



INTELLIGENT SECURITY HANDWERK

Weiterbildungsreihe für Handwerksbetriebe

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

Mittelstand-
Digital 

Inhaltsverzeichnis

1. Einführung in den Datenschutz

- Grundlagen des Datenschutzes
- Bedeutung und Notwendigkeit von Datenschutz

2. Die Datenschutz-Grundverordnung (DSGVO)

- Grundprinzipien und Anwendungsbereich
- Rechte der betroffenen Personen
- Rolle und Pflichten des Datenschutzbeauftragten
- Maßnahmen bei Datenschutzverletzungen und Sanktionen

3. Was sind personenbezogene Daten?

- Definition und besondere Kategorien
- Beispiele und rechtliche Grundlagen

Inhaltsverzeichnis

4. Verarbeitung personenbezogener Daten

- Definition und Anwendungsbeispiele
- Datenschutzprinzipien: Rechtmäßigkeit, Datenminimierung, Integrität, etc.
- Beispiele Datenschutzverletzungen

5. Datenschutz am Arbeitsplatz

- Umgang mit Mitarbeiterdaten
- Überwachungsmaßnahmen
- Bring Your Own Device (BYOD): Risiken und Regelungen

6. Datenschutz in sozialen Medien

- Risiken durch Social-Media-Nutzung
- Maßnahmen zur Risikominimierung

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

Inhaltsverzeichnis

7. Datenschutz bei WhatsApp und Alternativen

- Datenschutzprobleme bei WhatsApp
- Alternativen: Threema, Signal, Teamwire

8. Datenschutz in der Cloud

- Vorteile und Herausforderungen
- Sicherheitsmaßnahmen und Anbieter

9. Domain-Datenschutz

- Datenschutz bei der Domain-Registrierung
- Sicherheitsmaßnahmen für Webseiten und Online-Präsenzen

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

Inhaltsverzeichnis

10. Datenschutz und Kameradrohnen

- Einsatzbeispiele und Risiken
- Best Practices und Datenschutzkonzepte

11. Datenschutz und Künstliche Intelligenz (KI)

- Nutzung von KI im Handwerksbereich
- Datenschutzanforderungen und ethische Überlegungen

12. Beispiele für Datenschutzverletzungen bei Firmen

- Vorfälle und Konsequenzen

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

1. Einführung in den Datenschutz

Datenschutz bezieht sich auf den Schutz personenbezogener Daten vor unbefugtem Zugriff, Nutzung oder Verbreitung.

Es umfasst rechtliche, technische und organisatorische Maßnahmen, die darauf abzielen, sicherzustellen, dass personenbezogene Daten angemessen gesammelt, verarbeitet, gespeichert und übertragen werden, um die Privatsphäre und die Rechte der betroffenen Personen zu wahren.

Der Datenschutz regelt, wie Unternehmen, Organisationen und Behörden mit personenbezogenen Informationen umgehen dürfen, und schützt Einzelpersonen vor Missbrauch oder unerwünschter Offenlegung ihrer persönlichen Daten.

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

1. Einführung in den Datenschutz

Warum Datenschutz wichtig ist

1. Schutz der Privatsphäre: Datenschutz gewährleistet, dass persönliche Informationen, die eine Person preisgibt, angemessen geschützt werden. Jeder hat das Recht auf Privatsphäre, und Datenschutzbestimmungen sollen sicherstellen, dass persönliche Daten nicht missbräuchlich verwendet oder unerlaubt weitergegeben werden.

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

1. Einführung in den Datenschutz

Warum Datenschutz wichtig ist

2. Vertrauen und Glaubwürdigkeit: Organisationen, die sich aktiv um Datenschutz bemühen, gewinnen das Vertrauen ihrer Kunden. Durch die Sicherstellung, dass persönliche Informationen sicher und geschützt sind, stärken Unternehmen und Institutionen ihre Glaubwürdigkeit und Reputation.

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

1. Einführung in den Datenschutz

Warum Datenschutz wichtig ist

3. Schutz vor Identitätsdiebstahl: Wenn persönliche Daten in die falschen Hände geraten, kann dies zu Identitätsdiebstahl führen. Kriminelle könnten gestohlene Informationen verwenden, um Konten zu hacken, betrügerische Aktivitäten durchzuführen oder persönliche Identitäten zu missbrauchen. Datenschutzmaßnahmen helfen dabei, solche Risiken zu minimieren.

1. Einführung in den Datenschutz

Warum Datenschutz wichtig ist

4. Wahrung der individuellen Freiheit: Datenschutz ist eng mit dem Recht auf freie Meinungsäußerung und individuelle Freiheit verbunden. Wenn Menschen das Gefühl haben, dass ihre persönlichen Informationen ohne ihre Zustimmung überwacht oder verwendet werden, kann dies ihre Fähigkeit beeinträchtigen, frei zu denken, zu sprechen und zu handeln, ohne befürchten zu müssen, überwacht oder beeinflusst zu werden.

1. Einführung in den Datenschutz

Warum Datenschutz wichtig ist

5. Regulierung : Viele Länder haben Gesetze und Vorschriften zum Schutz der Privatsphäre und persönlicher Daten erlassen. Unternehmen und Organisationen müssen diese Gesetze einhalten, um rechtliche Konsequenzen zu vermeiden. Datenschutzbestimmungen wie die DSGVO (Datenschutz-Grundverordnung) in Europa oder der California Consumer Privacy Act in den USA legen fest, wie personenbezogene Daten gesammelt, gespeichert und verarbeitet werden dürfen.

1. Einführung in den Datenschutz

Warum Datenschutz wichtig ist

Fazit: Datenschutz ist ein grundlegendes Recht, das eng mit dem Schutz der Privatsphäre, der individuellen Freiheit und dem Vertrauen in Institutionen und Technologien verbunden ist. Es ist von entscheidender Bedeutung, dass Unternehmen, Organisationen und Regierungen Maßnahmen ergreifen, um die Privatsphäre und Sicherheit persönlicher Daten zu gewährleisten und so das Vertrauen der Öffentlichkeit zu stärken.

