Schulung zur Datenschutz-Grundverordnung (DSGVO)

Warum diese Schulung?

- „Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter“ (Art 39 Abs. 1b DSGVO)
- “organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung” (Art 32 Abs. 1 DSGVO)
- “Rechenschaftspflicht“ (Art 5 Abs. 2 DSGVO)

Wer und wann?

- Zielgruppe: alle Mitarbeitenden die mit personenbezogenen Daten zu tun haben (bsp. E-Mail)
- Zeitpunkt: unmittelbar nach Aufnahme der Tätigkeit
- Häufigkeit: i.d.R. einmal jährlich; oder bei wesentlichen Änderungen
- Für alle Branchen

Personenbezogene Daten

- Kundendatenbank, Mitarbeiterakte, Videoaufzeichnung
- Beispiele personenbezogene Daten: Name, Adresse, Kundennummer, Kfz-Kennzeichen, IP-Adresse
- Gilt für alle Branchen: von Kundendaten im Handel, bis Patientenakte in Arztpraxis

DSGVO-Grundsätze (Art. 5 DSGVO)

- Rechtmäßigkeit
- Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit

DSGVO-Grundsätze (Art. 5 DSGVO)

- Jede Verarbeitung benötigt Einwilligung oder gesetzliche Grundlage
- Daten nur für vorher festgelegte Zwecke nutzen
- Beispiel: Kundendaten nur für Werbung verwenden, falls Kunde zugestimmt hat

Betroffenenrechte

Personen haben Recht auf:

- Auskunft
- Berichtigung
- Löschung („Recht auf Vergessenwerden“)
- Einschränkung der Verarbeitung
- Datenübertragbarkeit in maschinenlesbaren Format
- Widerspruchrecht (bsp. Direktwerbung)

Verantwortlichkeit im Unternehmen

- Datenschutzbeauftragte
- Kontakt zum internen Ansprechpartner für Datenschutzfragen
- Verfahren bei Betroffenenrecht
- Beispiel:
  Kunde möchte Auskunft über gespeicherte Daten.
  → Datenschutzbeauftragten informieren bzw. zuständige Verfahren anstoßen (Auskunft muss innerhalb 1 Monats Frist erteilt werden)
- Alle Mitarbeitenden tragen zur Datenschutz-Compliance bei

Datenschutz in der Praxis
Do's & Don'ts

Minimalprinzip

- Nur so viele Daten erheben / verwenden wie nötig
- Beispiel: bei Formularen keine unnötigen Felder ausfüllen, welche nicht gebraucht werden

Keine Weitergabe ohne Berechtigung

- Personenbezogene Daten intern nur mit Berechtigung weitergeben (wer muss es wissen?).
- Extern Daten nur mit Einwilligung oder Absprache mit Vorgesetzten/Datenschutzbeauftragen herausgeben.
- Beispiel: Polizeianfrage nach Kundendaten – solche Fälle immer an Geschäftsführung/Datenschutzbeauftragten weiterleiten, nicht eigenmächtig herausgeben.

Datenvermeidung und Anonymisierung

- Daten: original < anonymisieren < vermeiden
- Beispiel: Kundennummern statt Klarnamen
- Alte Daten löschen / anonymisieren (Aufbewahrungsfristen!)

Arbeitsplatz

- Vertraulichkeit am Arbeitsplatz
- Clean-Desk-Policy: keine sensiblen Unterlagen offen auf dem Schreibtisch
- Bildschirme sperren beim Verlassen des Arbeitsplatzes
- Gespräche über persönliche Daten vertraulich führen (Bahnfahrt)
- E-Mail / Dokumentenversand: keine offenen E-Mailverteiler mit externen Empfängern (Verwendung BCC)
- Vertrauliche Daten verschlüsselt mailen. Übergabe Passwort per SMS/Anruf/Chat
- Adressaten prüfen

Verwendung privater Geräte/Dienste

- Nutzung privater USB-Sticks
- E-Mails für dienstliche Daten
- Falls eigene Geräte, Sicherheitsvorgaben einhalten

Meldepflicht

- Alle Mitarbeiter müssen Datenschutzbeauftragten jeden Datenschutzvorfall sofort melden
- Offenheit hilft, Schaden zu begrenzen
- „Lieber melden statt vertuschen“.

