Sicherheit im Netz

Carina Überle

ibi research an der Universität Regensburg GmbH

ERFOLGREICH HANDELN

Bayerisches Staatsministerium für Wirtschaft, Landesentwicklung und Energie

Agenda

01 Begrüßung und Einführung

02 Internet-Recht von A bis Z

03 Informationssicherheit

04 Datenschutz – Was bedeutet die DSGVO?

01 Begrüßung und Einführung

Projekt „Erfolgreich Handeln“ des Bayerischen Wirtschaftsministeriums

Der Handel soll wettbewerbsfähig bleiben – wir unterstützen dabei!

Die Corona-Pandemie, der Krieg in der Ukraine und die damit verbundenen Preissteigerungen haben massiven Einfluss auf den Handel.

Geändertes Einkaufsverhalten, veränderte Kundenbedürfnisse, hohe Energiekosten – wer in Zukunft noch erfolgreich sein will, muss sich anpassen.

Die Initiative „Erfolgreich handeln“, **initiiert und finanziert durch das Bayerische Staatsministerium für Wirtschaft, Landesentwicklung und Energie**, hilft Ihnen dabei!

Projektlaufzeit: Januar 2023 bis Dezember 2024

Vorgängerprojekt: Die Förderinitiative „Bayern hilft seinen Händlern“

www.erfolgreich-handeln.bayern

ERFOLGREICH HANDELN

Wie sieht unser Bildungsangebot aus?

Unsere Formate

Webseite & Newsletter

Workshops

Webinare

Mediathek | Webinar-aufzeichnungen

Unsere Themen

02 Internet-Recht von A bis Z

Rechtliche Aspekte

Häufigste Abmahngründe im Internet

1. Fehlerhafte Belehrung über das Widerrufsrecht
2. Markenrechtsverletzungen
3. Urheberrechtsverletzungen
4. Fehlerhafte Preisangaben
5. Fehlerhafte AGB
6. Fehlerhaftes/fehlendes Impressum (vgl. TMG)

Warum müssen Sie das wissen?

- Weil Abmahnungen nicht selten sind für Online-Händler,
- weil Abmahnungen Zeit kosten,
- weil Abmahnungen Geld kosten!

**Machen Sie deswegen alles gleich zu Beginn richtig –
oder fragen Sie jemanden, der etwas davon versteht!**

Impressumspflicht/Anbieterkennzeichnung

- **Jede** Website im geschäftlichen Umfeld benötigt ein **Impressum**, **nicht** nur **Online-Shops**!
- Die anzugebenden **Inhalte** richten sich nach **§ 5 Telemediengesetz** (TMG):
    - Name
    - Anschrift
    - bei juristischen Personen zusätzlich die Rechtsform und den Vertretungsberechtigten
    - Telefon, E-Mail-Adresse
    - ggf. Angaben zur zuständigen Aufsichtsbehörde (nicht Kammer!)
    - Handelsregisternummer
    - ggf. berufsrechtliche Angaben
    - Umsatzsteueridentifikationsnummer (nicht Steuernummer!)
    - …
- **Impressumspflicht** nach h.M. auch **für Social-Media-Auftritte** o.ä. (Facebook, XING, …)

Beispiel für ein Impressum

Impressum

Für allgemeine Fragen zur Stadtverwaltung wenden Sie sich bitte an:

E-Mail: stadt_regensburg@regensburg.de

Telefon: (0941) 507-0
Fax: (0941) 507-1199

Stadt Regensburg

Postfach 11 06 43
93019 Regensburg

Herausgeber (gemäß § 5 TMG; § 55 II RStV):

Stadt Regensburg

Altes Rathaus
Rathausplatz 1
93047 Regensburg

E-Mail: pressestelle@regensburg.de
Internet: www.regensburg.de

Die Stadt Regensburg ist eine Gebietskörperschaft des Öffentlichen Rechts.
Sie wird vertreten durch Oberbürgermeisterin Gertrud Maltz-Schwarzfischer.

USt-Identifikationsnummer gemäß
§ 27 a UStG: DE 133714341

Inhaltlich verantwortlich (nach § 55 II RStV):

Abteilung Presse- und Öffentlichkeitsarbeit
Juliane von Roenne-Styra

Altes Rathaus
Rathausplatz 1
93047 Regensburg

Telefon: +49 (0) 941 507-0
E-Mail: pressestelle@regensburg.de

Inhaltlich verantwortlich für das Geoportal

Amt für Stadtentwicklung
Dr. Volker Höcht

Neues Rathaus
D.-Martin-Luther-Straße 1
93047 Regensburg

E-Mail: stadtentwicklung@regensburg.de

Konzept und Online-Redaktion

Abteilung Presse- und Öffentlichkeitsarbeit

Stephan Rockinger
Telefon: +49 (0)941 507-4106
E-Mail: info@regensburg.de

Quelle: https://www.regensburg.de/impressum

Urheberrecht

- Sie müssen sicherstellen, dass auf Ihrer Website **keine** urheberrechtlich geschützten Inhalte verwendet werden, ohne dass Sie das Recht dazu haben.

- **JEDES** Bild
- **JEDER** Text
- **JEDE** Grafik, Video etc.

