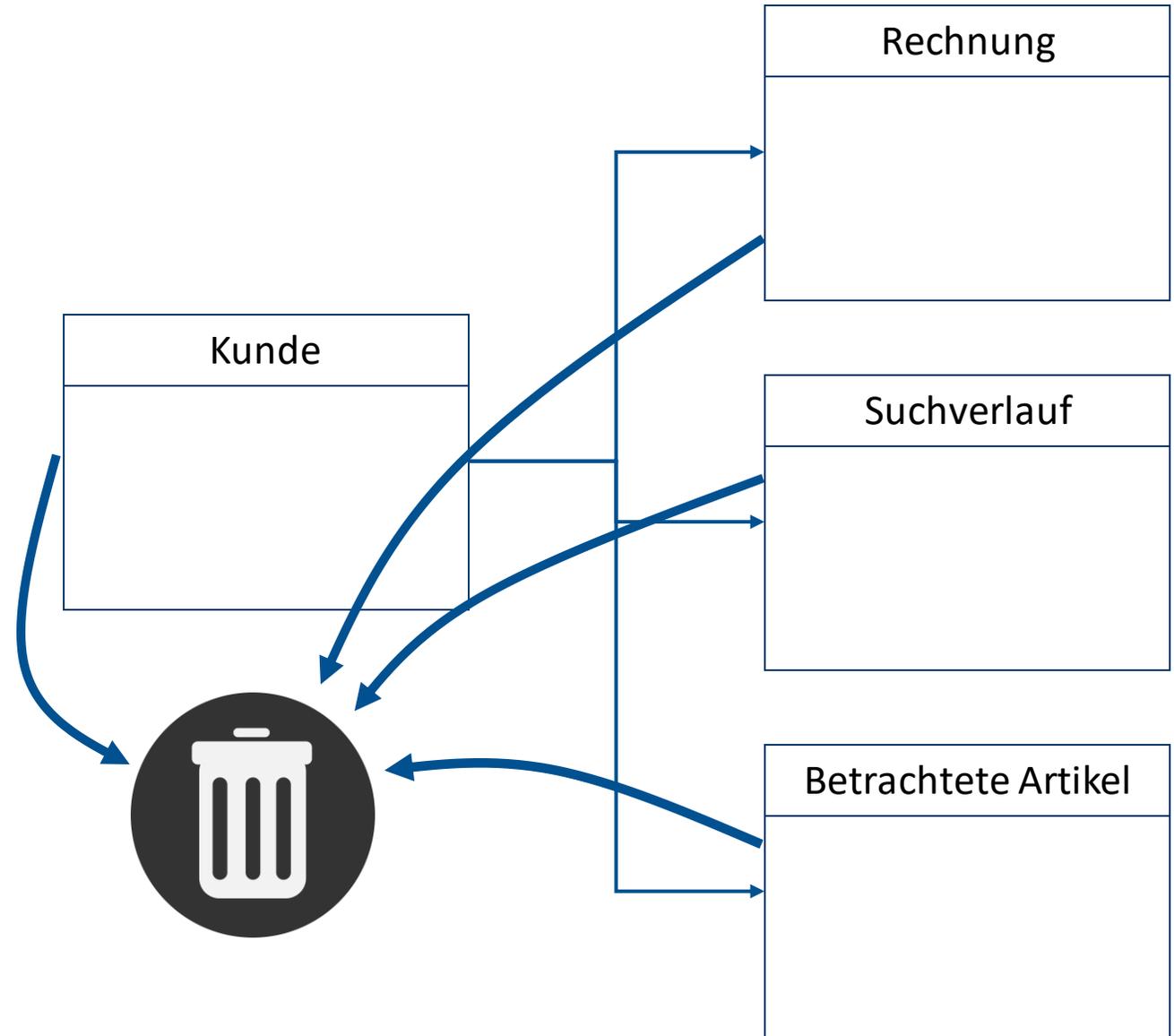


Elektronischer Zugang



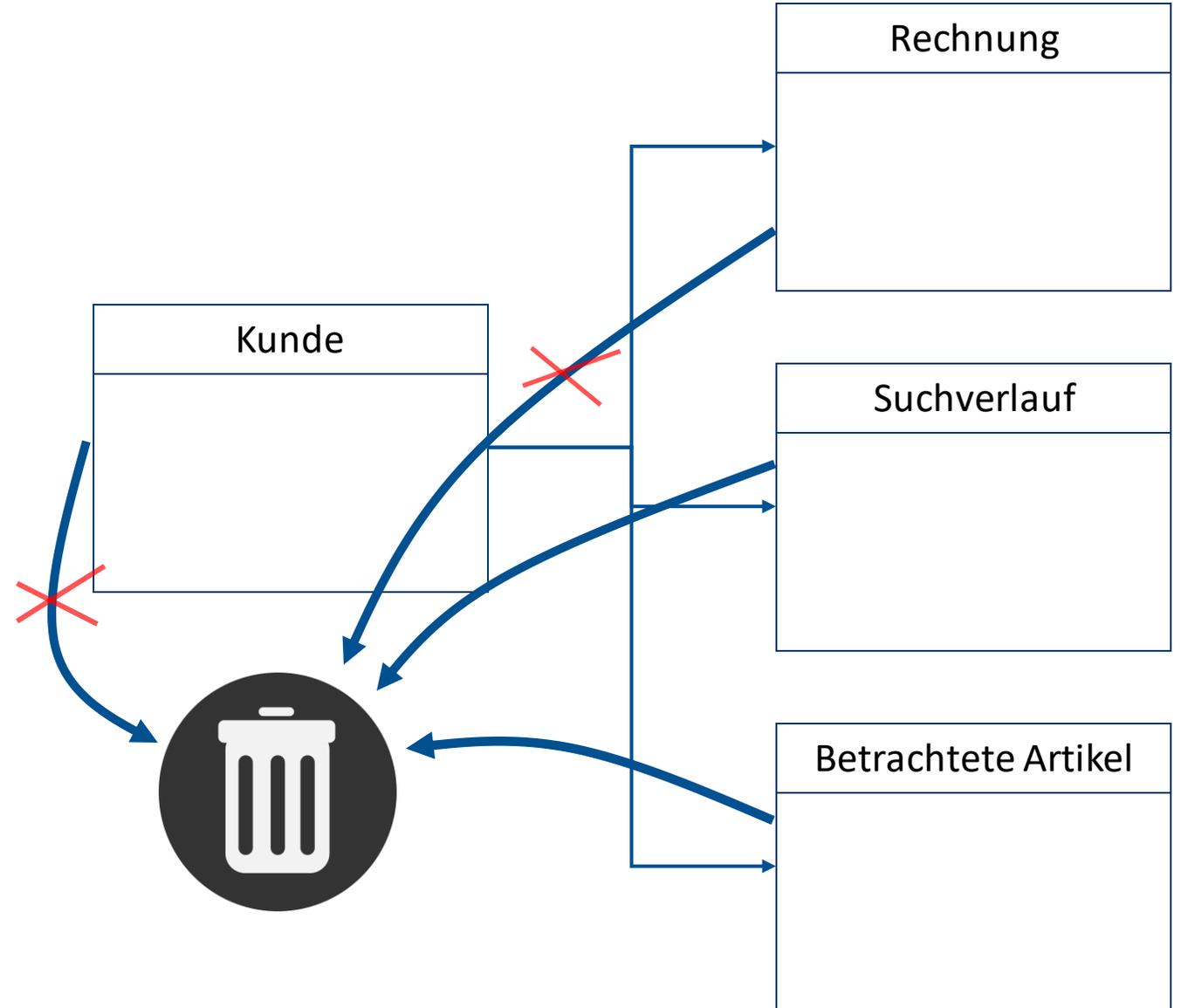
Recht auf Vergessenwerden