Geheimhaltung

- Vertraulichkeit von Kundendaten
- Verletzungen können Konsequenzen haben: Abmahnungen, Kündigung oder sogar Strafverfahren (bsp. Arzt §203 StGB)
- Datenschutz / IT-Richtlinien beachten

Konsequenzen von Verstößen

Folgen Datenschutzverstöße:

- **Betroffene**: bsp. Identitätsdiebstahl, Verlust Vertrauen
- **Unternehmen**: Bußgelder (20m€ oder 4% Umsatz), Schadensersatzansprüche, Image-Schaden

Beitrag Datenschutz

Datenschutz

- fördert Qualität und Vertrauen
- Wettbewerbsvorteil (werteorientiertes Marketing)
- auch Mitarbeiterdaten werden geschützt

Praxisbeispiele

E-Mail-Verteiler mit sichtbaren Empfängern

- Frau Müller möchte allen 200 Kunden einen Newsletter mit Angeboten schicken. Sie erstellt eine Rundmail und setzt die Kunden-E-Mail-Adressen ins „An:“ Feld. Nach dem Versand droht ein Kunde mit einer Meldung bei der Datenschutzaufsicht, da seine E-Mail-Adresse ohne Erlaubnis an Fremde ging.
- Analyse: Frau Müller hat gegen den Datenschutz verstoßen, da sie personenbezogene Daten (E-Mail-Adressen) unbefugt an Dritte offenlegte. Eine korrekte Vorgehensweise wäre gewesen, einen professionellen Newsletter-Dienst zu nutzen oder zumindest alle Empfänger ins „BCC“ (Blindkopie) zu setzen, damit Adressen verborgen bleiben.
- Folgen: Das Unternehmen musste den Vorfall dem Datenschutz-beauftragten melden. Man informierte die betroffenen Kunden und versprach Besserung. Zum Glück entstanden keine hohen Schäden, aber der Vertrauensverlust war spürbar.

Weitergabe von Kundendaten

- Ein Servicemitarbeiter erhält einen Anruf, in dem sich jemand als der Ehemann einer Kundin ausgibt und nach deren Vertragsdetails fragt. Ohne zu prüfen, gibt der Mitarbeiter gutgläubig Auskunft. Später stellt sich heraus, dass der Anrufer gar nicht berechtigt war – die Kundin beschwert sich, dass ihre Daten an Dritte gingen.
- Fazit: Identitäten von Anrufern immer prüfen, keinen Datenauskunft am Telefon ohne klare Berechtigung. Im Zweifel Rückruf anbieten oder interne Klärung. Solche konkreten Szenarien helfen den Mitarbeitenden, im Alltag richtig zu reagieren
- Achtung: es können falsche Telefonnummern angezeigt werden

Diebstahl Kundendaten

- Ein E-Commerce-Unternehmen speicherte Kundendaten (Namen, Adressen, Zahlungsinformationen) in einer unsicheren veralteten Cloud-Datenbank. Cyberkriminelle nutzten eine Schwachstelle in der veralteten Software aus, stahlen Daten von 50.000 Kunden und veröffentlichten diese im Darknet, was zu Identitätsdiebstahl führte.
- Der Verstoß verstieß gegen DSGVO-Artikel 32 (Datensicherheit). Ursachen:
  - Unverschlüsselte Daten: Sensible Informationen waren ungeschützt.
  - Veraltete Software: Fehlende Sicherheitsupdates ermöglichten den Angriff.
  - Schwache Authentifizierung: Keine Zwei-Faktor-Authentifizierung.
  - Keine Überwachung: Unautorisierte Zugriffe blieben unentdeckt.
- Regelmäßige Updates, Verschlüsselung und stärkere Sicherheitsmaßnahmen hätten den Vorfall verhindern können.

Checkliste für datenschutzgerechtes Verhalten

- Personenbezogene Daten
- Datenminimierung
- Zweckbindung
- Einwilligungen
- Vertraulichkeit
- Datensicherheit
- Saubere Kommunikation
- Betroffenenanfragen
- Private Nutzung von Geräten nur bei Freigabe
- Vorfälle melden
- Bei Unklarheit: Vorgesetzten oder Datenschutzbeauftragten fragen

Handlungsempfehlungen für Ihr Unternehmen

Datenschutz

Nichteinhaltung Datenschutz

- ungeschulte Mitarbeitende ermöglichen oft Datenschutzverstöße
- zerstört Qualität und Vertrauen
- Wettbewerbsnachteil
- Strafen (20m€ oder 4% Umsatz)

Handlungsempfehlungen

- Verankerung im Onboarding
- Jährliche Auffrischung
- Management einbeziehen
- Klare verständliche Sprache
- Unterlagen bereitstellen
- Feedback
- Verknüpfung mit anderen Themen
- Motivation und Kultur
- Externe Hilfe nutzen

Datenschutzbeauftragten

- Datenschutzbeauftragter Pflicht bei
  - > 20 Mitarbeitenden mit Persönlichen Daten (bsp. Outlook) oder
  - Geschäftsmodell mit regelmäßiger Überwachtung von Personen (bsp. Marktforschung, Gesundheitsdaten)
  - nach Artikel 37 DSGVO und §38 Bundesdatenschutzgesetz
- Qualifizierten Datenschutzbeauftragten bestellen
- Ressourcen fest einplanen
- Fortbildungsplan mit verpflichtender Teilnahme
- Netzwerk & Fachliteratur
- Herausforderungen antizipieren
- Verständnis bei Kollegen
- Datenschutzbeauftragten nicht isolieren
- Kontinuität
- Weitere Datenschutzakteure