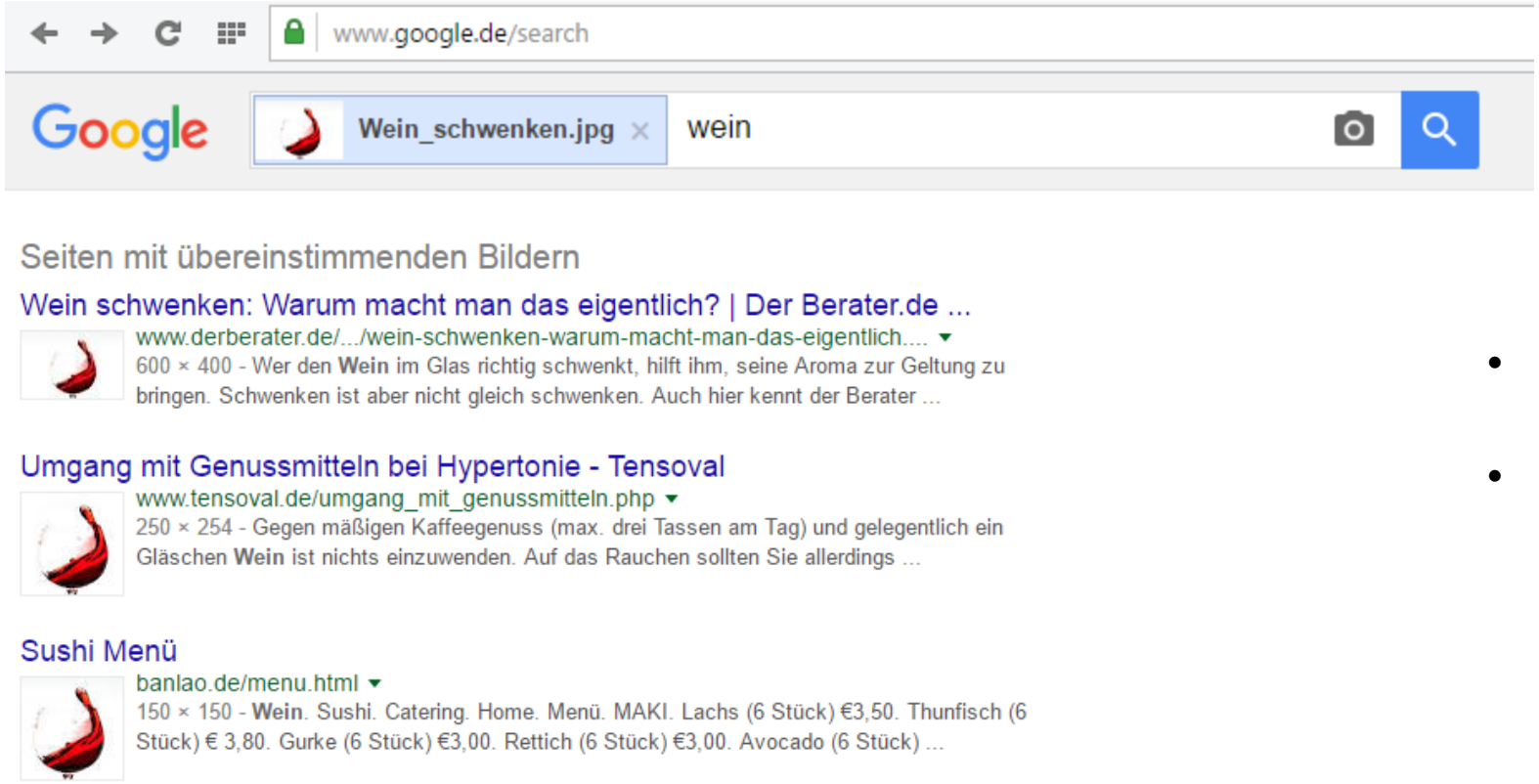
- **Häufiges Problem** bei Online-Shops: Produktbeschreibungen, Produktbilder

- **Lösung:**
    - Bilder, Texte u.ä. **selbst** produzieren
    - **Einwilligung** des Urhebers einholen
    - Erwerb einer **Lizenz** und Einhaltung der Lizenzbedingungen (z. B. Benennung von Bildquelle und Urheber)

- Daneben stehen andere **Schutzrechte**, z. B. Marken, Patente bzw. allg. Wettbewerb

Urheberrecht

- **Kopieren** Sie keinesfalls „Content“ von **fremden Quellen**, an welchem Sie keine Rechte/Lizenzen haben!



- Mit Google kann man nach Text und Bild (Inhalt!) suchen!
- Daher: Bilder entweder selbst produzieren oder kaufen.

Datenschutzerklärung

- **Pflicht** für **gewerbliche Internetseiten** und **Online-Shops**

- **Information** der Nutzer über Art, Umfang und Zwecke der Erhebung und der Verwendung personenbezogener Daten

- **Stichpunkte:**
    - Datenerhebung und -speicherung
    - Zweck
    - Verwendung von Cookies
    - Verwendung von Tracking-Tools wie Google Analytics
    - Auskunftsrecht des Nutzers
    - Möglichkeit des Widerrufs von Einwilligungen
    - Datenaustausch mit anderen Websites (z. B. Facebook-Like-Button)
    - Ansprechpartner/Datenschutzbeauftragter

Preisangaben

- Beim **Geschäft mit Verbrauchern** (B2C) gilt die **Preisangabenverordnung** (PAngV)
- **Angabe von Gesamtpreisen**, also inklusive Umsatzsteuer und sonstiger Preisbestandteile
- **Hinweis** auf **enthaltene Umsatzsteuer** sowie auf **Versandkosten**
- **Angabe des Grundpreises** „in unmittelbarer Nähe des Gesamtpreises“
- Grundsätze der **Preisklarheit** und **Preiswahrheit**

Fernabsatzvorschriften für Verbraucher

- Die **Regelungen** zum **Fernabsatz** wurden 2014 neu geregelt.
- **Neue EU-weite Widerrufsfrist** von 14 Tagen (bei wirksamer Belehrung über Widerrufsrecht; ansonsten maximal 12 Monate und 14 Tage)
- **Pflicht** zur **Zugänglichmachung** des einheitlichen **EU-Widerrufsformulars**
- **Ausdrücklicher Widerruf** durch den Kunden ist **nötig**, **nicht implizit** durch Rücksendung
- Im Rahmen des **Bestellprozesses** müssen **Angaben zum Liefertermin** gemacht werden
- Die **Rücksendekosten trägt** prinzipiell der **Käufer**
- Es gibt **Ausnahmen vom Widerrufsrecht**, z. B. individualisierte Produkte, Lebensmittel, …
- **Vorsicht bei B2B-Geschäft**: Räumen Sie nicht versehentlich auch Unternehmen Widerrufsrecht ein!

Praxistipp: Was machen Sie, wenn Sie eine Abmahnung erhalten?

Bildquelle: Flickr/Dirk Vorderstraße, CC-BY 2.0
https://www.flickr.com/photos/dirkvorderstrasse/15534064839

Verhalten bei Abmahnungen

- Eine **Abmahnung** besteht in der Regel aus **zwei Bestandteilen:**
    - Unterlassungserklärung
    - Übernahme der Kosten der Abmahnung

