



# Datenschutz 2023

## Information für die Mandatsträger der Stadt Erbach im Odenwald

Maurice Quirin, LL.M.

Zertifizierter Datenschutzbeauftragter und Datenschutz-Auditor

Jurist, Certified Compliance Professional (CCP)

Certified Lead Auditor IT Sicherheitsmanagementsysteme (ISO 27001)

# Wer wir sind?

- Datenschutzberatung, Zertifizierungs- und Normen-Beratung
- Gegründet zum 01.01.2019 als GmbH
- Hauptsitz in Mainz am Rhein
- Fokus auf
  - kleine und mittelständische Unternehmen, sowie Gemeinden und Kommunen
  - Einführung und Zertifizierung der wichtigsten Managementsysteme

**Wir wollen unsere Kunden erfolgreicher machen!**

**Dazu denken wir einen Schritt weiter!**





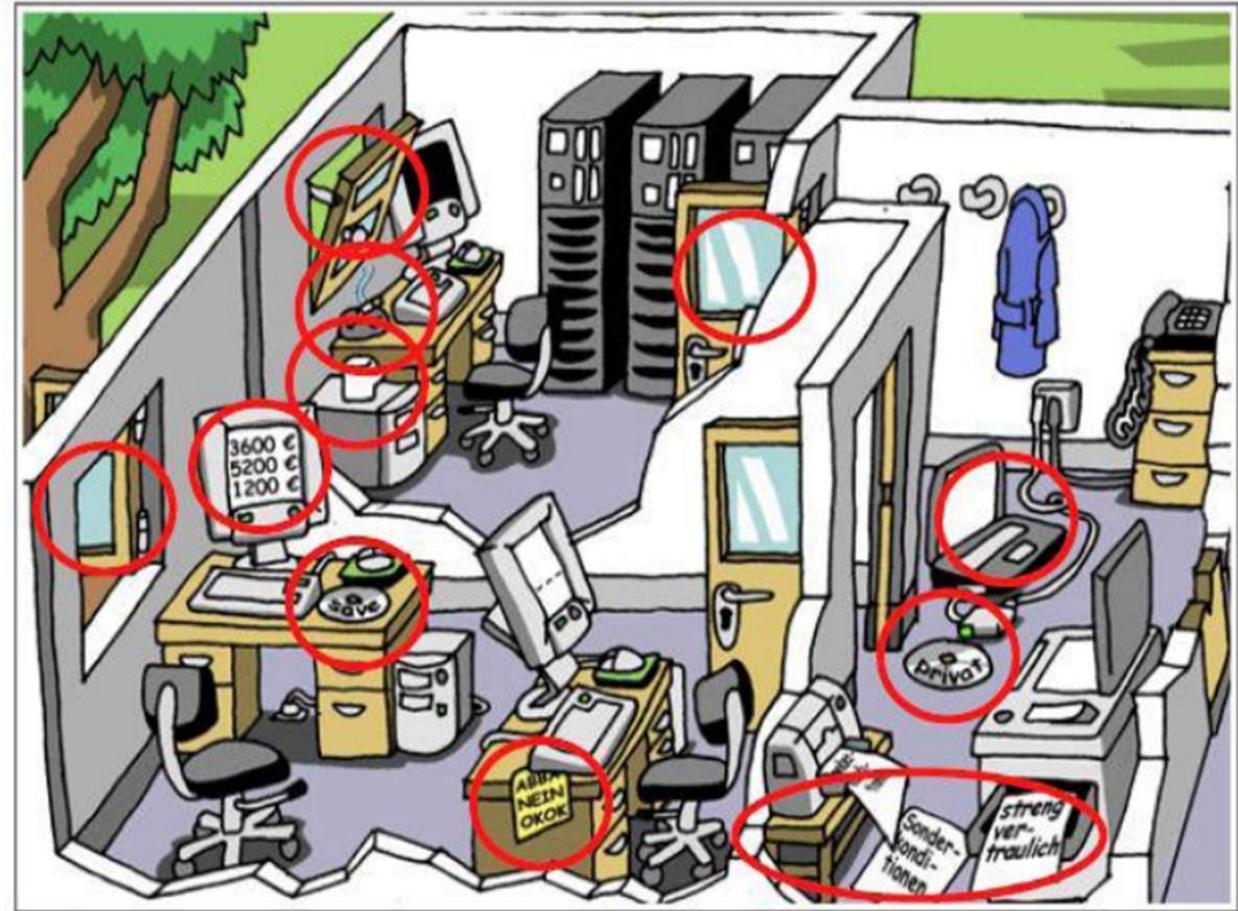
**Maurice Quirin, LL.M.**  
ist Consultant und DSB/DSA der  
varISO GmbH.