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

2. Die Datenschutz-Grundverordnung (DSGVO)

Die Datenschutz-Grundverordnung (DSGVO) ist eine EU-Verordnung, die am 25. Mai 2018 in Kraft getreten ist und die Datenschutzgesetze in allen EU-Mitgliedstaaten vereinheitlicht. Die grundlegenden Aspekte der DSGVO betreffen:

Einwilligung: Die DSGVO legt strenge Anforderungen an die Einholung von Einwilligungen zur Verarbeitung personenbezogener Daten fest. Einwilligungen müssen freiwillig, spezifisch, informiert und eindeutig sein.

Anwendungsbereich: Die DSGVO gilt für alle Unternehmen, die personenbezogene Daten von EU-Bürgern verarbeiten, unabhängig davon, ob das Unternehmen in der EU ansässig ist oder nicht.

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

2. Die Datenschutz-Grundverordnung (DSGVO)

Die DSGVO

Die Datenschutz-Grundverordnung (DSGVO) ist eine EU-Verordnung, die am 25. Mai 2018 in Kraft getreten ist und die Datenschutzgesetze in allen EU-Mitgliedstaaten vereinheitlicht. Die grundlegenden Aspekte der DSGVO betreffen:

Grundsätze der Datenverarbeitung: Die DSGVO legt eine Reihe von Grundsätzen fest, die bei der Verarbeitung personenbezogener Daten beachtet werden müssen. Dazu gehören Rechtmäßigkeit, Fairness und Transparenz; Zweckbindung; Datenminimierung; Richtigkeit; Speicherbegrenzung; Integrität und Vertraulichkeit; sowie Rechenschaftspflicht.

2. Die Datenschutz-Grundverordnung (DSGVO)

Die DSGVO

Die Datenschutz-Grundverordnung (DSGVO) ist eine EU-Verordnung, die am 25. Mai 2018 in Kraft getreten ist und die Datenschutzgesetze in allen EU-Mitgliedstaaten vereinheitlicht. Die grundlegenden Aspekte der DSGVO betreffen:

Datenschutzbeauftragter: In einigen Fällen müssen Unternehmen einen Datenschutzbeauftragten ernennen, insbesondere wenn sie in großem Umfang personenbezogene Daten verarbeiten. Nach § 38 Abs. BDSG ist ergänzend zu den Vorgaben der DSGVO ein Datenschutzbeauftragter zu benennen, soweit in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung (am PC oder Handy) personenbezogener Daten beschäftigt sind.

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

2. Die Datenschutz-Grundverordnung (DSGVO)

Die DSGVO

Die Datenschutz-Grundverordnung (DSGVO) ist eine EU-Verordnung, die am 25. Mai 2018 in Kraft getreten ist und die Datenschutzgesetze in allen EU-Mitgliedstaaten vereinheitlicht. Die grundlegenden Aspekte der DSGVO betreffen:

Rechte der betroffenen Personen: Die DSGVO stärkt die Rechte von Einzelpersonen in Bezug auf ihre personenbezogenen Daten. Dazu gehören das Recht auf Auskunft, das Recht auf Berichtigung, das Recht auf Löschung ("Recht auf Vergessenwerden"), das Recht auf Einschränkung der Verarbeitung, das Recht auf Datenübertragbarkeit und das Widerspruchsrecht.

2. Die Datenschutz-Grundverordnung (DSGVO)

Die DSGVO

Die Datenschutz-Grundverordnung (DSGVO) ist eine EU-Verordnung, die am 25. Mai 2018 in Kraft getreten ist und die Datenschutzgesetze in allen EU-Mitgliedstaaten vereinheitlicht. Die grundlegenden Aspekte der DSGVO betreffen:

Meldung von Datenschutzverletzungen: Unternehmen sind verpflichtet, Datenschutzverletzungen innerhalb von 72 Stunden nach ihrer Entdeckung an die zuständige Aufsichtsbehörde zu melden. (Meldung erfolgt via Formular beim hessischen Beauftragten für Datenschutz)

2. Die Datenschutz-Grundverordnung (DSGVO)

Die DSGVO

Die Datenschutz-Grundverordnung (DSGVO) ist eine EU-Verordnung, die am 25. Mai 2018 in Kraft getreten ist und die Datenschutzgesetze in allen EU-Mitgliedstaaten vereinheitlicht. Die grundlegenden Aspekte der DSGVO betreffen:

Sanktionen: Bei Verstößen gegen die DSGVO können Geldstrafen von bis zu 20 Millionen Euro oder bis zu 4 % des weltweiten Jahresumsatzes eines Unternehmens verhängt werden, je nachdem, welcher Betrag höher ist.

Meldeformular Datenschutzverletzung

Meldeformular

3. Was sind personenbezogene Daten?

Personenbezogene Daten sind „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen“ (Art. 4 Abs. 1 DSGVO).

Wenn sich durch einzelne Informationen zusammen eine Person identifizieren lässt, dann muss die DSGVO ebenfalls angewendet werden.

Beispiele für personenbezogene Daten:

Name und Vorname
eine Privatanschrift
eine IP-Adresse

3. Was sind personenbezogene Daten?

Es gibt besondere Kategorien von personenbezogenen Daten, deren Verarbeitung grundsätzlich **untersagt** ist.

Dazu gehören:

- „rassische und ethnische Herkunft“
- „politische Meinungen“
- „religiöse oder weltanschauliche Überzeugungen“
- „Gewerkschaftszugehörigkeit“
- „genetische Daten“
- „biometrische Daten“
- „Gesundheitsdaten“
- „Daten zum Sexualleben oder der sexuellen Orientierung“ (Art. 9 Abs. 1 DSGVO)

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

3. Was sind personenbezogene Daten?

In Ausnahmefällen können auch diese Daten verarbeitet werden. Nämlich, wenn die betroffene Person ausdrücklich zu einem oder mehreren Zwecken der Verarbeitung zugestimmt hat oder wenn es feststehende Bestimmungen gibt, die in Art. 9 DSGVO vorgeschrieben sind.