Schulung zur Informationssicherheit

Informationssicherheit

- Alle Mitarbeitenden in IT-Sicherheitsmaßnahmen schulen
- Technische und organisatorische Verhalten
- Ziel: Sicherheitsbewusstsein zu erhöhen um Gefahren zu minimieren
- Rechtliche Grundlage: Schulungen als Bestandteil „geeigneter Maßnahmen“ (Art. 32 DSGVO, NIS2-Richtlinie der EU)
- Verletzt ein Mitarbeiter fahrlässig die Datensicherheit können fehlende Schulungen dem Unternehmen angelastet werden (Organisationsversäumnis).
- Training idealerweise beim Start / 1x jährliche Wiederholung

Passwort-sicherheit

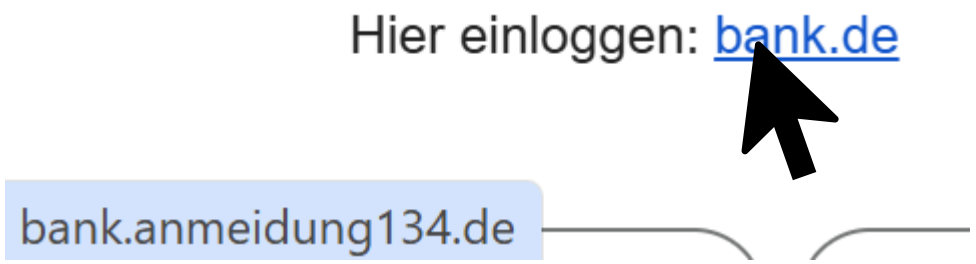
- Mindestens 8-12 Zeichen
- Groß/Kleinbuchstaben
- Zahlen
- Sonderzeichen
- Keine einfachen Wörter
- Keine Weitergabe
- Unterschiedliche Passwörter für unterschiedliche Zugänge
- evtl. Passwortmanager

Zugriffskontrolle

- Nur Zugriff auf Daten welcher Mitarbeiter benötigt
- Nicht mit fremden Accounts arbeiten
- Computer sperren (Str+Alt+Entf -> Sperren)
- Keine unbefugten Personen an eigenen PC lassen.

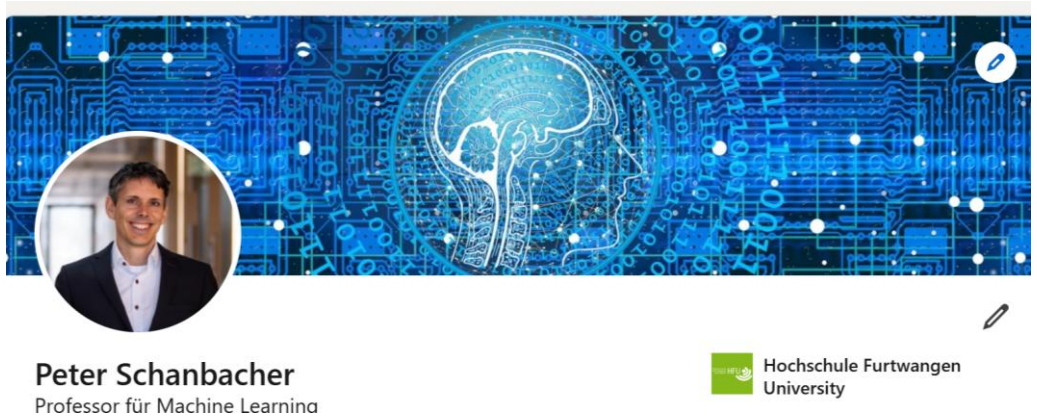
E-Mail

- Größte Einfallstür
- Phishing-Mails: typische Anzeichen
  - unpersönliche Anrede
  - Drängender Ton („sofort handeln“)
  - unbekannte Absenderadresse
  - ungewöhnliche Links
- Regeln:
  - Maus über Links hovern und Ziel kontrollieren
  - bank.anmeldung134.de ist eine Domain von anmeldung134 (mit großem I) nicht von bank.de
  - Nicht auf den Link klicken sondern selbst bei bank.de einloggen.
  - Keine unbekannte Anhänge (insb. keine .exe, .zip)
  - Bei Unsicherheit IT-Verantwortlichen fragen
  - Nicht auf dubiose E-Mails antworten



Social Engineering

- Betrüger können auch Informationen
  von Social Media erhalten
  und anrufen
  („Guten Tag [Name], hier ist der IT-Support“für [Unternehmen]“)
- Gefälschte E-Mails vom Chef
- Gesundes Misstrauen, Rückruf / Rückversicherung



Internetbrowser & Downloads

- Nur offizielle, zugelassene Software herunterladen
- Keine unbekannten Browser-Plugins installieren
- Vorsicht auf Websites mit Aufforderungen für Plugins
- Bei Unsicherheit IT-Verantwortlichen Fragen
- Regelung zur privaten Internetnutzung (darf in der Pause Facebook genutzt werden?)