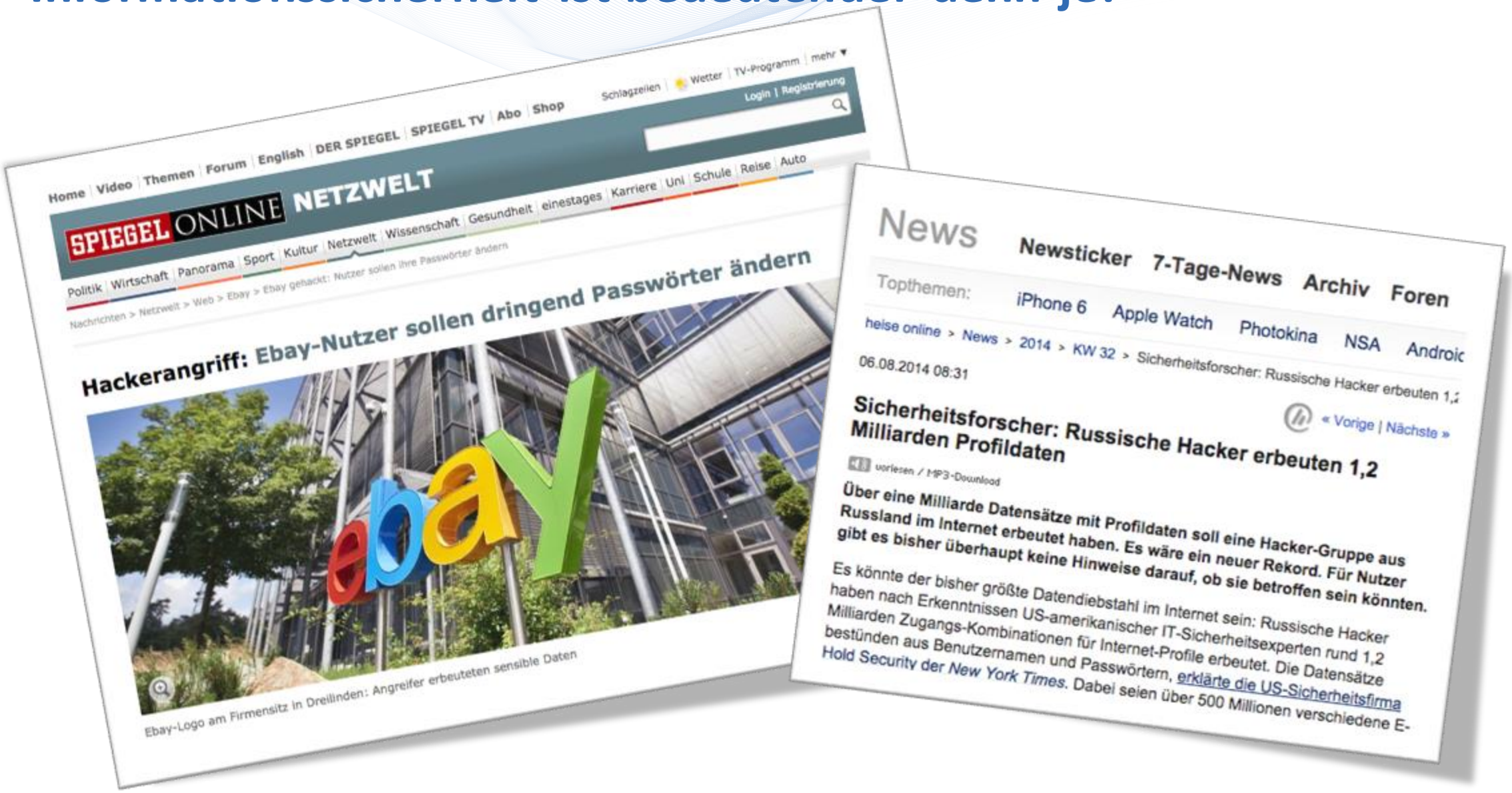
- **Unterschreiben** Sie **zunächst nichts!**

- Ziehen Sie einen **Rechtsanwalt zu Rate**!

- **Dieser wird zusammen mit Ihnen prüfen**,
    - ob die Abmahnung **berechtigt** und **rechtsfehlerfrei** ist,
    - ob die **Unterlassungserklärung modifiziert** werden sollte und
    - ob die **Kosten** bzw. der **Streitwert angemessen** sind.

03 Informationssicherheit

Informationssicherheit ist bedeutender denn je!



SPIEGEL ONLINE NETZWELT

Home | Video | Themen | Forum | English | DER SPIEGEL | SPIEGEL TV | Abo | Shop

Politik | Wirtschaft | Panorama | Sport | Kultur | Netzwelt | Wissenschaft | Gesundheit | einestages | Karriere | Uni | Schule | Reise | Auto

Nachrichten > Netzwelt > Web > Ebay > Ebay gehackt: Nutzer sollen ihre Passwörter ändern

Hackerangriff: Ebay-Nutzer sollen dringend Passwörter ändern

Ebay-Logo am Firmensitz in Dreilinden: Angreifer erbeuteten sensible Daten

News

Newsticker | 7-Tage-News | Archiv | Foren

Topthemen: iPhone 6 | Apple Watch | Photokina | NSA | Androic

heise online > News > 2014 > KW 32 > Sicherheitsforscher: Russische Hacker erbeuten 1,2

06.08.2014 08:31

« Vorige | Nächste »

Sicherheitsforscher: Russische Hacker erbeuten 1,2 Milliarden Profildaten

vorlesen / MP3-Download

Über eine Milliarde Datensätze mit Profildaten soll eine Hacker-Gruppe aus Russland im Internet erbeutet haben. Es wäre ein neuer Rekord. Für Nutzer gibt es bisher überhaupt keine Hinweise darauf, ob sie betroffen sein könnten.

Es könnte der bisher größte Datendiebstahl im Internet sein: Russische Hacker haben nach Erkenntnissen US-amerikanischer IT-Sicherheitsexperten rund 1,2 Milliarden Zugangs-Kombinationen für Internet-Profile erbeutet. Die Datensätze bestünden aus Benutzernamen und Passwörtern, erklärte die US-Sicherheitsfirma Hold Security der *New York Times*. Dabei seien über 500 Millionen verschiedene E-

Quelle: www.spiegel.de, www.heise.de

Was ist Informationssicherheit?

Zielsetzung von Informationssicherheit

Schutz von Informationen jeglicher Art und Herkunft

Wichtig: Informationen können vorliegen

- auf Papier
- in Rechnersystemen
- in den Köpfen der Nutzer

IT-Sicherheit versus Informationssicherheit

Elektronische Verarbeitung von Informationen in nahezu allen Lebensbereichen

→Unterscheidung, ob Informationen mit Informationstechnik, mit Kommunikationstechnik oder auf Papier verarbeitet werden, ist nicht mehr zeitgemäß.

→Begriff Informationssicherheit statt IT-Sicherheit ist umfassender und besser geeignet.

Quelle: Bundesamt für Sicherheit in der Informationstechnik

Klassische Grundwerte der Informationssicherheit sind Vertraulichkeit, Integrität und Verfügbarkeit

Vertraulichkeit
Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.

Integrität
Bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf Daten angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind.

Verfügbarkeit
Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.

Quelle: Bundesamt für Sicherheit in der Informationstechnik

Datenschutz und Informationssicherheit

Datenschutz ist Grundrechtsschutz

Artikel 1 Grundgesetz
(1) Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.

Artikel 2 Grundgesetz
(1) Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.

→ **Recht auf informationelle Selbstbestimmung**

Datenschutz verfolgt das Ziel, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

Was sind personenbezogene Daten?

Daten sind personenbezogen, wenn sie eindeutig einer bestimmten natürlichen Person zugeordnet sind oder diese Zuordnung zumindest mittelbar erfolgen kann (§ 46 BDSG).