Beispielsweise die Sicherung existenzieller Bedürfnisse. Wenn Daten der besonderen Kategorie verarbeitet werden, dann muss ein Verzeichnis angelegt werden, das sowohl alle Verarbeitungstätigkeiten und ihre Zuständigkeiten aufführt als auch die Personen, die die Daten verarbeiten.

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

4. Verarbeitung personenbezogener Daten

Wie die Daten verarbeitet werden, also digital oder analog, spielt dabei keine Rolle.
Der Schutz der DSGVO gilt für alle Verarbeitungstechniken.

Dazu gehören Vorgänge, wie „das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;“ (Art. 4 Abs. 2 DSGVO)

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

4. Verarbeitung personenbezogener Daten

Wichtige Begriffe



Betroffene Person:
Identifizierbare, natürliche Personen, deren
personenbezogene Daten verarbeitet werden
(Art 4 Abs. 1 DSGVO).



Verantwortlicher:
„Eine natürliche oder juristische Person oder Behörde,
Einrichtung oder andere Stelle, die allein oder gemeinsam
mit anderen über die Zwecke und Mittel der Verarbeitung
von personenbezogenen Daten entscheidet.“
(Art 4 Abs.7 DSGVO).



Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

4. Verarbeitung personenbezogener Daten

Datenschutzprinzipien

Die Datenschutzprinzipien sind Grundsätze, die den Umgang mit personenbezogenen Daten regeln. Sie dienen dazu, die Privatsphäre und die Rechte der Personen zu schützen, deren Daten verarbeitet werden.

Rechtmäßigkeit, Fairness und Transparenz: Die Verarbeitung personenbezogener Daten sollte auf rechtmäßige und in einer fairen und transparenten Weise erfolgen. Personen sollten darüber informiert werden, wie ihre Daten verwendet werden.

Gefördert durch:



4. Verarbeitung personenbezogener Daten

Datenschutzprinzipien

Die Datenschutzprinzipien sind Grundsätze, die den Umgang mit personenbezogenen Daten regeln. Sie dienen dazu, die Privatsphäre und die Rechte der Personen zu schützen, deren Daten verarbeitet werden.

Integrität und Vertraulichkeit: Personenbezogene Daten sollten auf eine Weise verarbeitet werden, die angemessene Sicherheit gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung sowie vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung.

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

4. Verarbeitung personenbezogener Daten

Datenschutzprinzipien

Die Datenschutzprinzipien sind Grundsätze, die den Umgang mit personenbezogenen Daten regeln. Sie dienen dazu, die Privatsphäre und die Rechte der Personen zu schützen, deren Daten verarbeitet werden.

Richtigkeit: Personenbezogene Daten sollten korrekt und gegebenenfalls auf dem neuesten Stand gehalten werden. Maßnahmen sollten ergriffen werden, um unrichtige oder unvollständige Daten zu korrigieren oder zu löschen.

4. Verarbeitung personenbezogener Daten

Datenschutzprinzipien

Die Datenschutzprinzipien sind Grundsätze, die den Umgang mit personenbezogenen Daten regeln. Sie dienen dazu, die Privatsphäre und die Rechte der Personen zu schützen, deren Daten verarbeitet werden.

Datenminimierung: Es sollten nur diejenigen personenbezogenen Daten erhoben werden, die für die jeweiligen Zwecke erforderlich sind, und sie sollten auf das notwendige Minimum beschränkt werden.

4. Verarbeitung personenbezogener Daten

Datenschutzprinzipien

Die Datenschutzprinzipien sind Grundsätze, die den Umgang mit personenbezogenen Daten regeln. Sie dienen dazu, die Privatsphäre und die Rechte der Personen zu schützen, deren Daten verarbeitet werden.

Zweckbindung: Personenbezogene Daten sollten nur für festgelegte, eindeutige und legitime Zwecke erhoben und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverarbeitet werden.

4. Verarbeitung personenbezogener Daten

Datenschutzprinzipien

Die Datenschutzprinzipien sind Grundsätze, die den Umgang mit personenbezogenen Daten regeln. Sie dienen dazu, die Privatsphäre und die Rechte der Personen zu schützen, deren Daten verarbeitet werden.

Rechenschaftspflicht: Der Verantwortliche für die Datenverarbeitung ist verpflichtet, die Einhaltung der Datenschutzprinzipien nachzuweisen. Gegebenenfalls muss die Einhaltung von Gesetzen und Vorschriften gegenüber den Datenschutzbehörden nachgewiesen werden.

4. Verarbeitung personenbezogener Daten

Beispiele Datenschutzverletzungen

Verlust oder Diebstahl von Kundendaten: Ein Handwerksbetrieb könnte Opfer eines Einbruchs oder Diebstahls werden, bei dem physische oder digitale Datenträger gestohlen werden, die persönliche Informationen von Kunden enthalten. Dies könnte Namen, Adressen, Telefonnummern oder sogar Zahlungsinformationen umfassen.

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

4. Verarbeitung personenbezogener Daten

Beispiele Datenschutzverletzungen

Unbefugter Zugriff auf Kundendaten: Mitarbeiter des Handwerksbetriebs könnten unbefugt auf Kundendaten zugreifen, entweder aus Neugier oder in betrügerischer Absicht. Dies könnte zu Datenschutzverletzungen führen, wenn sensible Informationen ohne Genehmigung eingesehen oder weitergegeben werden.

4. Verarbeitung personenbezogener Daten

Beispiele Datenschutzverletzungen

Mangelnde Datensicherheit bei der Speicherung: Wenn ein Handwerksbetrieb nicht angemessene Sicherheitsmaßnahmen für die Speicherung von Kundendaten implementiert hat, könnten diese Daten durch einen Cyberangriff oder eine Datenpanne kompromittiert werden. Dies könnte durch unsichere Netzwerke, ungeschützte Geräte oder fehlende Verschlüsselung verursacht werden.

4. Verarbeitung personenbezogener Daten

Beispiele Datenschutzverletzungen

Unbefugte Weitergabe von Daten an Dritte: Ein Handwerksbetrieb könnte versehentlich oder absichtlich Kundendaten an Dritte weitergeben, ohne die erforderliche Einwilligung der betroffenen Personen einzuholen. Dies könnte geschehen, wenn beispielsweise Daten an externe Dienstleister oder Partnerunternehmen übermittelt werden, ohne angemessene Datenschutzvereinbarungen zu treffen.