„Löschen – ääähhh, das geht nicht!“



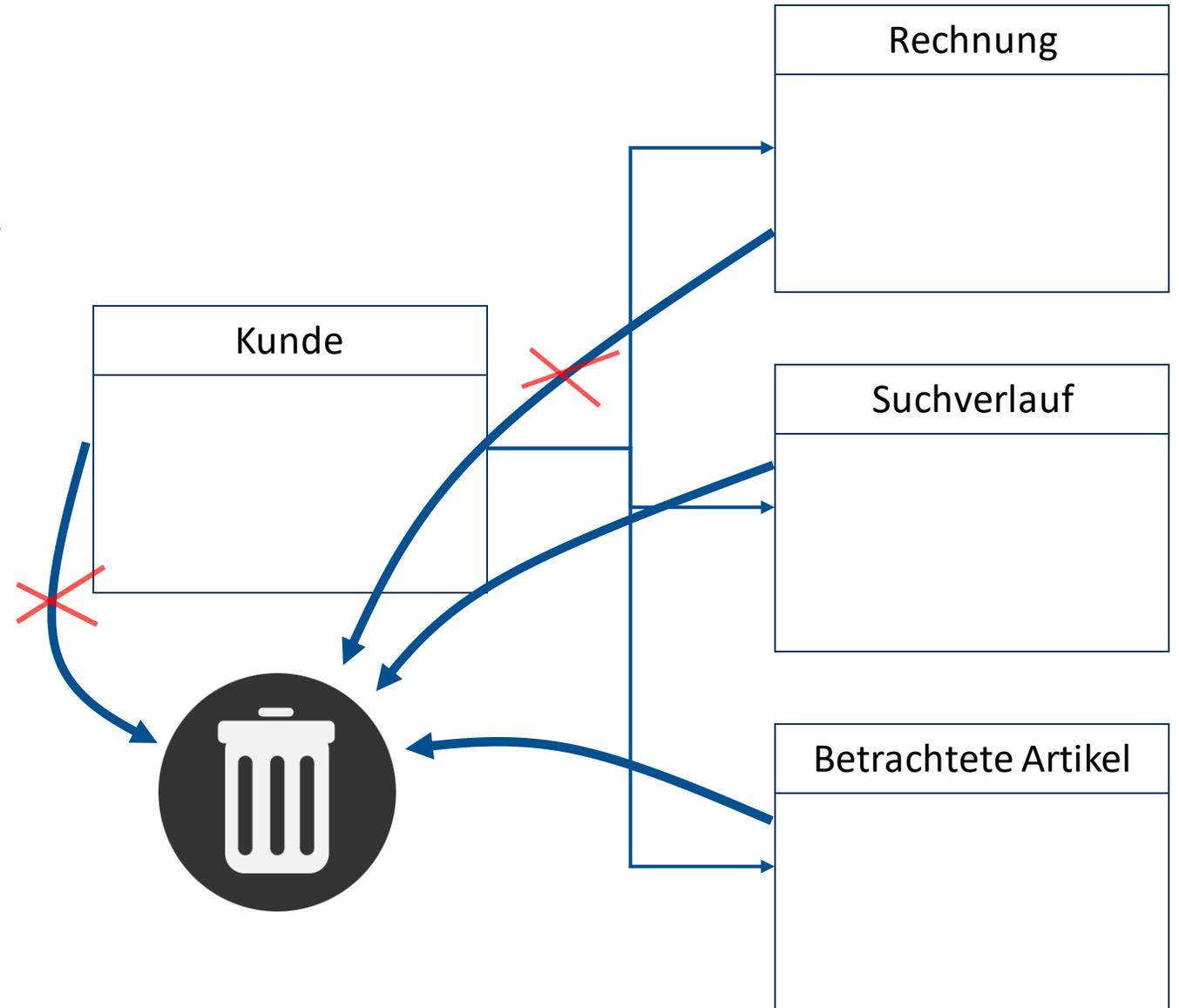
„Löschen – ääähhh, das geht nicht!“

Jeder Datensatz muss
einzeln betrachtet
werden!