Beispiele:

- Anschrift, Telefonnummer, E-Mail-Adresse, Beruf, Einkommen
- Name, Alter, Familienstand, Geburtsdatum, Verwandtschafts- und soziale Beziehungen
- Vorstrafen
- Surfgewohnheiten (z. B. Surfhistorie)
- Genetische/biometrische Daten (z. B. Schuh-, Körpergröße), Krankendaten
- Kraftfahrzeugnummer, Kfz-Kennzeichen
- Konto-, Kreditkartennummer, Kundennummer, IP-Adresse
- Werturteile (z. B. Zeugnisse)

Besonders sensible personenbezogene Daten

§46 Nr. 14 BDSG

Angaben über:

- rassische und ethnische Herkunft
- religiöse oder philosophische Überzeugungen
- politische Meinungen
- Gewerkschaftszugehörigkeit
- Gesundheit
- Sexualleben

Die acht Gebote des Datenschutzes stellen eine direkte Verbindung zur Informationssicherheit her

WENN: Erhebung, Verarbeitung oder Nutzung personenbezogener Daten selbst oder im Auftrag

- Treffen von technischen und organisatorischen Maßnahmen zur Gewährleistung der Ausführung der Vorschriften dieses Gesetzes (BDSG)
- Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

1. Zutrittskontrolle
(Schutz vor unbefugtem Zutritt zu DV-Anlagen)

2. Zugangskontrolle
(Schutz vor unbefugter Nutzung von DV-Anlagen)

3. Zugriffskontrolle
(Schutz vor unbefugtem Zutritt auf pers. Daten)

4. Weitergabekontrolle
(Kontrolle der Verarbeitung, Übermittlung, Entsorgung pers. Daten)

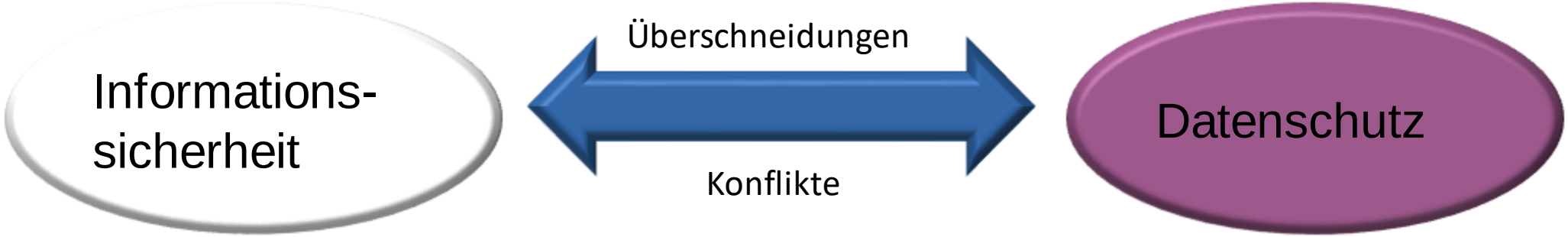
5. Eingabekontrolle
(Protokollierung von Dateneingaben)

6. Auftragskontrolle
(Kontrollen bzgl. Auftragsdatenverarbeitung)

7. Verfügbarkeitskontrolle
(Gewährleistung der Verfügbarkeit pers. Daten)

8. Trennungsgebot
(Gewährleistung der Trennung von Datenbeständen)

Informationssicherheit ist nicht gleichbedeutend mit Datenschutz

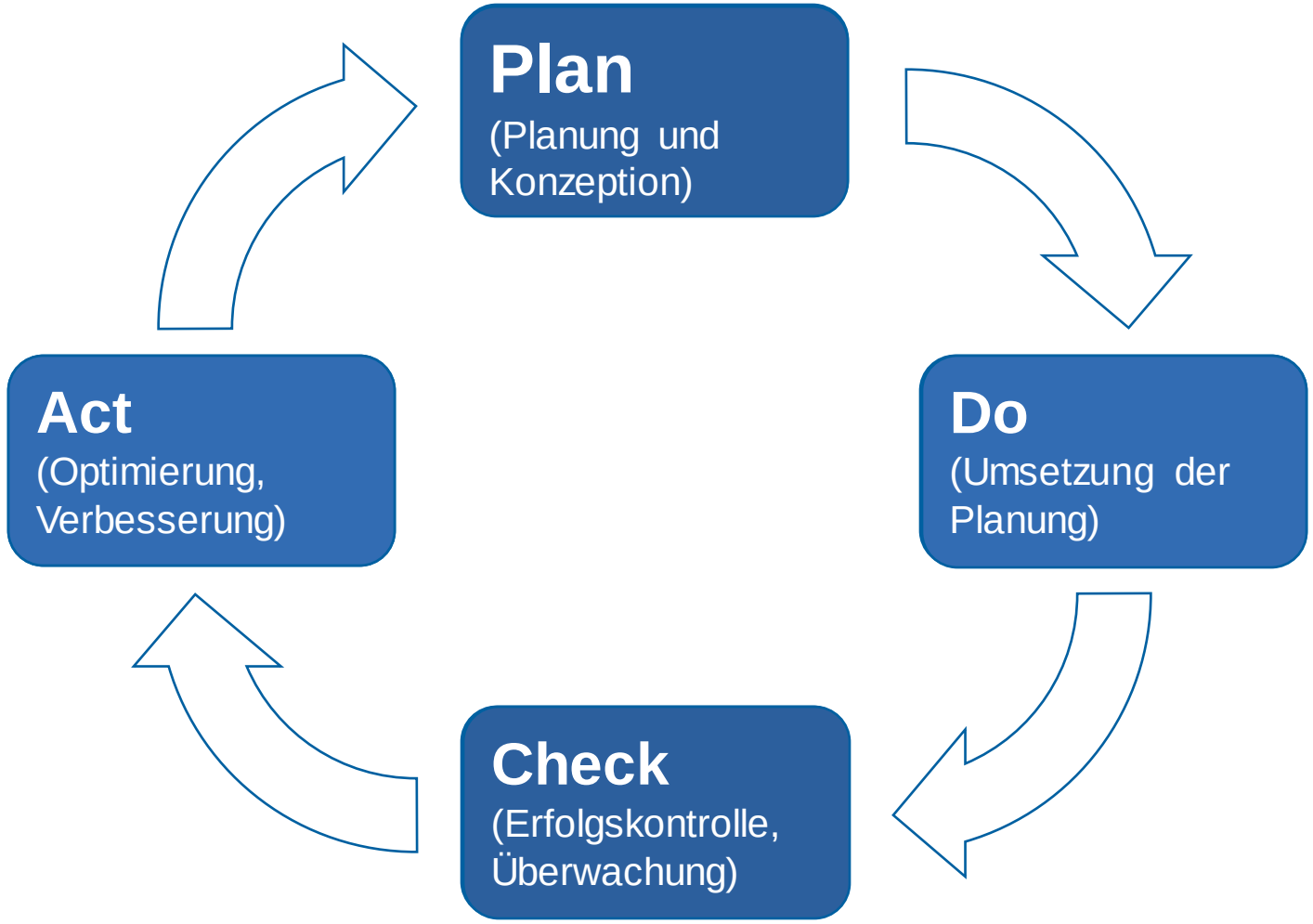


- Es gibt kein spezielles Gesetz, dass sich mit Informationssicherheit beschäftigt und Unternehmen bestimmte Maßnahmen vorschreibt.
- Datenschutz ist gesetzlich insbesondere in der DS-GVO und im BDSG geregelt.