4. Verarbeitung personenbezogener Daten

Beispiele Datenschutzverletzungen

Mangelnde Aufbewahrung und Vernichtung von Daten: Wenn ein Handwerksbetrieb keine klaren Richtlinien für die Aufbewahrung und Vernichtung von Kundendaten hat, könnten veraltete oder unnötige Informationen weiterhin gespeichert werden, was ein Risiko für Datenschutzverletzungen darstellt. Daten sollten ordnungsgemäß vernichtet werden, sobald sie nicht mehr benötigt werden, um unbefugten Zugriff zu verhindern.

5. Datenschutz am Arbeitsplatz

Da am Arbeitsplatz oftmals personenbezogene Daten, wie z. B. Name, Anschrift und Kontodaten erhoben, verarbeitet und übermittelt werden, besteht ein hohes Risiko für die Wahrung der Datensicherheit.

Um diese personenbezogenen Daten zu schützen, haben Arbeitgeber umfangreiche Vorkehrungen zu schaffen, umzusetzen und in regelmäßigen Abständen zu überprüfen.

Damit der Schutz der Daten so gut wie möglich gewährleistet ist, sind auch Arbeitnehmer zur Mitwirkung verpflichtet.

5. Datenschutz am Arbeitsplatz

Arten der Überwachung am Arbeitsplatz

Videoüberwachung: Die Videoüberwachung am Arbeitsplatz ist nur unter strengen Bedingungen zulässig. Sie muss gerechtfertigt sein, zum Beispiel zum Schutz vor Diebstahl oder zur Sicherung von Gebäuden und Anlagen. Eine verdeckte Überwachung ist in der Regel unzulässig und nur in Ausnahmefällen erlaubt.

E-Mail- und Internetüberwachung: Die Überwachung der E-Mail- und Internetnutzung der Mitarbeiter muss klar geregelt sein. Arbeitgeber sollten transparente Richtlinien aufstellen und die Mitarbeiter über die Art und den Umfang der Überwachung informieren.

5. Datenschutz am Arbeitsplatz

Arten der Überwachung am Arbeitsplatz

Rechte der Arbeitnehmer

GPS-Überwachung: Bei Mitarbeitern, die im Außendienst tätig sind, kann die GPS-Überwachung sinnvoll sein. Auch hier müssen die Mitarbeiter informiert und die Maßnahme gerechtfertigt sein.

5. Datenschutz am Arbeitsplatz

Arten der Überwachung am Arbeitsplatz

Pflichten der Arbeitnehmer

Rechtfertigung und Verhältnismäßigkeit: Jede Form der Überwachung muss gerechtfertigt und verhältnismäßig sein. Es muss ein legitimer Grund vorliegen, und die Maßnahme darf nicht über das notwendige Maß hinausgehen.

Datensicherheit: Arbeitgeber müssen sicherstellen, dass die gesammelten Daten sicher gespeichert und vor unbefugtem Zugriff geschützt sind.

Dokumentation und Rechenschaftspflicht: Arbeitgeber sollten alle Überwachungsmaßnahmen dokumentieren und in der Lage sein, deren Rechtmäßigkeit nachzuweisen.

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

5. Datenschutz am Arbeitsplatz

BYOD (Bring Your Own Device)

Bring Your Own Device (BYOD) ist ein Konzept und eine Praxis in Unternehmen und Organisationen, bei dem Mitarbeiter ihre eigenen persönlichen Geräte wie Laptops, Smartphones, Tablets oder andere mobile Geräte am Arbeitsplatz verwenden, um auf Unternehmensressourcen und -daten zuzugreifen.

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

5. Datenschutz am Arbeitsplatz

Risiken von Bring Your Own Device (BYOD)

Sicherheitsrisiken: Persönliche Geräte sind möglicherweise nicht so gut gesichert wie Firmenhardware, was zu Sicherheitslücken und Datenverlust führen kann.

Datenschutzprobleme: Es besteht die Gefahr, dass sensible Unternehmensdaten auf privaten Geräten gespeichert und nicht ausreichend geschützt werden.

Compliance und rechtliche Herausforderungen: BYOD kann es schwierig machen, gesetzliche und regulatorische Anforderungen bezüglich Datenschutz und Datensicherheit einzuhalten.

5. Datenschutz am Arbeitsplatz

Risiken von Bring Your Own Device (BYOD)

Kontrollverlust: Unternehmen haben weniger Kontrolle über persönliche Geräte, was zu Schwierigkeiten bei der Durchsetzung von Richtlinien und der Verwaltung von Updates und Patches führen kann.

Kosten für Sicherheitsmaßnahmen: Um die Sicherheitsrisiken zu minimieren, müssen möglicherweise zusätzliche Sicherheitslösungen und -maßnahmen implementiert werden, was zusätzliche Kosten verursachen kann.

5. Datenschutz am Arbeitsplatz

Risiken von Bring Your Own Device (BYOD)

IT-Support und Kompatibilität: Die Vielzahl unterschiedlicher Geräte und Betriebssysteme kann den IT-Support komplizierter machen und Kompatibilitätsprobleme verursachen.

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

5. Datenschutz am Arbeitsplatz

Fazit Bring Your Own Device

BYOD kann sowohl Vorteile als auch Risiken mit sich bringen. Unternehmen sollten eine umfassende BYOD-Richtlinie erstellen, die Sicherheitsmaßnahmen, Datenschutz, Compliance und IT-Support berücksichtigt, um die Vorteile zu maximieren und die Risiken zu minimieren.

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

6. Datenschutz in sozialen Medien

Die Nutzung von Social Media birgt für Unternehmen, einschließlich Handwerksbetriebe, verschiedene Datenschutz- und Datensicherheitsrisiken. Hier sind einige der wichtigsten Aspekte:

Datenlecks: Durch die Interaktion mit Kunden und die Veröffentlichung von Inhalten auf Social-Media-Plattformen können sensible Unternehmensdaten versehentlich preisgegeben werden.