- Studium der Rechtswissenschaften Universität Mannheim und Guildford (UK)
- Unternehmensjurist seit 2013
- (externer) zertifizierter Datenschutzbeauftragter (DSB-TÜV) seit 2016
- Master of Laws, LL.M. (Schwerpunkt Compliance) seit 2017
- (externer) zertifizierter Datenschutzauditor (DSA-TÜV) seit 2020
- Certified Compliance Professional, CCP (Schwerpunkt Corporate Compliance), Frankfurt School of Finance and Management seit 2021
- Certified Lead Auditor IT-Sicherheitsmanagement ISO 27001
- Berufliche Stationen bei Ebner Stolz, EY Law Rechtsanwaltsgesellschaft mbH und DB Cargo AG
- Privatdozent  
Compliance, Prozess- und Qualitätsmanagement, Besonderes Wirtschaftsrecht, IU Internationale Hochschule Mannheim, Augsburg und Mainz;  
IT-Sicherheitsmanagement, Business Intelligence, Trendforschung und Innovation, Führung und Nachhaltigkeit an der FOM Hochschule für Oekonomie & Management gemeinnützige Gesellschaft mbH bundesweit

# Grundlagen Datenschutz



# Grundlagen Datenschutz



# Was ist Datenschutz ? (I)

Der Schutz von personenbezogenen oder personenbeziehbaren Daten vor:

- Missbrauch
- Unberechtigter Einsicht oder Verwendung
- Änderung oder Verfälschung



## Personenbezogene Daten

- Daten, welche eine Person identifizierbar machen, wie z.B. Familienname
- Je mehr an personenbezogenen Daten dazukommen, desto leichter fällt die Identifikation, wie z.B. Familienname + Vorname

## Personenbeziehbare Daten

- Daten ohne direkten Bezug, aus denen sich aber eine Person herleiten lässt, wie z.B. ein Autokennzeichen

# Was ist Datenschutz ? (II)



- Personenbezogene Daten sind mehr als nur Name, Geburtsdatum, Anschrift, sondern **ALLE Daten, die sich auf eine natürliche Person beziehen.**
- Es ist irrelevant, ob dieser Bezug in der gleichen Datenbank hergestellt wird, so lange der Bezug mit vertretbarem Aufwand hergestellt werden könnte (!)

# Was ist Datenschutz ? (III)

- Missbrauch ist im Zweifel jeder Umgang mit Daten außer ...



- ... es gibt eine rechtswirksame Einwilligung
- ... es gibt eine Rechtsgrundlage
- ... es gibt ein übergeordnetes Interesse

Im Zweifelsfall lieber einmal zu viel fragen, statt etwas falsch zu machen und es sich unwissentlich als „richtig“ anzueignen!

- Bei Datenmissbrauch haftet man unmittelbar und persönlich mit evtl. Schadensersatzforderungen des Betroffenen
- § 823 Abs. 2 BGB i.V.m. Artikel 82 DSGVO → übergeordnet BGB § 832 Abs. 2 f
- Schadensersatz gilt z.B. auch für Kommunen



# Datenschutzgesetze

- Bei Datenschutz denkt man sofort an die **DSGVO**, die seit 2018 verbindlich anzuwenden ist.
- Aber es gibt weitere, zahlreiche Gesetze zum Datenschutz oder Gesetze, die die Einhaltung zum Datenschutz fordern:



- BDSG: Bundesdatenschutzgesetz
- LDSG: Landesdatenschutzgesetze der jeweiligen Bundesländer
- LTranspG: Landestransparenzgesetz der einzelnen Bundesländer
- TTDSG: Telekommunikations-Telemedien Datenschutzgesetz
- StGB: Strafgesetzbuch des Bundes
- und noch viele weitere ...



Teilweise mit empfindlichen Strafen



JEDER kann bei Verstößen auch privat haftbar gemacht werden

# Ziel und Gegenstand von Datenschutz



## Ziel von Datenschutz

Der Einzelne soll davor geschützt werden, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird

→ Datenschutz schützt vorrangig den **MENSCHEN** und nur nachrangig die Daten

### Datenschutz

Schützt natürliche Personen wie Mitarbeiter, Bürger, Kunden, Lieferanten etc.