Gerätesicherheit

- Virenschutz / Firewall etc. nicht umgehen oder ausschalten
- Software-Updates durchführen
- Beim Handy: keine Fremd-Apps außerhalb dem App-Store
- Geräte nicht frei herumliegen lassen
- Verlust immer sofort melden (evtl. Fernlöschung möglich)
- Unverschlüsselte Datenträger
- Keine unbekannten USB-Sticks in Firmen-PCs
- Im öffentlichen Raum niemand in den Bildschirm sehen lassen (Bahn/Flugzeug)

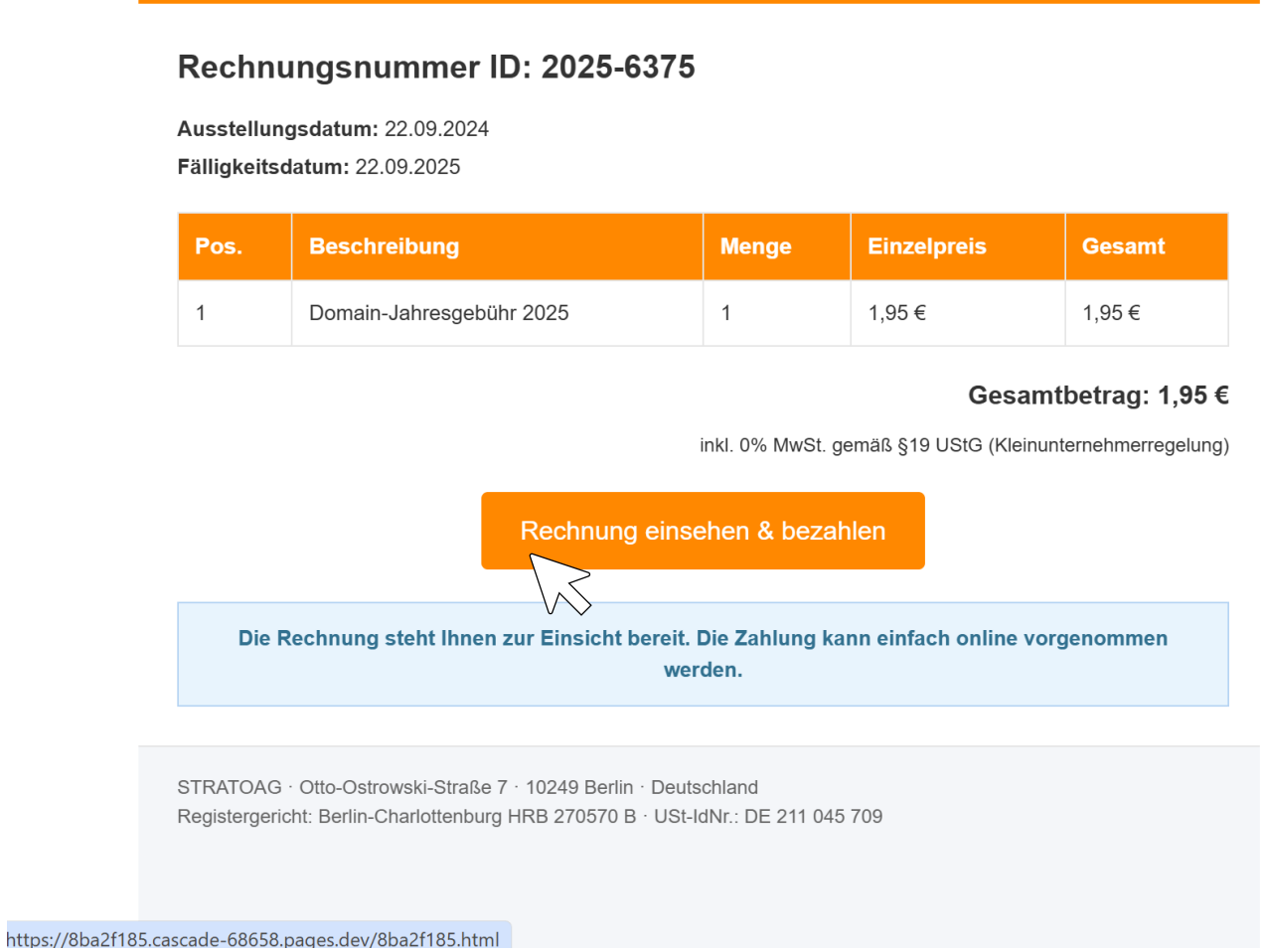
Arbeitsplatz

- Clean-Desk
- Keine Post-its mit Passwörtern am Bildschirm oder unter Ablagen
- Keine Zugangskarten herumliegen lassen
- Schränke für Laptops abschließen sofern möglich
- Notfallnummer/Ansprechpartner für IT notieren

IT-Sicherheitsvorfälle

- Bei merkwürdigem Verhalten des Computers
  - Netzwerkkabel ziehen / W-Lan ausschalten
  - IT informieren
  - Keine falsche Scheu, sondern schnelle Reaktion
- Konsequenz von zu spätem Handeln führt bei vielen Unternehmen zu wochenlangem Stillstand

Praxisbeispiele



Rechnungsnummer ID: 2025-6375

Ausstellungsdatum: 22.09.2024

Fälligkeitsdatum: 22.09.2025

Pos.	Beschreibung	Menge	Einzelpreis	Gesamt
1	Domain-Jahresgebühr 2025	1	1,95 €	1,95 €

Gesamtbetrag: 1,95 €

inkl. 0% MwSt. gemäß §19 UStG (Kleinunternehmerregelung)

Rechnung einsehen & bezahlen

Die Rechnung steht Ihnen zur Einsicht bereit. Die Zahlung kann einfach online vorgenommen werden.