Datenmissbrauch: Informationen über Kunden, Mitarbeiter oder interne Geschäftsprozesse könnten von Dritten missbraucht werden, sei es für Identitätsdiebstahl, Phishing-Angriffe oder andere Formen von Betrug.

5. Datenschutz am Arbeitsplatz

Die Nutzung von Social Media birgt für Unternehmen, einschließlich Handwerksbetriebe, verschiedene Datenschutz- und Datensicherheitsrisiken. Hier sind einige der wichtigsten Aspekte:

Datenschutzverletzungen: Wenn ein Unternehmen personenbezogene Daten seiner Kunden auf Social-Media-Plattformen sammelt, speichert oder verarbeitet, muss es sicherstellen, dass dies den geltenden Datenschutzbestimmungen entspricht, wie z.B. der DSGVO in der Europäischen Union. Auch muss ein Unternehmen die Rechte einfordern, ein Kundenobjekt auf Social-Media veröffentlichen zu dürfen.

5. Datenschutz am Arbeitsplatz

Die Nutzung von Social Media birgt für Unternehmen, einschließlich Handwerksbetriebe, verschiedene Datenschutz- und Datensicherheitsrisiken. Hier sind einige der wichtigsten Aspekte:

Phishing und Social Engineering: Social Media ist oft ein Tummelplatz für Phishing-Angriffe und Social Engineering, bei denen Betrüger versuchen, sensible Informationen von Mitarbeitern oder Kunden zu stehlen, indem sie sich als vertrauenswürdige Kontakte ausgeben.

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

5. Datenschutz am Arbeitsplatz

Risikominimierung

Um diese Risiken zu minimieren, sollten Unternehmen und Handwerksbetriebe folgende Maßnahmen ergreifen:

Klare Richtlinien zur Nutzung von Social Media für Mitarbeiter erstellen und schulen, die festlegen, welche Informationen das Unternehmen sammelt, wie sie verwendet werden und wie sie geschützt werden.

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

5. Datenschutz am Arbeitsplatz

Risikominimierung

Um diese Risiken zu minimieren, sollten Unternehmen und Handwerksbetriebe folgende Maßnahmen ergreifen:

Regelmäßige Überprüfung der Datenschutzrichtlinien und Sicherheitsvorkehrungen für die Verwaltung von Kundendaten.

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

5. Datenschutz am Arbeitsplatz

Risikominimierung

Um diese Risiken zu minimieren, sollten Unternehmen und Handwerksbetriebe folgende Maßnahmen ergreifen:

Zugriffskontrolle einschränken: Verwenden Sie starke Passwörter und Zwei-Faktor-Authentifizierung für Social-Media-Konten und vermeiden Sie die gemeinsame Nutzung von Anmeldedaten.

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

5. Datenschutz am Arbeitsplatz

Risikominimierung

Um diese Risiken zu minimieren, sollten Unternehmen und Handwerksbetriebe folgende Maßnahmen ergreifen:

Berechtigungen verwalten: Definieren Sie Rollen und Berechtigungen innerhalb des Unternehmens für den Zugriff auf und die Verwaltung von Social-Media-Konten. Begrenzen Sie den Zugriff auf sensible Informationen nur auf diejenigen, die sie benötigen.

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

5. Datenschutz am Arbeitsplatz

Risikominimierung

Um diese Risiken zu minimieren, sollten Unternehmen und Handwerksbetriebe folgende Maßnahmen ergreifen:

Vertrauliche Informationen schützen: Vermeiden Sie die Veröffentlichung von vertraulichen Unternehmensinformationen auf öffentlichen sozialen Medien. Sensibilisieren Sie Mitarbeiter für die Risiken und die richtige Handhabung von vertraulichen Informationen.

5. Datenschutz am Arbeitsplatz

Risikominimierung

Um diese Risiken zu minimieren, sollten
Unternehmen und Handwerksbetriebe folgende
Maßnahmen ergreifen:

Regelmäßige Schulungen und Sensibilisierung der Mitarbeiter für Phishing-
und Social-Engineering-Angriffe.

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

5. Datenschutz am Arbeitsplatz

Risikominimierung

Um diese Risiken zu minimieren, sollten Unternehmen und Handwerksbetriebe folgende Maßnahmen ergreifen:

Fazit: Durch eine proaktive Herangehensweise können Unternehmen die Vorteile von Social Media nutzen, während sie gleichzeitig die damit verbundenen Risiken minimieren.

7. Datenschutz bei WhatsApp und Alternativen

Warum sind die WhatsApp App und WhatsApp Business App nicht DSGVO-konform?

- WhatsApp verarbeitet Metadaten, die DSGVO-relevant sein können.
- WhatsApp hat in den Standardeinstellungen Zugriff auf Kontaktdaten.
- WhatsApp speichert Backups in den Standardeinstellung unverschlüsselt.
- WhatsApp speichert Nachrichten, die nicht zugestellt werden konnten, vorübergehend auf den eigenen Servern zwischen.

7. Datenschutz bei WhatsApp und Alternativen

Was sind Metadaten?

- Standort
- Uhrzeit
- Profilbilder
- Profilnamen
- Profilbeschreibungen
- Gerätenamen
- **Kontakte**

Gefördert durch:



Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

7. Datenschutz bei WhatsApp und Alternativen

Datenschutz bei WhatsApp

3 mögliche Alternativen:

Threema: Diese WhatsApp-Alternative ist ein Schweizer Messenger-Dienst mit über 8 Millionen Nutzer:innen. Der Nachrichtenaustausch kann hier völlig anonym erfolgen, also ohne Übermittlung von personenbezogenen Daten. Speziell für Unternehmen gibt es Threema Work.

Signal: Signal ist ein sehr datensparsamer Messenger, der ebenfalls Ende-zu-Ende verschlüsselt arbeitet. Durch das angewandte „Zero-Knowledge-Prinzip“ wird sichergestellt, dass die Betreiber:innen keinerlei Zugriff auf die Daten der Nutzer:innen haben.