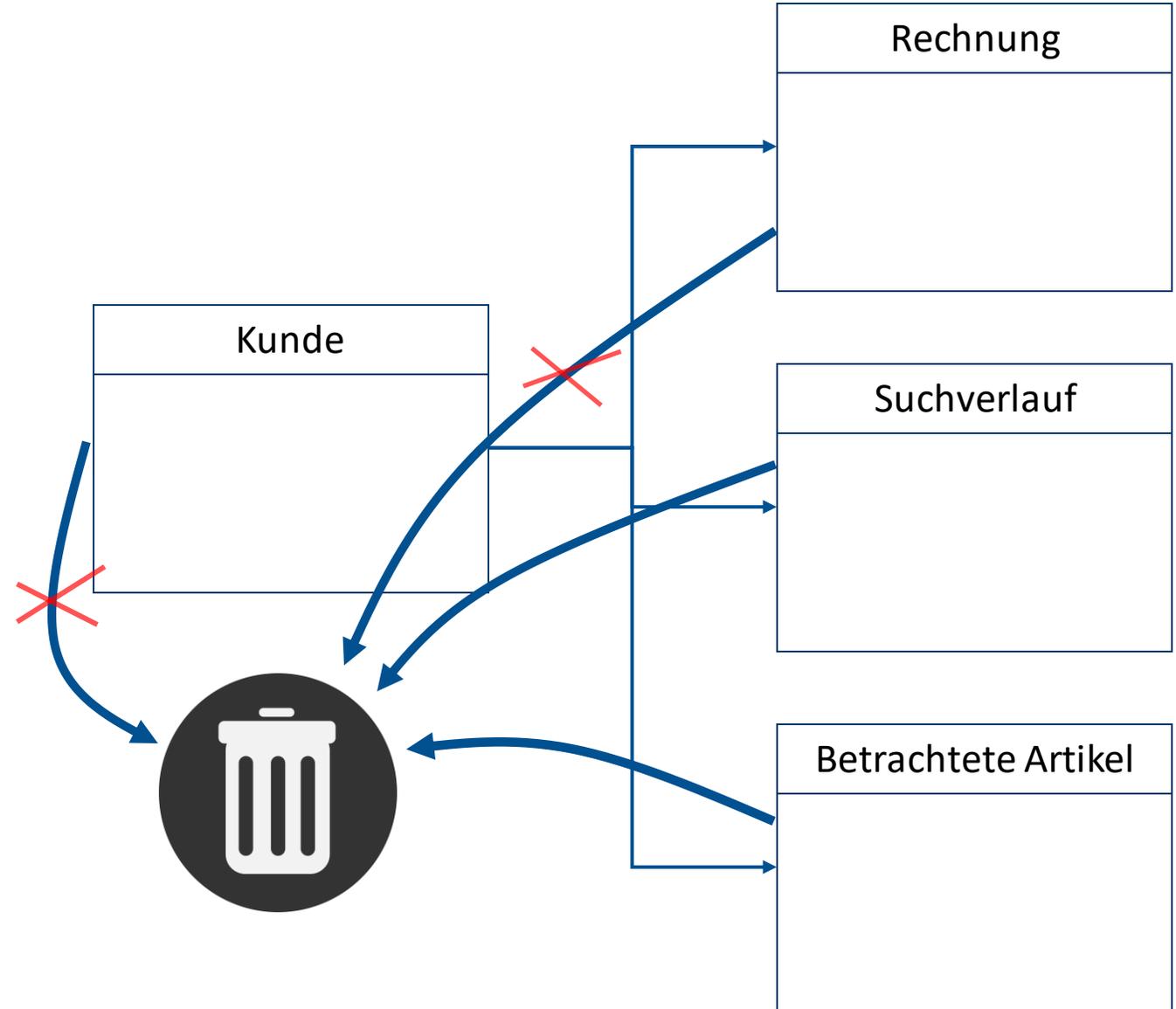
„Löschen – ääähhh, das geht nicht!“

~~Als gelöscht markieren~~



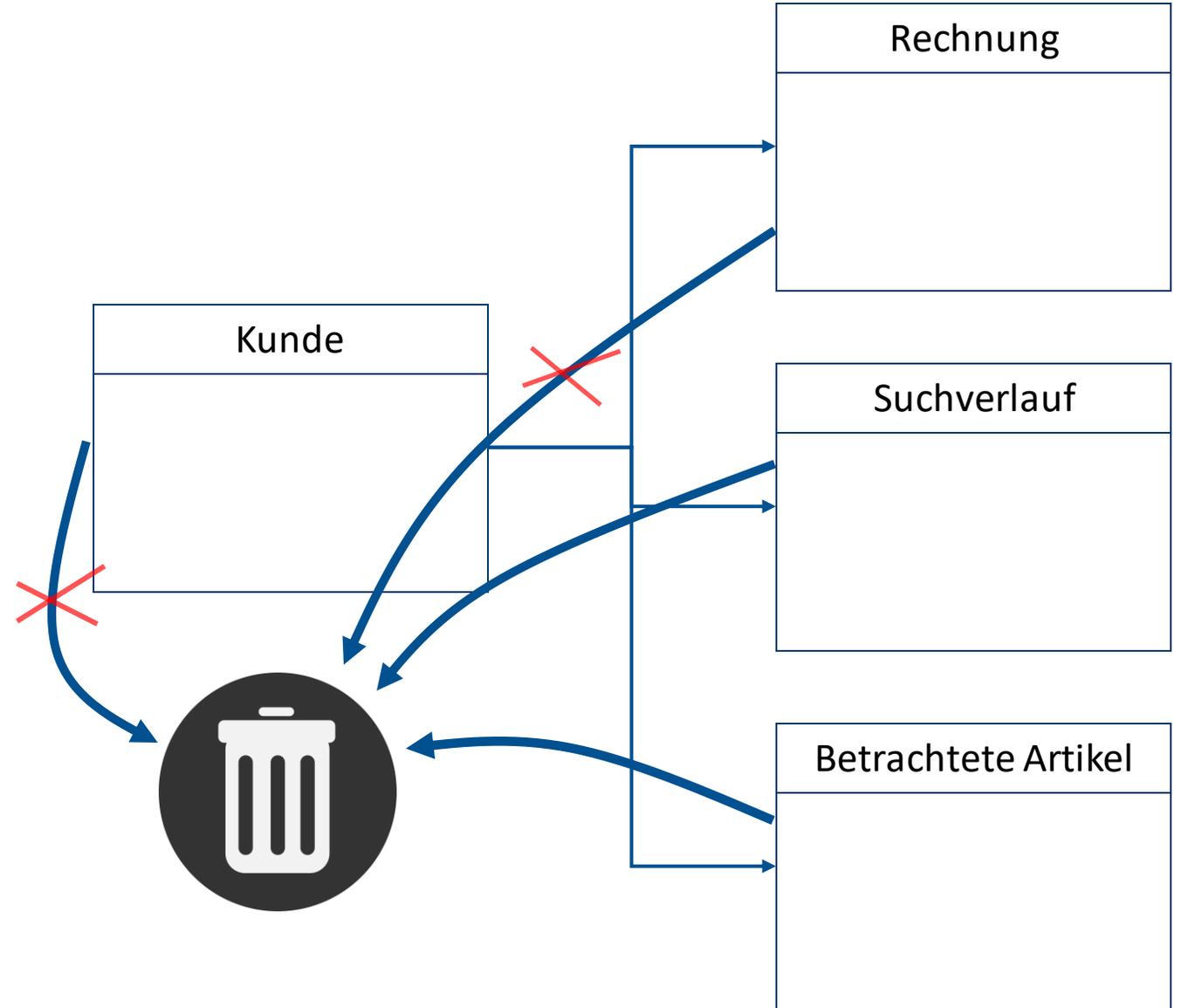
„Löschen – ääähhh, das geht nicht!“

**Nachvollziehbarkeit,
Erfüllung anderer
Gesetze!**



„Löschen – ääähhh, das geht nicht!“

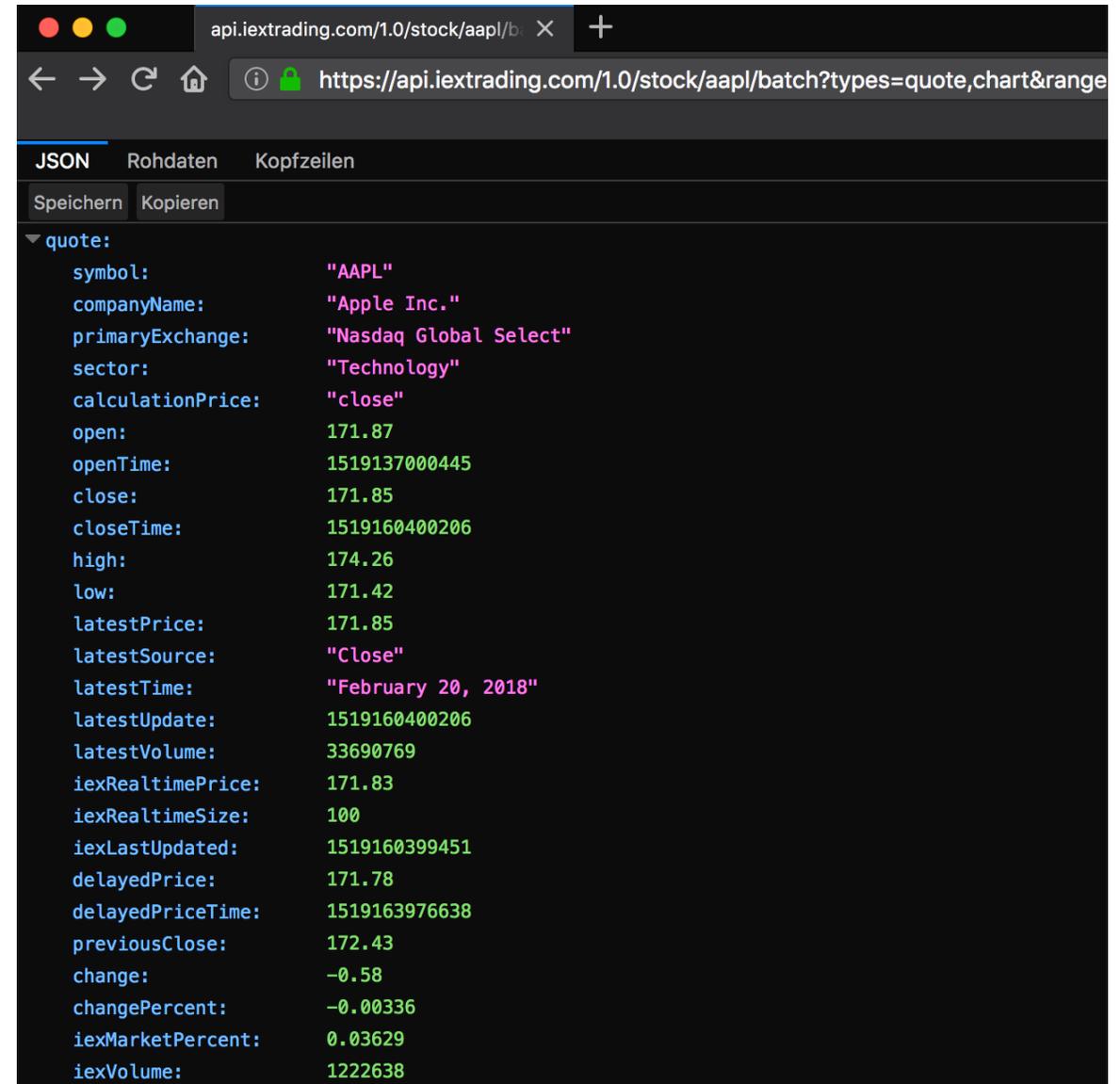
Daten aus Backups
löschen ist technisch
(fast) unmöglich!



„Löschen – ääähhh, das geht nicht!“



Unstrukturierte Daten
müssen ebenfalls
„durchkämmt“
werden.



```
api.iextrading.com/1.0/stock/aapl/b... X +
https://api.iextrading.com/1.0/stock/aapl/batch?types=quote,chart&range
JSON Rohdaten Kopfzeilen
Speichern Kopieren
quote:
  symbol: "AAPL"
  companyName: "Apple Inc."
  primaryExchange: "Nasdaq Global Select"
  sector: "Technology"