STRATOAG · Otto-Ostrowski-Straße 7 · 10249 Berlin · Deutschland
Registergericht: Berlin-Charlottenburg HRB 270570 B · USt-IdNr.: DE 211 045 709

https://8ba2f185.cascade-68658.pages.dev/8ba2f185.html

Spam. Hinweise:

- Keine Ansprache
- Merkwürdiger Link

Handeln:

- Direkt bei www.strato.de einloggen
- Dort die Rechnungen einsehen

Praxisbeispiele

Critical Update Regarding Your Distribution:

We must inform you that our recent effort to process your distribution claim was unsuccessful. As a result of this failed processing and considerable unclaimed distributions from earlier phases, the remaining distribution amount now available to you has grown significantly.

Urgent Action Required: Your enhanced distribution has been reserved and is currently available for immediate processing. To guarantee successful completion, please update your account details and claim information. Unclaimed funds may be subject to redistribution once the final distribution period concludes.

You can now access your enhanced distribution details and modify your settings via the FTX Claims Portal. We highly recommend you access your account immediately to update your information and ensure you receive your full distribution.

To process your outstanding distribution:

- Access the FTX Claims Portal
- Examine your updated claim status and distribution amount
- Complete the instructions to process your outstanding funds

Access Portal

We sincerely appreciate your patience during this process.

egards,

https://bpmaneesha.com/yu/

Spam. Hinweise:

- Keine Ansprache
- Merkwürdiger Link
- Handlungsdruck
  „Urgent Action required“

Handeln:

- Nicht auf „Access Portal“ klicken
- Direkt im Browser beim
  FTX Portal einloggen
- Dort die ausstehenden Aktionen durchführen

Praxisbeispiel

- Frau Schulz, Assistentin der Geschäftsführung, erhält eines Tages eine E-Mail angeblich vom CEO. Dieser ist gerade auf Geschäftsreise. In der Mail bittet „Herr CEO“ sie, schnell 50 iTunes-Geschenkkarten zu kaufen für Kundenpräsente und ihm die Codes zu mailen, da er gerade nicht telefonieren kann. Ohne Rückfrage kauft sie eilig die Gutscheine (im Wert von 2.000 €) und sendet die Codes an die angegebene Adresse. Erst später merkt sie, dass die Absenderadresse nicht die echte des Chefs war. Sie ist Opfer eines „CEO-Fraud“ geworden. Das Geld ist weg.
- Analyse: Hier war Social Engineering im Spiel. Offenbar hatte die Firma keine ausreichende Security Awareness hierzu – oder Frau Schulz war nicht geschult genug, misstrauisch zu sein. Hätte sie von solchen Betrugsfällen gehört (die Warnzeichen: merkwürdige Sprache, ungewöhnliche Bitte um Vertraulichkeit, Eile, Gutscheinkarten verlangen), hätte sie misstrauisch sein können und z. B. per SMS oder alternativen Kanal Rückfrage beim Chef gehalten.

Checkliste

- Passwörter & Login
- Zugang sperren
- E-Mail-Vorsicht
- Phishing-Erkennung
- Keine unbekannten USB-Geräte
- Software-Updates
- Vertrauliche Daten verschlüsseln
- Geräte schützen
- Keine dubiosen Websites
- Meldewesen
- Regeln einhalten

Handlungsempfehlung für IT-Sicherheit für KMUs

Handlungsempfehlungen

- Awareness-Programm etablieren
- Simulierte Angriffe nutzen
- Schulung für Führungskräfte
- Kultur der Offenheit
- Klare Richtlinien (IT-Sicherheitsrichtlinie)
- IT-Notfallkontakt

- Technische Unterstützung
  - E-Mail-Filter
  - Passwortmanager
  - Automatisierte Backups
  - Schulungen
- Belohnung positiver Beispiel
- Bei Zertifizierung (bsp. ISO 27001) Nachweis der Schulungen führen

KI-Schulung

EU AI Act

- erstes umfassende KI-Gesetz
- Vertrauenswürdige KI & Risikominimierung
- für alle Unternehmen in EU
  (Sitz oder wirtschaftlich tätig)
- Ausnahme: rein private & militärische Nutzung
- Erste Teile (bsp. verpflichtende Schulungen) sind bereits in Kraft