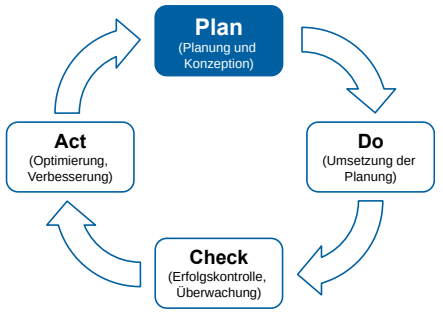
- **Informationssicherheit ist eine zentrale Voraussetzung zur Umsetzung des Datenschutzes.**

Quelle

Der PDCA-Zyklus ist von zentraler Bedeutung für die Informationssicherheit



Bestandsaufnahme „Infrastruktur“



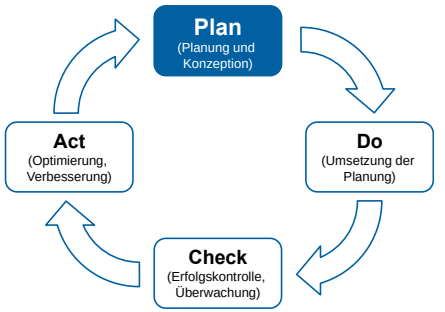
- Welche **Infrastruktur** kommt im Unternehmen zum **Einsatz**?
  - Rechner
  - Laptops
  - Smartphones
  - Maschinen

- Wird diese **Infrastruktur** auch von Ihnen oder Ihren **Mitarbeitern privat genutzt** (Facebook, eBay, E-Mail,...)?

- Welche **privat beschaffte Infrastruktur** kommt im **Unternehmen zum Einsatz**?
  - Greifen Sie oder Ihre Mitarbeiter mit dem privaten Smartphone auf Firmen-E-Mails zu?
  - Nutzen Sie auch Ihren privaten Rechner um Angebote/ Rechnungen zu schreiben, die Buchhaltung zu erledigen oder auf Bankkonten der Firma zuzugreifen?

Infrastruktur
Rechner Büro
Rechner Werkstatt
Mobiltelefone Mitarbeiter

Bestandsaufnahme „Anwendungen“



- Welche **Anwendungen** kommen auf der **identifizierten Infrastruktur zum Einsatz**?
  - Existieren für alle Anwendungen gewerbliche Lizenzen?

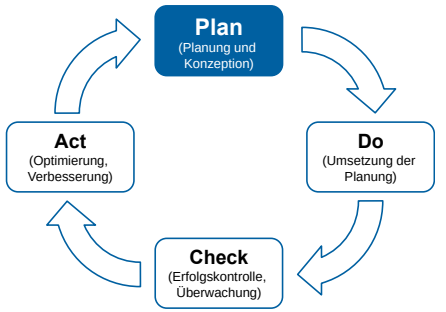
- Fragen Sie Ihre **Mitarbeiter, welche Anwendungen** Sie nutzen!
  - Werden Anwendungen genutzt, von denen Sie nichts wissen?
  - Dürfen Ihre Mitarbeiter selbständig Anwendungen installieren?

- **„Cloud-Dienste“?**
  - Auftragsdatenverarbeitung!

Infrastruktur	Anwendungen
Rechner Büro	Online-Banking
	CRM
	Buchhaltung
	Angebote/Rechnungen
	E-Mail
Rechner Werkstatt	Browser
	Warenwirtschaft
	CAD/CAM
	Zeiterfassung
	E-Mail
Mobiltelefone Mitarbeiter	E-Mail
	Browser

Bestandsaufnahme „Informationen“

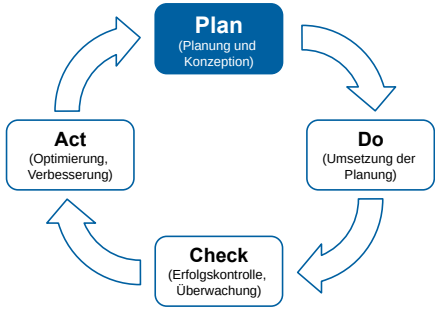
- Welche **Informationen** werden von **den erfassten Anwendungen** verarbeitet?
  - In welchen Situationen werden die Anwendungen verwendet?
  - Welche Eingaben erfordern die Anwendungen
  - Greifen die Anwendungen auf Datenbanken zu?



Infrastruktur	Anwendungen	Informationen
Rechner Büro	Online-Banking	Kontodaten Kreditor/Debitor
		Umsätze
		Ausgaben
	CRM	Kundendaten
		Lieferantendaten
		Mitarbeiterdaten
	Buchhaltung	Kundendaten
		Lieferantendaten
		Mitarbeiterdaten
		Umsätze
		Ausgaben
	Angebote/Rechnungen	Kundendaten
		Umsätze
	E-Mail	Kundendaten
Rechner Werkstatt	Browser	technische Daten
	Warenwirtschaft	Lieferantendaten
		Bestandsdaten
	CAD/CAM	technische Daten
	Zeiterfassung	Mitarbeiterdaten
	E-Mail	Kundendaten
Mobiltelefone Mitarbeiter	E-Mail	Kundendaten
	Browser	technische Daten

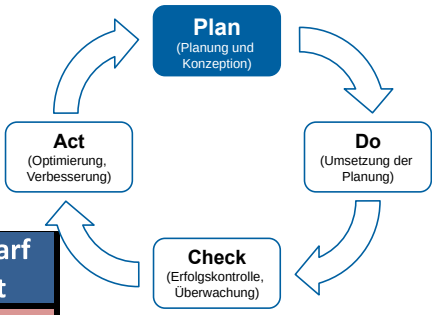
Bestandsaufnahme „rechtliche Aspekte“

- **An welche Gesetze müssen Sie sich halten?**
- **Welche Auflagen entstehen durch vertragliche Pflichten?**