  calculationPrice: "close"
  open: 171.87
  openTime: 1519137000445
  close: 171.85
  closeTime: 1519160400206
  high: 174.26
  low: 171.42
  latestPrice: 171.85
  latestSource: "Close"
  latestTime: "February 20, 2018"
  latestUpdate: 1519160400206
  latestVolume: 33690769
  iexRealtimePrice: 171.83
  iexRealtimeSize: 100
  iexLastUpdated: 1519160399451
  delayedPrice: 171.78
  delayedPriceTime: 1519163976638
  previousClose: 172.43
  change: -0.58
  changePercent: -0.00336
  iexMarketPercent: 0.03629
  iexVolume: 1222638
```

Recht auf Vergessen werden – Eine Herausforderung für sich!

Off Topic...





Breach Notification



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

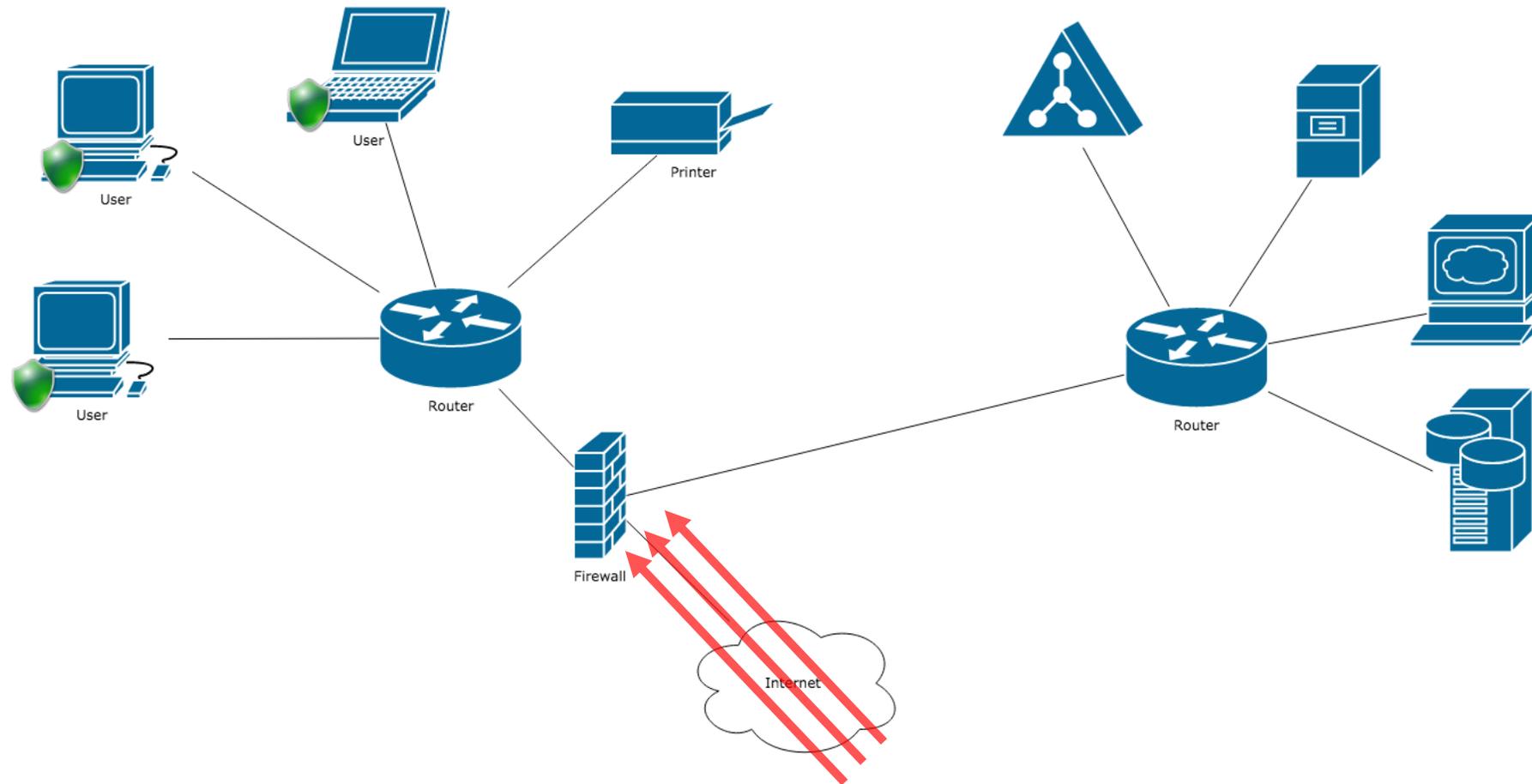
Robert S. Mueller, Director FBI (damals)