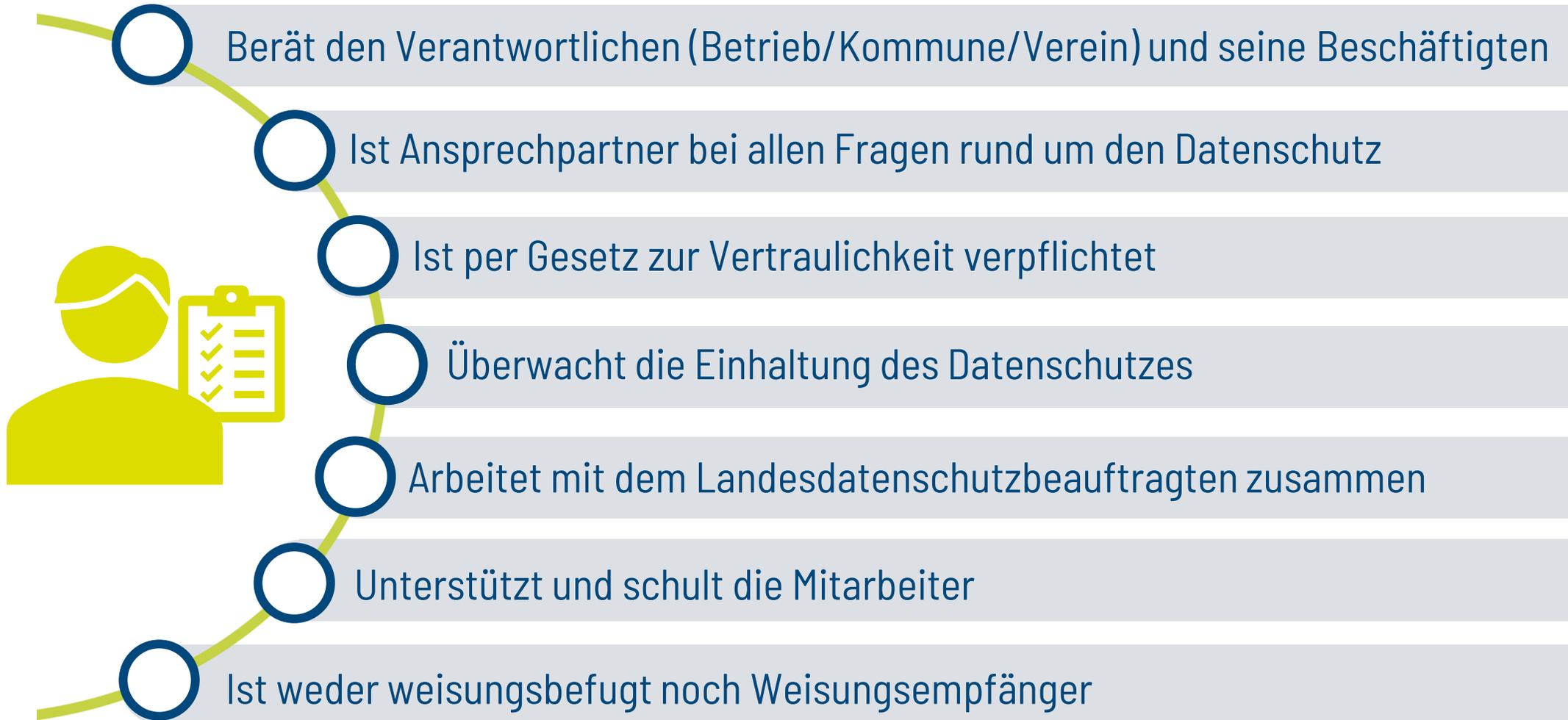
### Datensicherheit

Schützt Hardware, Software und Daten (auch nicht personenbezogene)  
→ die Institution

**Aber: ohne Datensicherheit kein Datenschutz!**



# Aufgaben Datenschutzbeauftragter



# Datenschutz-Grundsätze



Die Datenschutzgrundsätze sind **stets** einzuhalten.

Auch muss der Verantwortliche den Nachweis über die Einhaltung der Datenschutzgrundsätze erbringen (Rechenschaftspflicht).