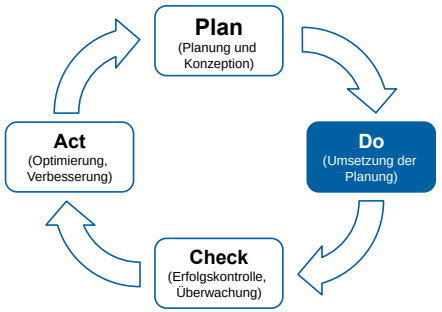
Infrastruktur	Anwendungen	Informationen	BDSG
Rechner Büro	Online-Banking	Kontodaten Kreditor/Debitor	✔
		Umsätze	✗
		Ausgaben	✗
	CRM	Kundendaten	✔
		Lieferantendaten	✗
		Mitarbeiterdaten	✔
	Buchhaltung	Kundendaten	✔
		Lieferantendaten	✗
		Mitarbeiterdaten	✔
		Umsätze	✗
		Ausgaben	✗
	Angebote/Rechnungen	Kundendaten	✔
		Umsätze	✗
	E-Mail	Kundendaten	✔
Rechner Werkstatt	Browser	technische Daten	✗
	Warenwirtschaft	Lieferantendaten	✗
		Bestandsdaten	✗
	CAD/CAM	technische Daten	✗
	Zeiterfassung	Mitarbeiterdaten	✔
	E-Mail	Kundendaten	✔
Mobiltelefone Mitarbeiter	E-Mail	Kundendaten	✔
	Browser	technische Daten	✗

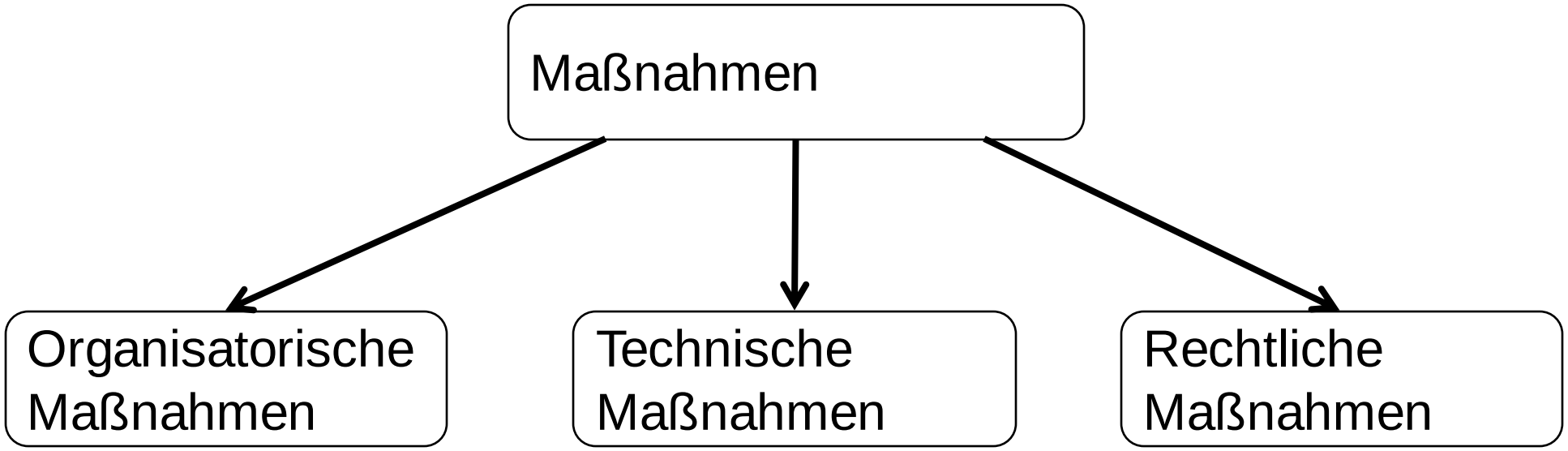
Bewertung hinsichtlich der Schutzziele durchführen



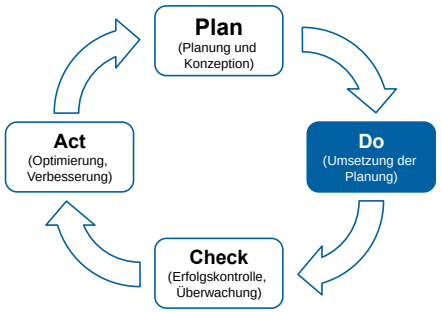
Infrastruktur	Anwendungen	Informationen	BDSG	Schutzbedarf Vertraulichkeit	Schutzbedarf Verfügbarkeit	Schutzbedarf Integrität
Rechner Büro	Online-Banking	Kontodaten Kreditor/Debitor	✔	hoch	mittel	hoch
		Umsätze	✗	mittel	mittel	hoch
		Ausgaben	✗	mittel	mittel	hoch
	CRM	Kundendaten	✔	hoch	mittel	hoch
		Lieferantendaten	✗	mittel	mittel	mittel
		Mitarbeiterdaten	✔	hoch	mittel	mittel
	Buchhaltung	Kundendaten	✔	hoch	mittel	hoch
		Lieferantendaten	✗	mittel	mittel	mittel
		Mitarbeiterdaten	✔	hoch	mittel	mittel
		Umsätze	✗	mittel	mittel	hoch
		Ausgaben	✗	mittel	mittel	hoch
	Angebote/Rechnungen	Kundendaten	✔	hoch	mittel	hoch
		Umsätze	✗	mittel	mittel	hoch
	E-Mail	Kundendaten	✔	hoch	mittel	hoch
Rechner Werkstatt	Browser	technische Daten	✗	niedrig	mittel	mittel
	Warenwirtschaft	Lieferantendaten	✗	mittel	mittel	mittel
		Bestandsdaten	✗	niedrig	mittel	mittel
	CAD/CAM	technische Daten	✗	hoch	mittel	hoch
	Zeiterfassung	Mitarbeiterdaten	✔	hoch	mittel	mittel
	E-Mail	Kundendaten	✔	hoch	mittel	hoch
Mobiltelefone Mitarbeiter	E-Mail	Kundendaten	✔	hoch	mittel	hoch
	Browser	technische Daten	✗	niedrig	niedrig	mittel

Drei Blöcke von Maßnahmen sind zu unterscheiden und jeweils zu betrachten



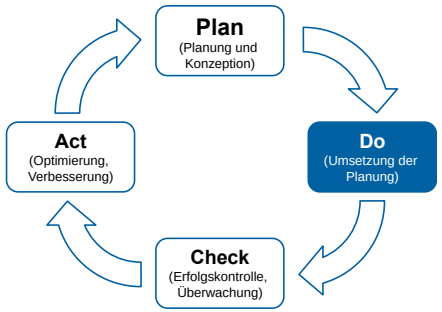


Organisatorische Maßnahmen



- Mitarbeiter unterweisen:
  - Was soll wie gemacht werden?
  - Was soll unterlassen werden?
    (z. B. Private Internetnutzung, E-Mail-Richtlinie, Social-Media, Passwort-Richtlinie, (Wechsel-)Datenträger-Richtlinie, BYOD, Cloud-Speicher-Dienste)
- Mitarbeiter regelmäßig schulen.
- Strikte Trennung von privat und geschäftlich.
- Checklisten für Ein- und Ausstellung von Mitarbeitern.
- Sicherheitsvorfälle ernst nehmen.
- Besucher, Servicekräfte etc. nicht unbeaufsichtigt lassen.
- Notfallplan erstellen und Ernstfälle regelmäßig durchspielen.