„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

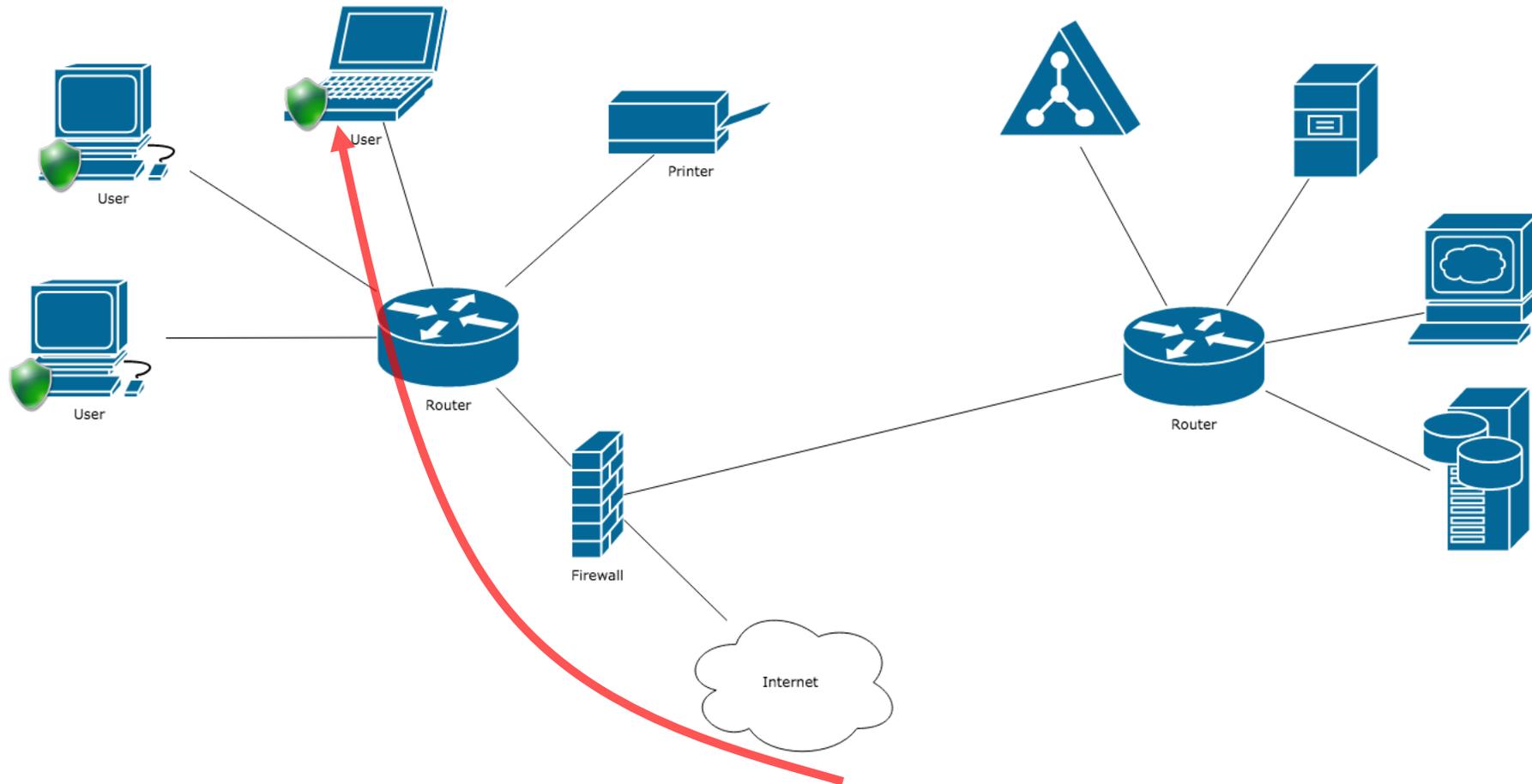
Security Breach verteidigen





BIRGIT KINDER
VI. 1990
IX. 1996
IX. 1998
V. 2000
VII. 2009

Security Breach verteidigen



Security Breach verteidigen – Betreff: Bitte dringend um Hilfe



Am 17.01.2018 um 12:25 schrieb F. xxxxxxx:

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

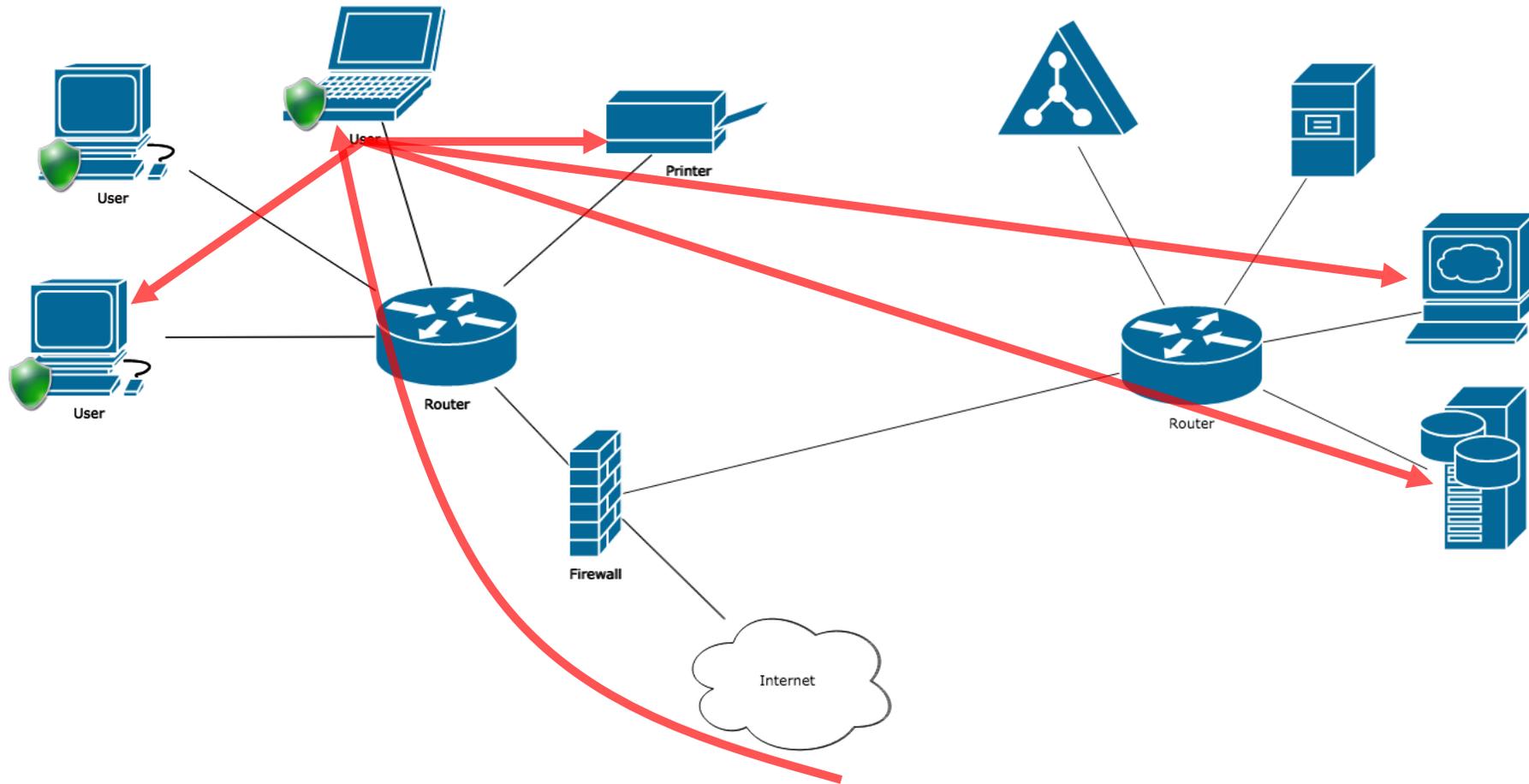
Betrag:3.525 €

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

Gruß

Fxxxxxx xxxxxx

Security Breach verteidigen

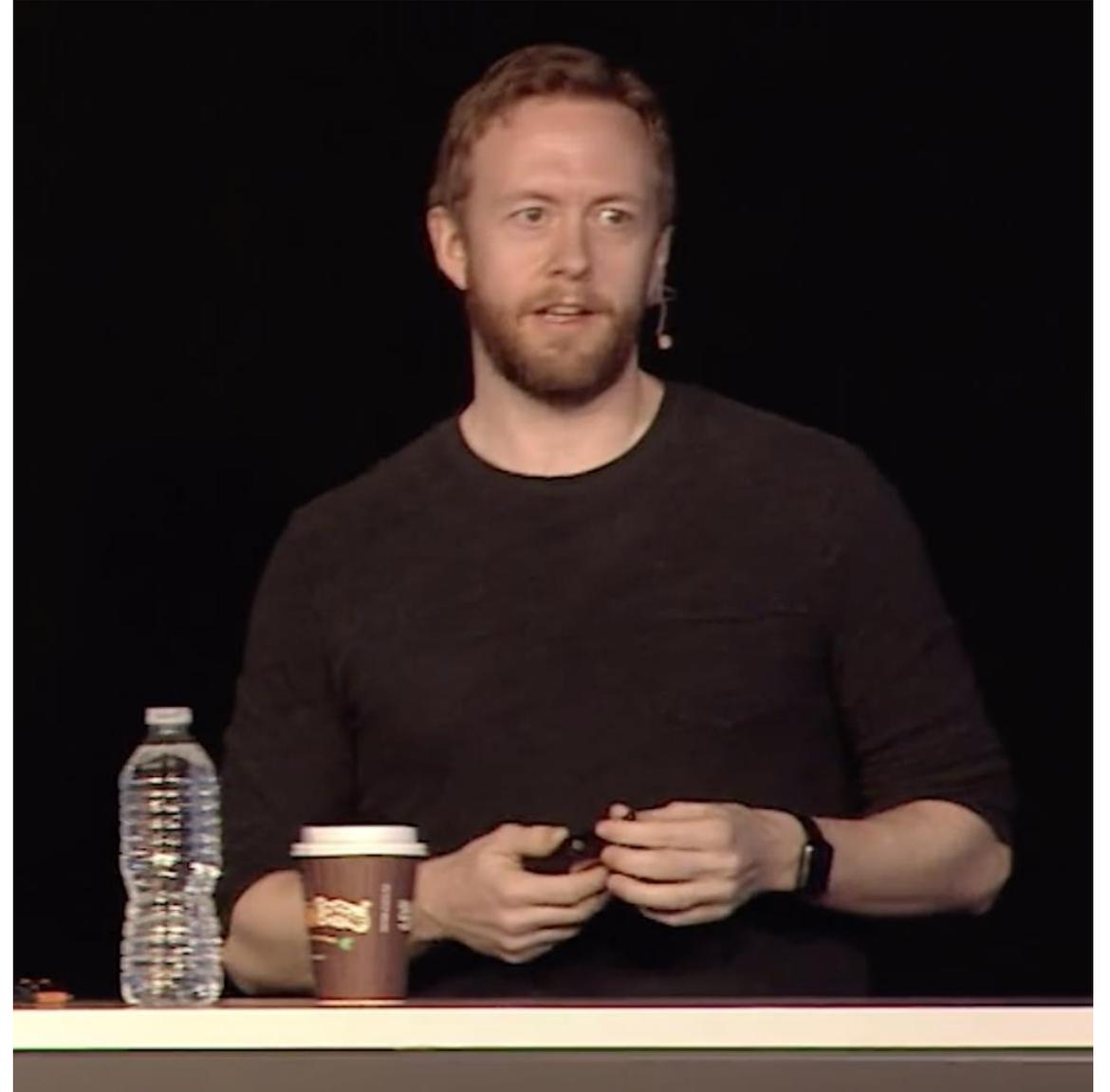


Logs

„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

ORACLE Management Cloud
Log Analytics

Log Analytics Save Open Add Data

Severity = 'error' AND 'Target Type' = 'Database Instance' | timestats count by 'Host IP Address (Server)' Last 30 Days Run