7. Datenschutz bei WhatsApp und Alternativen

Datenschutz bei WhatsApp

3 mögliche Alternativen:

Teamwire: Der deutsche Messenger-Dienst Teamwire ist speziell auf die Sicherheits- und Datenschutzbedürfnisse von Behörden, Institutionen und Organisationen ausgelegt.

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

8. Datenschutz in der Cloud

Cloud Computing ist die Bereitstellung von Rechenressourcen
(Server, Speicher, Datenbanken, Netzwerkkomponenten oder Software)
über das Internet ("die Cloud")

8. Datenschutz in der Cloud

Vorteile durch Cloud-Nutzung:

Skalierbarkeit und Flexibilität

Datenmanagement: Cloud-Services ermöglichen eine einfache Skalierung von Speicherplatz und Rechenleistung. Unternehmen können schnell auf veränderte Anforderungen reagieren, ohne in teure Hardware investieren zu müssen.

Flexibilität: Daten können von überall aus und zu jeder Zeit abgerufen werden, was die Zusammenarbeit und Produktivität erhöht.

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

8. Datenschutz in der Cloud

Vorteile durch Cloud-Nutzung:

Kostenersparnis

Infrastrukturkosten: Unternehmen sparen durch die Nutzung von Cloud-Services die Kosten für den Aufbau und die Wartung eigener Server.

Aktualität

Aktuelle Technologien: Cloud-Provider stellen regelmäßig Updates bereit, sodass Nutzer immer von den neuesten Technologien und Sicherheitsstandards profitieren.

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

8. Datenschutz in der Cloud

Nachteile durch Cloud-Nutzung:

Datenschutz

Datenkontrolle: Unternehmen geben einen Teil der Kontrolle über ihre Daten an den Cloud-Anbieter ab. Dies kann insbesondere in Branchen mit hohen Datenschutzanforderungen problematisch sein.

Rechtskonformität: Cloud-Anbieter haben oft Server in verschiedenen Ländern, was die Einhaltung regionaler Datenschutzgesetze wie der DSGVO erschweren kann.

8. Datenschutz in der Cloud

Nachteile durch Cloud-Nutzung:

Datenverletzungen

Cloud-Services sind attraktive Ziele für Cyberangriffe. Daten können bei Sicherheitsvorfällen kompromittiert werden.

Verfügbarkeit

Die Abhängigkeit von der Internetverbindung und der Verfügbarkeit der Dienste des Anbieters kann zu Ausfallzeiten führen.

Eingeschränkte Sichtbarkeit

Unternehmen haben möglicherweise nicht die gleiche Transparenz und Kontrolle über Sicherheitsmaßnahmen und Datenmanagementprozesse des Cloud-Anbieters.

Gefördert durch:

8. Datenschutz in der Cloud

Tipps für die Nutzung:

Verschlüsselung im Ruhezustand und während der Übertragung: sicherstellen, dass Daten sowohl bei der Übertragung als auch im Ruhezustand verschlüsselt werden.

Ende-zu-Ende-Verschlüsselung: Dienste nutzen, die Ende-zu-Ende-Verschlüsselung bieten, um sicherzustellen, dass nur autorisierte Nutzer Zugriff auf die Daten haben.

Sicherheitszertifizierungen: Cloud-Anbieter wählen, die über anerkannte Sicherheitszertifizierungen verfügen (z.B. ISO 27001, SOC 2)

8. Datenschutz in der Cloud

Tipps für die Nutzung:

Starke Authentifizierung: Multi-Faktor-Authentifizierung implementieren, um den Zugang zu sensiblen Daten zu schützen.

Zugriffsrechte: Zugang zu Daten auf Basis der Rolle des Mitarbeiters und den notwendigen Berechtigungen beschränken.

Anonymisierung: persönlich identifizierbare Informationen aus Datensätzen, wenn sie für Analysezwecke oder Tests verwendet werden entfernen.

Vertragsprüfung: Verträge und Datenschutzvereinbarungen mit Cloud-Anbietern überprüfen, um sicherzustellen, dass sie den gesetzlichen Anforderungen entsprechen.

8. Datenschutz in der Cloud

Beispiele für sichere Anbieter

pCloud: pCloud hat seinen Sitz in der Schweiz und unterliegt der entsprechenden Gesetzgebung. Gleichzeitig ist pCloud vollends DSGVO-konform. Auch die Lage der Rechenzentren und deren ISO-Zertifizierung kommen den Anwendern zugute.

HiDrive von Strato: HiDrive speichert Daten ebenfalls DSGVO-konform in Rechenzentren, die sich ausschließlich in Deutschland befinden und entsprechend ISO zertifiziert sind. Optional kann bei diesem Anbieter auch eine „Ende-zu-Ende“-Verschlüsselung sowie eine Zwei-Faktor-Authentifizierung aktiviert werden.

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

9. Domain-Datenschutz

Datenschutz im Bereich von Domains für Handwerksbetriebe ist ein wichtiger Aspekt, den es zu berücksichtigen gilt, um die persönlichen Daten von Kunden, Mitarbeitern und Geschäftspartnern zu schützen. Hier sind einige zentrale Punkte, die Handwerksbetriebe beachten sollten.

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

9. Domain-Datenschutz

Domainregistrierung und Whois-Daten

Bei der Registrierung einer Domain werden bestimmte personenbezogene Daten wie Name, Adresse und Kontaktdaten des Domaininhabers im sogenannten Whois-Verzeichnis veröffentlicht. Um den Datenschutz zu gewährleisten, können Handwerksbetriebe:

- Whois-Privacy-Services nutzen: Diese Dienste schützen die persönlichen Daten des Domaininhabers, indem sie deren Informationen durch die Daten des Dienstansbieters ersetzen.
- Datenminimierung: Nur die notwendigen Informationen angeben und auf die Veröffentlichung unnötiger persönlicher Daten verzichten.