- Ziele:
  - Diskriminierung verhindern
  - Transparenz in KI-Entscheidungen
  - Schutz Grundrechte & Sicherheit
- Sanktionen:
  - Bußgelder bis 35m€ / 7% Jahresumsatz
  - höher als DSGVO
  - KI-Systeme verbieten

Überblick

- Wer ist betroffen?
- Risikobasierter Ansatz
- Anforderungen an Hochrisiko-KI-Systeme
- Umsetzung im Unternehmensalltag

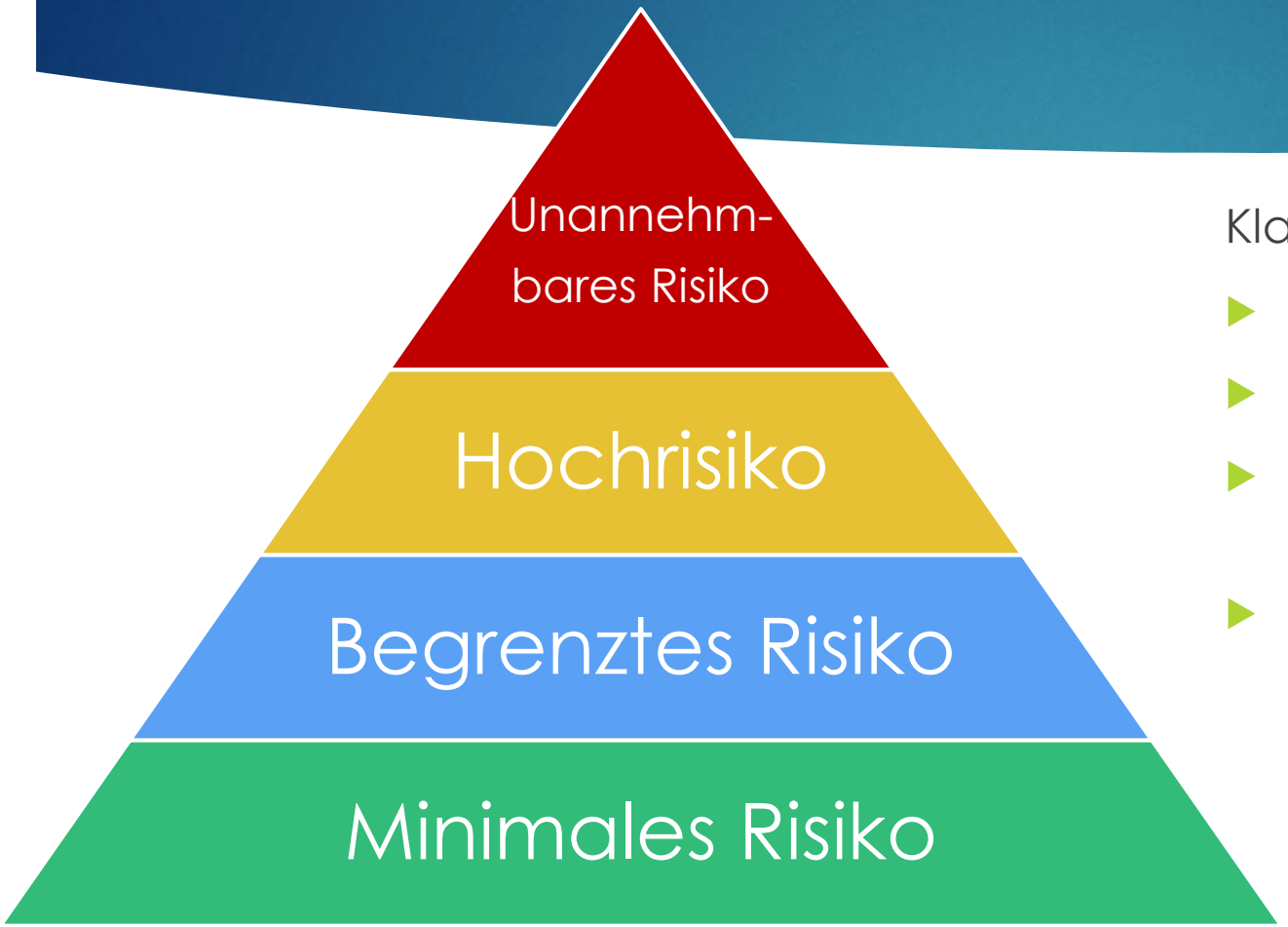
Definition KI-System

- „*KI-System ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und [..] das aus den erhaltenen Eingaben [..] Ziele ableitet, wie [..] Empfehlungen oder Entscheidungen [..] die physische oder virtuelle Umgebungen beeinflussen können;* “ (Art. 3 EU AI Act, gekürzt)
- sehr allgemein
- komplexe Programme im Zweifel als KI-System einzustufen

Verantwortung abhängig von der Rolle

- Anbieter:
  - entwickelt KI-System
  - Hauptverantwortung
- Betreiber:
  - setzt KI-System ein
  - Verantwortung für korrekte Nutzung
- Händler:
  - verkauft / vermittelt KI-Systeme
  - prüfen Konformität
- Importeur:
  - bringt KI-Systeme aus einem Drittland in die EU
  - Prüft Konformität / Bevollmächtigter benennen