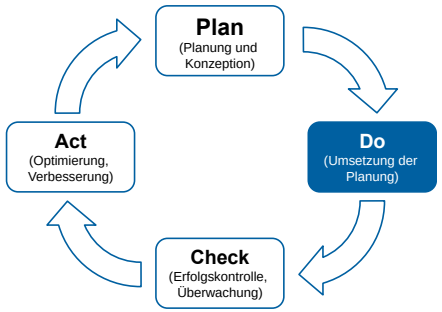
Technische Maßnahmen



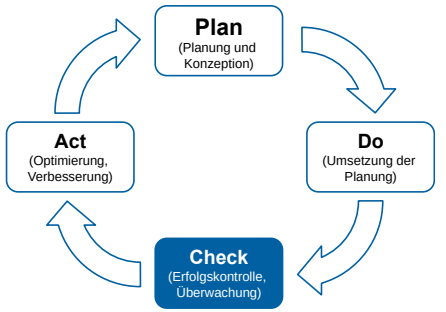
- Ein (nicht mehrere) Virenscanner auf allen Rechnern, Laptops etc.
- Softwareupdates zeitnah einspielen.
- Keine unnötige Software auf den Rechnern, Laptops etc. installieren.
- WLAN absichern (WPA3-Verschlüsselung).
- Need-to-know-Prinzip
  - Jeder sollte nur Zugriff auf die Informationen und Anwendungen haben, die er braucht.
  - Benutzerrollen
  - Keine Administrator-Benutzerkonten
- Regelmäßige Backups erstellen, am besten automatisiert.
- Sensible Daten verschlüsseln.
- Elementarschäden berücksichtigen.

Rechtliche Maßnahmen

- Mit allen (IT-)Dienstleistern schriftliche Verträge über die vereinbarten Leistungen abschließen.
- Vorliegen von Auftragsdatenverarbeitung prüfen.
- Relevante gesetzliche Veränderungen laufend verfolgen.
- Achtung: Eigenes juristisches Wissen nicht überschätzen, sondern im Zweifel lieber einen Spezialisten (z. B. Anwalt) hinzuziehen.

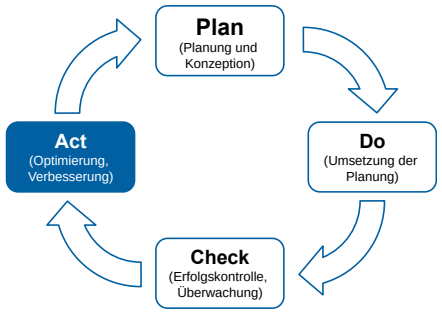


Die Wirksamkeit der Maßnahmen muss kontrolliert werden



- Ist der Virenscanner aktiv und aktuell?
- Ist die verwendete Software auf dem aktuellen (nicht unbedingt auf dem neuesten!) Stand?
- Werden sensible Daten verschlüsselt?
- Funktionieren die Backups und lassen sich die Backups einspielen?
- Halten sich die Mitarbeiter an die Anweisungen/Einschränkungen oder haben sie Wege gefunden die Einschränkungen zu umgehen?
- Funktioniert der Notfallplan?
- Sind nur erlaubten Geräte (Rechner, Laptop etc.) mit dem Unternehmensnetzwerk verbunden?
- etc.

Informationssicherheit ist kein Zustand sondern ein kontinuierlicher Prozess



- Welche Maßnahmen funktionieren, welche nicht?
- Was kann (noch) besser gemacht bzw. gestaltet werden?
- Gibt es neue Prioritäten, Gesetze oder Verträge?
- Auf welche technischen Entwicklungen muss reagiert werden?
  - Smartglasses?
  - Smartwatches?
- Ist die Leistungserbringung der Dienstleister hinsichtlich der Informationssicherheit noch zufriedenstellend?
- etc.

Handlungsempfehlungen und Tipps (1/2)

- ✓ Beziehen Sie ihre Mitarbeiter grundsätzlich immer ein; erklären Sie ihnen warum Sie diese und jene Maßnahme umsetzen.
- ✓ Wenn es etwas zu regeln gibt, dann schreiben Sie es auf, das ist immer besser als eine mündliche Absprache.
- ✓ Idealfall: Verbieten Sie die private Nutzung von dienstlichen Geräten und die Nutzung privater Geräte für dienstliche Zwecke.
- ✓ Versehen Sie alle dienstlichen Geräte zumindest mit einem Passwortschutz. → Minimum acht Zeichen
- ✓ Öffnen Sie niemals Anhänge von E-Mails und Daten unbekannter/ zweifelhafter Herkunft und klicken Sie nicht auf dubiose Internetlinks.

Handlungsempfehlungen und Tipps (2/2)

- ✓ Spielen Sie Updates für verwendete Software (Betriebssystem, Anwendungen, Content-Management-System etc.) zeitnah ein.
- ✓ Achten Sie sorgfältig darauf, welche (IT-)Dienstleister Sie für welche Leistungen (E-Mail, Internetauftritt, Datenauslagerung etc.) auswählen bzw. beauftragen. → möglichst Server in der EU/EWR
- ✓ Lassen Sie besondere Sorgfalt walten, wenn personenbezogene Daten im Spiel sind.
- ✓ Achten Sie bei der Speicherung und Verarbeitung personenbezogener Daten durch Dritte auf eine korrekte, vertraglich fixierte Auftragsdatenverarbeitung (§11 BDSG).
  - ✓ Sie als Auftraggeber sind für die Einhaltung der Gesetzesvorschriften verantwortlich!