# Rechtsgrundlagen



Die Verarbeitung von Daten unterliegt dem **Verbot mit Erlaubnisvorbehalt!**  
**Keine Verarbeitung ohne Rechtsgrundlage!**



Die Rechtsgrundlage für eine Datenverarbeitung im gemeindlichen Bereich ist in der Regel Art. 6 Abs. 1 lit. e) DSGVO in Verbindung mit

- einem Fachgesetz (überwiegend im Bereich der Pflichtaufgaben) oder
- § 4 LDSG (überwiegend im freiwilligen Bereich)



Bei der Erhebung und Verarbeitung von personenbezogenen Daten ist stets vorab zu prüfen, ob diese zur **Erfüllung des beabsichtigten Zweckes** erforderlich sind. Daten die darüber hinaus gehen, dürfen nicht erhoben werden.

# Rechte des Betroffenen



Anfragen von Betroffenen sollten umgehend bearbeitet werden, da hinter allen Rechten auch entsprechende Fristen stehen. Der/die Datenschutzbeauftragte unterstützt bei der Beantwortung.

# Pflichtinformationen und Auskunft

Bei Datenerhebung müssen dem Betroffenen die sog. Pflichtinformationen nach Art. 13 ff. DSGVO bereitgestellt werden. Unter anderem muss über den Zweck und den Umfang der Verarbeitung, die Rechtsgrundlage, die voraussichtliche Dauer der Speicherung der Daten sowie über die Betroffenenrechte informiert werden.



Datenschutzhinweise müssen **proaktiv** dem Betroffenen zur Verfügung gestellt werden und die verschiedenen Verarbeitungen darstellen.



Datenschutzhinweise dürfen **keine falschen Informationen** enthalten und sollten stets mit dem **Datenschutzbeauftragten** abgestimmt werden



**Konkrete Auflistungen** der gespeicherten Daten sind i.d.R. **nicht notwendig**, es reichen Datenkategorien. Sie müssen aber ermittelbar sein können



Auf Nachfrage **MUSS Auskunft gegeben** werden, welche konkreten Daten erhoben/verarbeitet werden, zu welchem Zweck und wann diese gelöscht werden

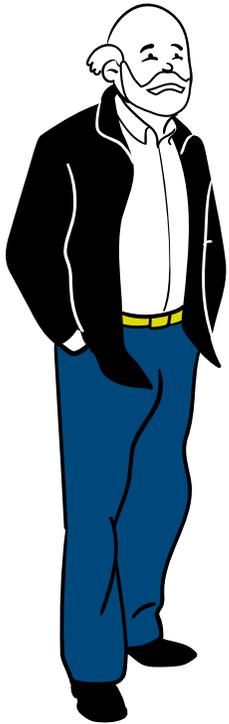


# Externe Dienstleister

- Bei der Beauftragung von externen Dienstleistern **müssen** datenschutzrechtliche Anforderungen beachtet werden
- Prüfung ob **Vereinbarung auf Vertraulichkeit** ausreicht (z.B. Reinigungsdienstleister) oder ob ein **Auftragsverarbeitungsvertrag** (z.B. IT-Dienstleister) notwendig wird
- Auftragsverarbeitungsverträge müssen DSGVO-konform ausgestaltet sein



Artikel 28 DSGVO: Prüfung des AV-Vertrages auf DSGVO-Konformität sowie Angemessenheitsprüfung der Schutzmaßnahmen



# Aktuelle Bedrohungslage / Cyberrisiken

## Aktuelle Warnungen und Gesetze

**BSI – Bundesamt für Sicherheit in der Informationstechnik** warnt 2022:  
(mit Ausbruch des Ukraine-Krieges)

- „Abstrakt erhöhte Bedrohungslage“
- Empfehlung, wachsam zu bleiben und „digitalen Hausaufgaben“ zu machen
- Auch 2023 noch eine nicht zu vernachlässigende Bedrohung

**Neues IT-Sicherheitsgesetz (IT-Sig 2.0)** ist gültig seit April 2022:

- Kommunen sind kritische Infrastruktur, ebenso alle Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen
- → erhöhte Sicherheits- und Datenschutzanforderungen im Betriebsalltag und zwar an alle Mitarbeiter der Organisation



# Aktuelle Bedrohungslage / Cyberrisiken

## Die Lage der IT-Sicherheit in Deutschland 2022 im Überblick

Quelle: BSI

### Top 3-Bedrohungen je Zielgruppe:



### Erster digitaler Katastrophenfall in Deutschland



**207** Tage Katastrophenfall

Nach Ransomware-Angriff konnten Elterngeld, Arbeitslosen- und Sozialgeld, Kfz-Zulassungen und andere bürgernahe Dienstleistungen nicht erbracht werden.