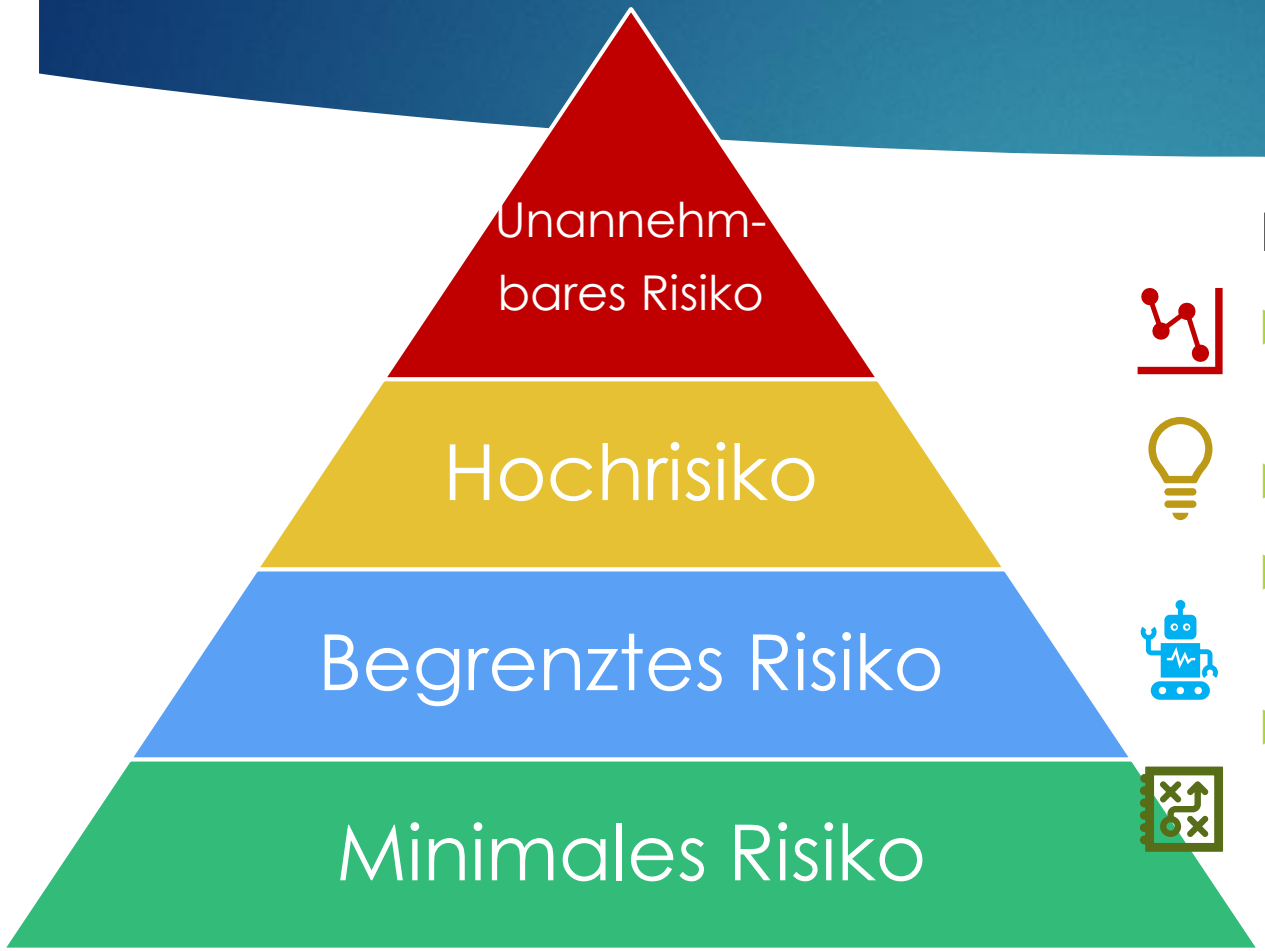
Risikobasierter Ansatz



Klassifizierung in 4 Risikostufen

- Unannehmbares Risiko: verboten
- Hochrisiko: strenge Überwachung
- Begrenztes Risiko: Transparenzanforderungen
- Minimales Risiko: Erlaubt