9. Domain-Datenschutz

Datenschutzerklärung auf der Webseite

Jede Webseite eines Handwerksbetriebs muss eine Datenschutzerklärung enthalten, die über die Art, den Umfang und den Zweck der Erhebung und Verwendung personenbezogener Daten informiert. Diese Erklärung sollte:

- Klar und verständlich sein.
- Kontaktdaten des Datenschutzbeauftragten oder Ansprechpartners enthalten.
- Informationen zu den Rechten der Nutzer (z.B. Auskunftsrecht, Recht auf Löschung) beinhalten.

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

9. Domain-Datenschutz

Umgang mit Cookies

Wenn die Webseite Cookies verwendet, muss der Handwerksbetrieb:

- Cookie-Banner: Implementierung eines Banners, das die Nutzer über die Verwendung von Cookies informiert und ihre Zustimmung einholt.
- Detaillierte Cookie-Informationen: Bereitstellung von Informationen darüber, welche Cookies verwendet werden, zu welchem Zweck und wie lange sie gespeichert werden.

9. Domain-Datenschutz

Vertrag zur Auftragsverarbeitung (AV-Vertrag)

Falls der Handwerksbetrieb Drittanbieter zur Datenverarbeitung nutzt (z.B. Hosting-Anbieter, Webdesigner), muss ein Vertrag zur Auftragsverarbeitung abgeschlossen werden, der sicherstellt, dass auch diese Dienstleister den Datenschutzanforderungen entsprechen.

9. Domain-Datenschutz

Schulung und Sensibilisierung

Mitarbeiter sollten regelmäßig geschult und für Datenschutzthemen sensibilisiert werden, um sicherzustellen, dass sie die datenschutzrechtlichen Anforderungen kennen und einhalten.

9. Domain-Datenschutz

Handwerksbetriebe sollten sicherstellen, dass die auf ihren Domains gehosteten Webseiten sicher sind, um Datenschutzverletzungen zu vermeiden. Dazu gehören:

- ✓ Regelmäßige Updates und Patches: Aktualisierung von Content-Management-Systemen (CMS), Plugins und anderer Software, um Sicherheitslücken zu schließen.

9. Domain-Datenschutz

- ✓ Sichere Passwörter und Authentifizierungsverfahren: Einsatz von starken Passwörtern und, wenn möglich, Zwei-Faktor-Authentifizierung (2FA).
- ✓ SSL/TLS-Verschlüsselung: Sicherstellung, dass die Webseite über HTTPS erreichbar ist.

9. Domain-Datenschutz

Zusammenfassung

Datenschutz in Domains für Handwerksbetriebe umfasst die Registrierung und Verwaltung der Domain, die Sicherstellung der Datensicherheit auf der Webseite, die Einhaltung rechtlicher Vorgaben wie der DSGVO, und die Sensibilisierung der Mitarbeiter. Durch die Umsetzung dieser Maßnahmen können Handwerksbetriebe den Schutz personenbezogener Daten gewährleisten und Vertrauen bei ihren Kunden und Partnern schaffen.

10. Datenschutz und Kameradrohnen

Praxisbeispiele aus dem Handwerk

- ✓ Dokumentation von Baustellenfortschritt
- ✓ Inspektion von Dächern und Fassaden
- ✓ Erstellung von Marketingmaterial

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

10. Datenschutz und Kameradrohnen

Datenschutz bei Verwendung von Kameradrohnen

Risiken und Herausforderungen

- Unbeabsichtigte Erfassung von Nachbargrundstücken oder Passanten
- Datensicherheit und -speicherung

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

10. Datenschutz und Kameradrohn

Datenschutz bei Verwendung von Kameradronen

Best Practices

- Vorab-Checklisten zur Planung von Drohneneinsätzen
- Sicherstellung der Einwilligung von Betroffenen
- Implementierung technischer und organisatorischer Maßnahmen zum Datenschutz (z.B. Geofencing, Datenverschlüsselung)

10. Datenschutz und Kameradrohnen

Datenschutz bei Verwendung von Kameradrohnen

Ein Datenschutzkonzept dient dazu, den Einsatz von Kameradrohnen im Handwerk datenschutzkonform zu gestalten. Ziel ist es, die Erfassung, Verarbeitung und Speicherung personenbezogener Daten im Einklang mit der DSGVO und dem BDSG zu gewährleisten.

Gefördert durch:



10. Datenschutz und Kameradrohn

Datenschutzkonzept für einen Drohneneinsatz

Beschreibung des Drohneneinsatzes

- ✓ **Anwendungsbereich:** Dokumentation des Baufortschritts einer Baustelle.
- ✓ **Ziel:** Regelmäßige visuelle Inspektion und Fortschrittsdokumentation.

10. Datenschutz und Kameradrohn

Datenschutzkonzept für einen Drohneneinsatz

Beschreibung des Drohneneinsatzes

- ✓ **Dauer:** Wöchentlicher Einsatz für die Dauer von sechs Monaten.
- ✓ **Verantwortliche Stelle:** Musterbau GmbH,
Datenschutzbeauftragter: Max Mustermann

10. Datenschutz und Kameradrohn Datenschutzkonzept für einen Drohneneinsatz

Erfassung und Verarbeitung personenbezogener Daten

- ✓ **Art der erfassten Daten:** Video- und Bildaufnahmen der Baustelle, möglicherweise auch angrenzender Bereiche (Nachbargrundstücke, Passanten).
- ✓ **Zweck der Verarbeitung:** Fortschrittsdokumentation, Qualitätssicherung, interne Berichterstattung.

10. Datenschutz und Kameradrohn Datenschutzkonzept für einen Drohneneinsatz

Erfassung und Verarbeitung
personenbezogener Daten

✓ **Rechtsgrundlage:** Einwilligung der betroffenen Personen (Art. 6 Abs. 1 lit. a DSGVO).

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

10. Datenschutz und Kameradrohn Datenschutzkonzept für einen Drohneneinsatz

Einwilligungserklärung

- ✓ Einholung der Einwilligung von Mitarbeitern und Anwohnern vor Beginn der Drohnenflüge.

10. Datenschutz und Kameradrohn Datenschutzkonzept für einen Drohneneinsatz

Einwilligungserklärung

- ✓ Information der Betroffenen über Zweck, Umfang und Dauer der Datenverarbeitung.