Die Anzahl der Schadprogramme steigt stetig. Die Anzahl neuer Schadprogramm-Varianten hat im aktuellen Berichtszeitraum um rund

**116,6** Millionen zugenommen.

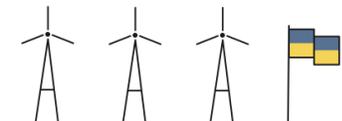


### Hackivismus im Kontext des russischen Krieges:

Mineralöl-Unternehmen in Deutschland muss kritische Dienstleistung einschränken.



**Kollateralschaden** nach Angriff auf Satellitenkommunikation



**20.174**

Schwachstellen in Software-Produkten (13% davon kritisch) wurden im Jahr 2021 bekannt. Das entspricht einem **Zuwachs von 10%** gegenüber dem Vorjahr.



**15 Millionen** Meldungen zu Schadprogramm-Infektionen in Deutschland übermittelte das BSI im Berichtszeitraum an deutsche Netzbetreiber.



**34.000**

Mails mit Schadprogrammen wurden monatlich durchschnittlich in deutschen Regierungsnetzen abgefangen.

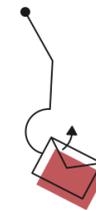


**78.000**

neue Webseiten wurden wegen enthaltener Schadprogramme für den Zugriff aus den Regierungsnetzen gesperrt.

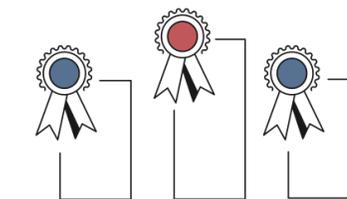
**69%**

aller Spam-Mails im Berichtszeitraum waren Cyber-Angriffe wie z.B. Phishing-Mails und Mail-Erpressung.



**90%**

des Mail-Betrugs im Berichtszeitraum war Finance Phishing, d.h. die Mails erweckten betrügerisch den Eindruck, von Banken oder Sparkassen geschickt worden zu sein.



BSI ist weltweit der führende Dienstleister im Bereich Common-Criteria-Zertifikaten.

**4.400** → **5.100**  
2020 → 2021

Zehn Jahre Allianz für Cyber-Sicherheit: 2022 sind wir bereits **6.220** Mitglieder.



Deutschland Digital•Sicher•BSI•

# Aktuelle Bedrohungslage / Cyberrisiken



## 3.2 Was also tun? (I)

! Immer mit **gesundem Menschenverstand** und **überlegt handeln**, nicht **vorschnell und hektisch!**

! **Digitale Sicherheitsmaßnahmen überprüfen** und **Schwachstellen beseitigen**

! Mails im **Zusammenhang mit Ukraine Krieg** **IMMER** kritisch prüfen, insbesondere bei Anhängen

! Reißerische Nachrichten, bei denen man den Bericht selbst nur über **„Weiter klicken“ Buttons** erreicht, niemals öffnen

! IT Abteilung sollte die **Meldungen des BSI und ACS\*** täglich lesen: wichtige Informationen hieraus, die den Alltag betreffen, sollten immer sofort mit den Vorgesetzten besprochen werden

! Es sind auch verstärkt **gefälschte Mails** von Banken, Onlinelieferdiensten usw. im Umlauf, die ihre „Sicherheitsmaßnahmen“ zum Schutz erhöhen wollen: Hierbei handelt es sich um Phishing-Attacken um an Ihre Daten zu kommen

# Aktuelle Bedrohungslage / Cyberrisiken



## 3.2 Was also tun? (II)



**Niemals Daten preisgeben**, vor allem Banken werden Sie NIEMALS nach Zugangsdaten fragen



Mails die einem **merkwürdig** vorkommen mit der IT besprechen



Gibt man den Text solcher Mails z.B. grob in eine **Internet-Suchmaschine** ein, erscheinen oft sehr schnell Warnmeldungen verschiedener Stellen zu Fake Mails – so kann man selbst im Vorfeld grob vorfiltern



Wenn der **Absender bekannt** ist, hilft es auch oft den Absender zu kontaktieren und nach der besagten, fragwürdigen Mail zu fragen



**Sicherungs- und Löschkonzepte** sind nicht nur gesetzlich vorgeschrieben, sondern unerlässlich um den Betriebsalltag aufrecht erhalten zu können



**Vielen Dank für Ihre  
Aufmerksamkeit**

**varISO**  
certified values

Maurice Quirin, LL.M.



+49 176 316 10 316



[maurice.quirin@variso.de](mailto:maurice.quirin@variso.de)