04 Datenschutz – Was bedeutet die DSGVO?

BDSG-neu: Bestellung eines Datenschutzbeauftragten

- „Ergänzend zu Artikel 37 Absatz 1 Buchstabe b und c der Verordnung (EU) 2016/679 …
  - … benennen der Verantwortliche und der Auftragsverarbeiter …
  - … eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten, …
  - … soweit sie in der Regel **mindestens zehn Personen** ständig mit der …
  - … automatisierten **Verarbeitung personenbezogener Daten** …

… beschäftigen.“ → §38 BDSG-neu

Quelle: https://dsgvo-gesetz.de/bdsg-neu/38-bdsg-neu

Was bedeutet „Verarbeitung“ von „personenbezogenen Daten“? ■□

- „Im Sinne dieser Verordnung bezeichnet der Ausdruck: […] ‚Verarbeitung‘ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung,

  […] das Löschen oder die Vernichtung;“

  → Art. 4 DSGVO

Quelle: https://dsgvo-gesetz.de/art-4-dsgvo

Was bedeutet „Verarbeitung“ von „personenbezogenen Daten“? ▫■

- „Im Sinne dieser Verordnung bezeichnet der Ausdruck: […] ‚personenbezogene Daten‘„ “ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche **Person angesehen**, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem **Namen**, zu einer **Kennnummer**, zu **Standortdaten**, zu einer **Online-Kennung** […] identifiziert werden kann“

  → Art. 4 DSGVO

Quelle: https://dsgvo-gesetz.de/art-4-dsgvo

DSGVO

Ausgewählte Aspekte!

- **Sehr hohe Bußgelder bei Datenschutz-Verstößen!**
  Die DSGVO sieht vor, dass Verstöße gegen die geltende Verordnung (z.B. Art. 5, 6, 7 oder 9 DSGVO) mit bis zu **4% des weltweiten Konzern-Vorjahresumsatzes** oder bis zu **20 Millionen Euro** geahndet werden können.
- **Nutzer bekommen mehr Rechte!**
  - Auskunftsrecht über die einer Person gespeicherten Daten und dem damit verbundenen Zweck!
  - Recht, die eigenen personenbezogene Benutzerdaten portieren zu können!
  - Nutzer haben zukünftig die Möglichkeit, über sie gespeicherte Daten löschen zu lassen!
- **„Kopplungsverbot“: Entkoppeln Sie Verträge, d.h. holen Sie sich die Einwilligung separat ein.**
- **Auftragsdatenverarbeitung (ADV): Haftung durch Verantwortliche und Auftragsverarbeiter!**

  Art. 28 ff. DSGVO gibt einheitlich vor, wie Daten durch Dritte verarbeitet werden dürfen. Zukünftig sind die sog. **Verantwortlichen** (z. B. Betreiber einer Webpräsenz) für die Datenverarbeitung erster Ansprechpartner für Betroffene. Dieser hat **Auftragsverarbeiter** (z. B. Google) sorgfältig auszuwählen und ist grundsätzlich zur Einhaltung der DSGVO verantwortlich!

Rechenbeispiel:

Online-Shop erzielte im Jahr 2022 einen Umsatz von 500.000 €.
→ 4% entsprechen 20.000 €!

Quelle: https://www.datenschutzbeauftragter-info.de/eu-datenschutzgrundverordnung-das-sind-die-neuerungen
https://www.datenschutzbeauftragter-info.de/auftragsdatenverarbeitung-und-datenschutz-grundverordnung
https://www.datenschutzbeauftragter-info.de/kopplungsverbot-bei-online-gewinnspielen-nach-dsgvo
https://dsgvo-gesetz.de

Ausgewählte Aspekte!

- **Ggf. Pflicht zur Erstellung einer „Datenschutz-Folgeabschätzung“**

  Gemäß Art. 33 DSGVO müssen Verantwortliche im Vorfeld der Verarbeitung von personenbezogenen Daten eine sog. Datenschutz-Folgeabschätzung verfassen, sofern ein **erhebliches Risiko für die Rechte von betroffenen Personen** besteht. Eine Rücksprache mit der zuständigen Aufsichtsbehörde ist ggf. ratsam. → Art. 35 f. DSGVO

  - Beschreibung der Vorgänge in denen personenbezogene Daten verarbeitet werden und deren Zweck
  - Einschätzung der Erfordernis dieser Vorgänge bezogen auf den eigentlichen Zweck
  - Analyse der Risiken im Kontext der Betroffenenrechte (z.B. haben Unbefugte Zugriff auf pers.bez. Daten erlangt)
  - Auflistung geeigneter Maßnahmen zur Abwendung von Risiken

- **Mindestalter zum Einverständnis der Verarbeitung personenbezogener Daten steigt auf 16!**

- **Stärkere Integration der Informationssicherheit zum Schutz personenbezogener Daten!**
  „Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen (‚Integrität und Vertraulichkeit‘)“
  → Art. 5 Abs. 1 lit. f) DSGVO

- **Nachweis zur Einhaltung des Schutzes personenbezogener Daten**
  Rechenschaftspflicht! → Art. 5 (2) DSGVO

Quelle: https://www.datenschutzbeauftragter-info.de/eu-datenschutzgrundverordnung-das-sind-die-neuerungen
https://www.datenschutzbeauftragter-info.de/auftragsdatenverarbeitung-und-datenschutz-grundverordnung
https://dsgvo-gesetz.de

DSGVO & BDSG-neu: Was nun zu tun ist!

- ✓ **Grundsätzlich: Datenschutz ist Chefsache!**
- ✓ **Bestellung einer/eines DSB** (falls erforderlich)
- ✓ **Verfahrensverzeichnis** (Fokus: Zweck und Dauer der Verarbeitung personenbezogener Daten)
  - Verwaltung von Kundendaten, z. B. Rechnungsausgangsprozess; Personalaktenführung; …
  - Registrierung für Newsletter
  - …
- ✓ **Vervollständigung bzw. Optimierung des Datenschutz-Konzepts**
  - Nachweise zu Mitarbeiter-Schulungen
  - Einforderung von Verträgen zur Auftragsdatenverarbeitung (ADV), z.B. Google Analytics
  - Ggf. Überarbeitung der veröffentlichten Informationen zum Datenschutz
  - Ablauf-Beschreibung: Betroffen-Auskunftsrechte, Recht auf Löschung von Daten, …
  - …
- ✓ **Dokumentation von Maßnahmen zur Gewährleistung der Informationssicherheit**
- ✓ **Datenschutz-Folgeabschätzung** (falls erforderlich)

Tipp: Prüfen Sie Ihre Prozesse!
Wozu werden welche Daten von wem verarbeitet und wie lange werden diese gespeichert?

Praxis-Tipp: Informieren Sie sich regelmäßig bei Ihrem zuständigen Landesamt für Datenschutzaufsicht

Quelle: www.baden-wuerttemberg.datenschutz.de

Vielen Dank für Ihre Aufmerksamkeit!

ibi research an der Universität Regensburg GmbH

Galgenbergstr. 25

93053 Regensburg

Tel.: 0941 943-1901

Fax: 0941 943-1888

E-Mail: info@ibi.de

ERFOLGREICH HANDELN

Bayerisches Staatsministerium für Wirtschaft, Landesentwicklung und Energie