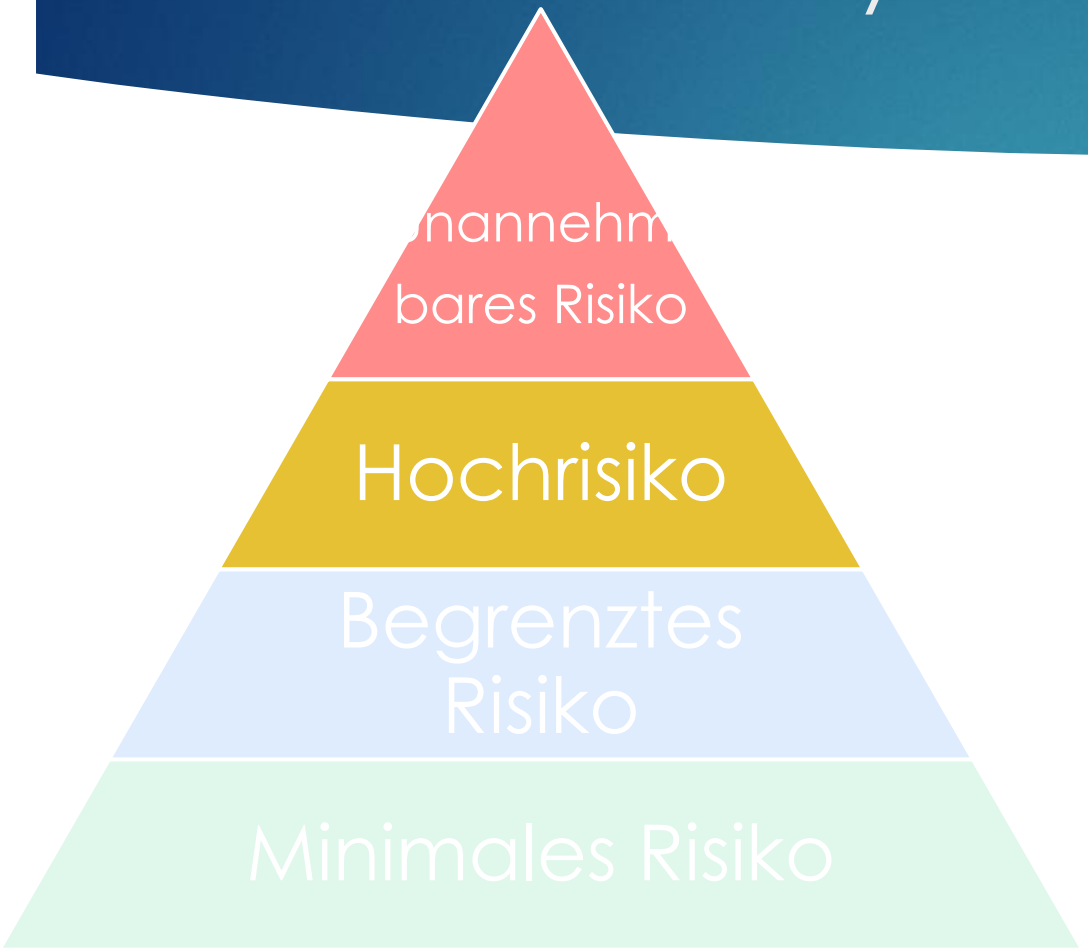
Risikobasierter Ansatz



Klassifizierung in 4 Risikostufen

- Unannehmbares Risiko: Social Scoring, Echtzeit-Gesichtserkennung
- Hochrisiko: KI in kritischer Infrastruktur
- Begrenztes Risiko: Chatbots, generative KI
- Minimales Risiko: Spamfilter, Empfehlungssysteme eCommerce

Hochrisiko-KI-Systeme



- Fokus: Hochrisiko-KI-Systeme
- KI mit erheblichen Auswirkungen auf Gesundheit, Sicherheit oder Grundrechte
- Definition Anhang III EU AI Act
- Kategorie 1: Bestandteil sicherheitsrelevanter Produkte (bsp. Medizinprodukt)
- Kategorie 2: eigenständige KI-Systeme mit potentieller Grundrechtsverletzung (bsp. Prüfung auf Sozialleistungen)

Hochrisiko-KI-Systeme

- Biometrie (falls überhaupt zulässig)
- Steuerung kritischer Infrastruktur
- Einsatz in Bildung
- Personalmanagement
- Grundlegende Dienste (Gesundheitsdienste, Kreditwürdigkeit, Versicherungspreise)
- Strafverfolgung (sofern zulässig)
- Migration & Grenzkontrolle (sofern zulässig)
- Rechtspflege & demokratische Prozesse

Prüfung KI-Systems

- Prüfung ob KI-System hochriskant ist
- Falls ja, gilt Technische & organisatorische Vorkehrungen (vor Inverkehrbringen) umzusetzen:
  - Risiko / Qualitäts-management
  - Data-governance
  - Technische Dokumentation
  - Protokollierung
  - Transparenz & Nutzerinformation
  - Robustheit & Sicherheit
  - Menschliche Aufsicht (finale Entscheidung beim Mensch)

Best-Practices

- Führungskräfte & Entwickler schulen
- AI-Verantwortlichen benennen (analog zum Datenschutzbeauftragten)
- KI-Systeme inventarisieren
- Risikoeinstufungen vornehmen
- Dokumentation für Hochrisiko-KI-System aufbauen
- (regelmäßige) Menschliche Überwachung sicherstellen
- Risiken evaluieren und Meldewesen verankern
- Learnings zur Produktverbesserung verwenden