Data

Targets

- Group
- System
- Target
- Target Type | clear

Sources

- Log Entity
- Log Source

Fields

Search Fields

- Component
- Error ID
- Host Name (Server)
- Module
- Severity | clear
- Address
- ECID
- Host IP Address (Server)**
- Incident
- Message ID

Visualize

Records With Histogram

Display Options

Show Message Field

Records to Display: 25

Display Fields

- Host Name (Server)
- Host IP Address (Server)

Group by

- Host IP Address (Server)

Showing 11 of 11

Time	Original Log Content
Oct 22, 2015 03:39:01.356 AM	<pre><msg time='2015-10-21T22:09:01.356+00:00' org_id='oracle' comp_id='rdbms' msg_id='dbgripsto_sweep_staged_obj:15736:70631439' type='ERROR' group='ami_comp' level='8' host_id='unit0081' host_addr='140.84.11.157'> <txt>Sweep [inc2][145437]: completed </txt> </msg></pre> <p>Host Name (Server) = unit0081 Host IP Address (Server) = 140.84.11.157</p>
Oct 22, 2015 03:38:59.380 AM	<pre><msg time='2015-10-21T22:08:59.380+00:00' org_id='oracle' comp_id='rdbms' msg_id='dbgripsto_sweep_staged_obj:15736:70631439' type='ERROR' group='ami_comp' level='8' host_id='unit0081' host_addr='140.84.11.157'> <txt>Sweep [inc][145437]: completed </txt> </msg></pre> <p>Host Name (Server) = unit0081 Host IP Address (Server) = 140.84.11.157</p>
Oct 22, 2015 02:50:34.230 AM	<pre><msg time='2015-10-21T21:20:34.230+00:00' org_id='oracle' comp_id='rdbms' msg_id='dbgripsto_sweep_staged_obj:15736:70631439' type='ERROR' group='ami_comp' level='8' host_id='unit0081' host_addr='140.84.11.157'> <txt>This source specifies a file that cannot be found. Either the path or filename may be incorrect or the file may not exist yet. Check the source definition and verify the path is correct. </txt> </msg></pre>



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

„**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

Feuerwehrrübung:

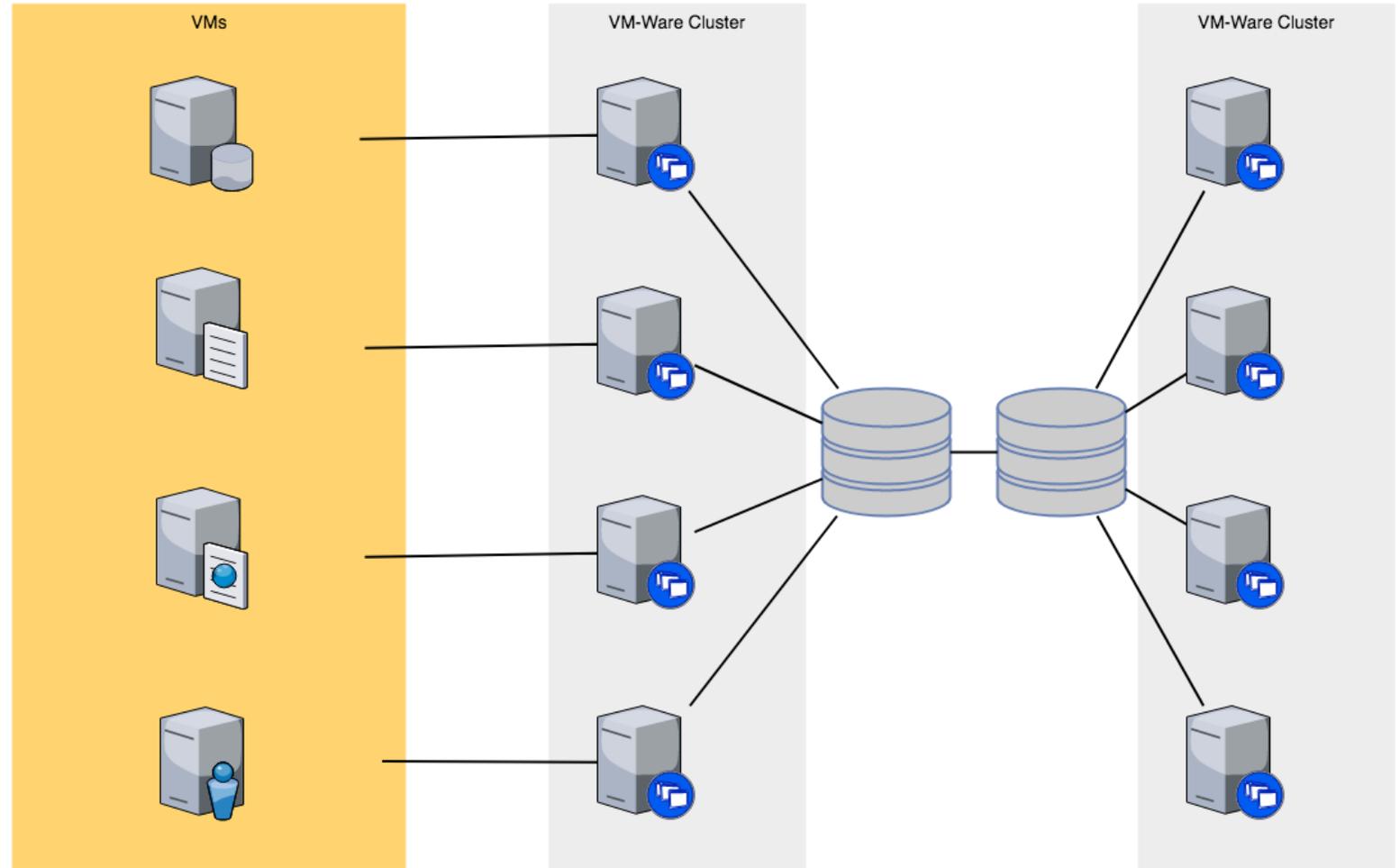
- Reine Rechenzeit: 12h
- Inkl. Arbeitszeit: 18h

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

Feuerwehrrübung:

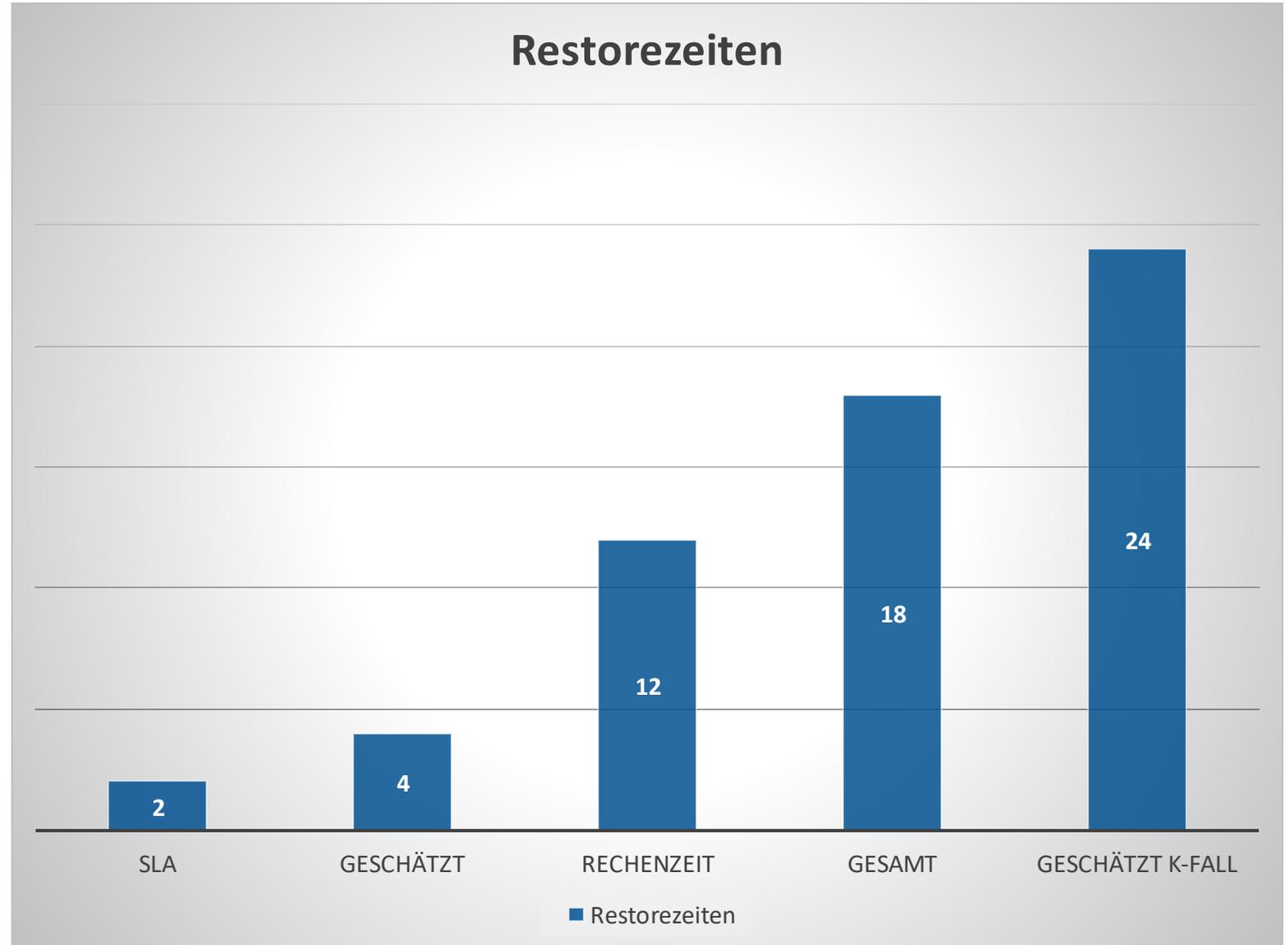
- Reine Rechenzeit: 12h
- Inkl. Arbeitszeit: 18h

Geschätzte Downtime im K-Fall:

- 24h

Vertragsstrafe bei diesem K-Fall:

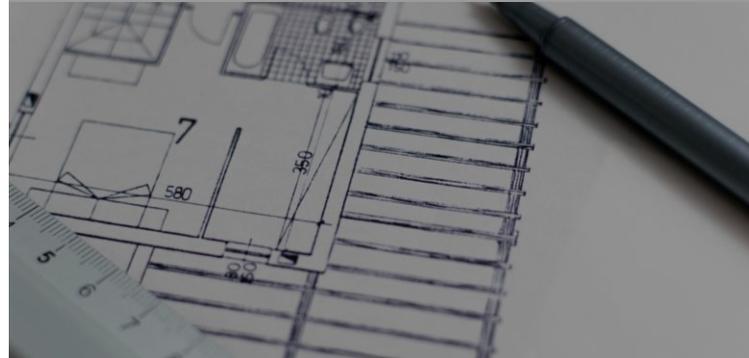
- 6-Stelliger Betrag
- Vertrauen des Kunden verloren



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

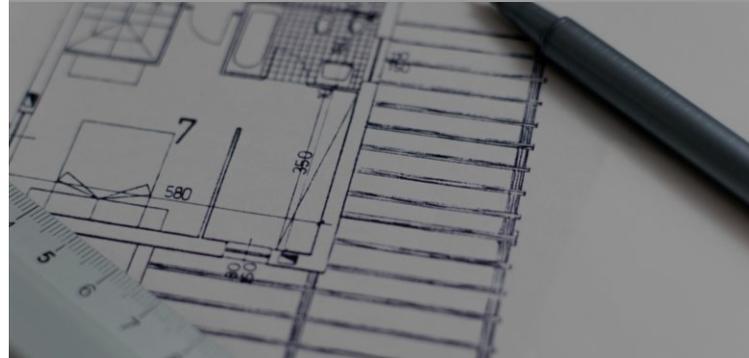


Wiederherstellbarkeit & Verfügbarkeit

Persönliches Fazit zum Datenschutz



Stand der Technik



Data Protection by Design & Default



Zugangskontrolle



Recht auf Vergessenwerden



Breach Notification

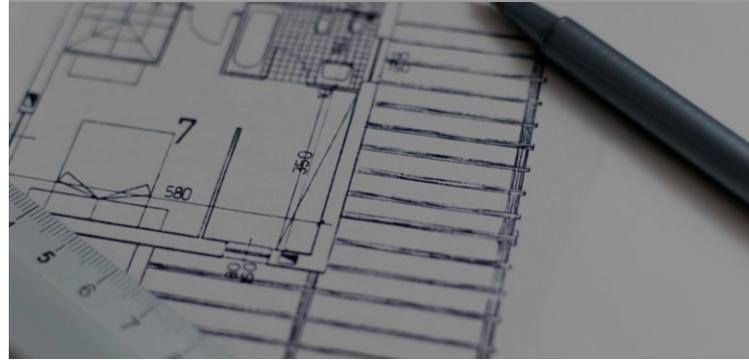


Wiederherstellbarkeit & Verfügbarkeit

Persönliches Fazit zum Datenschutz



Stand der Technik



Data Protection by Design & Default



Zugangskontrolle



Recht auf Vergessenwerden



Breach Notification



Wiederherstellbarkeit & Verfügbarkeit



Frenetischer Jubel... JETZT!

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>