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

10. Datenschutz und Kameradrohn Datenschutzkonzept für einen Drohneneinsatz

Einwilligungserklärung

✓ Dokumentation der Einwilligungserklärungen.

10. Datenschutz und Kameradrohn

Datenschutzkonzept für einen Drohneneinsatz

Transparenz und Informationspflichten

- ✓ Aushang von Hinweisschildern auf der Baustelle und angrenzenden Bereichen.
- ✓ Veröffentlichung der Drohnenflugzeiten auf der Unternehmenswebsite und per Aushang.

10. Datenschutz und Kameradrohn

Datenschutzkonzept für einen Drohneneinsatz

Datenminimierung und Speicherbegrenzung

- ✓ Einsatz von Geofencing, um Aufnahmen auf das Baustellengelände zu beschränken.
- ✓ Regelmäßige Sichtung und Löschung nicht relevanter Aufnahmen.

10. Datenschutz und Kameradrohn

Datenschutzkonzept für einen Drohneneinsatz

Datenminimierung und Speicherbegrenzung

- ✓ Speicherung der relevanten Aufnahmen nur für den erforderlichen Zeitraum (maximal 6 Monate).

11. Datenschutz und Künstliche Intelligenz (KI)

Definition

- ✓ **Künstliche Intelligenz (KI)** ist ein Teilbereich der Informatik, der sich mit der Entwicklung von Systemen beschäftigt, die menschenähnliche Intelligenz aufweisen. Diese Systeme sollen Aufgaben übernehmen können, die normalerweise menschliche Intelligenz erfordern, wie z.B. das Verstehen von natürlicher Sprache, Bilderkennung, Entscheidungsfindung und Problemlösung.

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

11. Datenschutz und Künstliche Intelligenz (KI)

Datenschutz im Zusammenhang mit der Nutzung von Künstlicher Intelligenz

Arten von KI

- ✓ **Schwache KI (Weak AI)**, auch bekannt als enge KI (Narrow AI), bezieht sich auf Systeme, die für spezifische Aufgaben entwickelt wurden. Diese Systeme können eine oder mehrere Aufgaben ausführen, für die sie programmiert wurden, aber sie haben kein Bewusstsein oder allgemeines Verständnis über ihre Aufgabe hinaus. Beispiele für schwache KI sind Sprachassistenten wie Siri oder Alexa, die Spracherkennung und einfache Konversationsfähigkeiten besitzen.

11. Datenschutz und Künstliche Intelligenz (KI)

Datenschutz im Zusammenhang mit der Nutzung von Künstlicher Intelligenz

Mögliche Einsatzgebiete im Handwerk

- ✓ Automatisierung von Verwaltungsaufgaben
- ✓ Kundendienst und Kommunikation
- ✓ Projektmanagement und Planung
- ✓ Qualitätskontrolle und Wartung
- ✓ Produktion und Fertigung
- ✓ Design und Produktentwicklung

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

11. Datenschutz und Künstliche Intelligenz (KI)

Datenschutz im Zusammenhang mit der Nutzung von Künstlicher Intelligenz

Mögliche Einsatzgebiete im Handwerk

- ✓ Lagerhaltung und Logistik
- ✓ Marketing und Vertrieb
- ✓ Schulung und Weiterbildung
- ✓ Sicherheitsüberwachung

11. Datenschutz und Künstliche Intelligenz (KI)

Datenschutz im Zusammenhang mit der Nutzung von Künstlicher Intelligenz

Datenschutz im Zusammenhang mit der KI

Der Datenschutz im Zusammenhang mit der Nutzung von Künstlicher Intelligenz (KI) ist ein komplexes und wichtiges Thema, das viele Aspekte der Datenverarbeitung und -sicherheit betrifft.

Hier sind einige der wichtigsten Punkte:

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

11. Datenschutz und Künstliche Intelligenz (KI)

Datenschutz im Zusammenhang mit der Nutzung von Künstlicher Intelligenz

Datensammlung und -verarbeitung

- **Datenminimierung:** Die Menge der gesammelten Daten sollte auf das notwendige Minimum beschränkt werden, um die angestrebten Ziele zu erreichen.

11. Datenschutz und Künstliche Intelligenz (KI)

Datenschutz im Zusammenhang mit der Nutzung von Künstlicher Intelligenz

Datensammlung und -verarbeitung

- **Transparenz:** Nutzer sollten darüber informiert werden, welche Daten gesammelt werden, zu welchem Zweck und wie sie verarbeitet werden.
- **Einwilligung:** Personenbezogene Daten sollten nur mit der ausdrücklichen Zustimmung der betroffenen Person gesammelt und verarbeitet werden.

11. Datenschutz und Künstliche Intelligenz (KI)

Datenschutz im Zusammenhang mit der Nutzung von Künstlicher Intelligenz

Anonymisierung und Pseudonymisierung

- **Anonymisierung:** Daten sollten so verarbeitet werden, dass die betroffenen Personen nicht mehr identifiziert werden können. Dies ist ein starker Schutzmechanismus, reduziert aber auch den Nutzen der Daten.

11. Datenschutz und Künstliche Intelligenz (KI)

Datenschutz im Zusammenhang mit der Nutzung von Künstlicher Intelligenz

Anonymisierung und Pseudonymisierung

- **Pseudonymisierung:** Daten können durch Pseudonyme ersetzt werden, was die Identifikation der betroffenen Personen erschwert, aber unter bestimmten Bedingungen rückgängig gemacht werden kann.

11. Datenschutz und Künstliche Intelligenz (KI)

Datenschutz im Zusammenhang mit der Nutzung von Künstlicher Intelligenz

Ethik und Bias

- **Vermeidung von Bias:** KI-Modelle sollten darauf überprüft werden, ob sie Verzerrungen enthalten, die bestimmte Gruppen benachteiligen könnten.
- **Ethik-Richtlinien:** Unternehmen sollten ethische Richtlinien entwickeln und implementieren, um sicherzustellen, dass KI-Systeme verantwortungsvoll eingesetzt werden.

11. Datenschutz und Künstliche Intelligenz (KI)

Datenschutz im Zusammenhang mit der Nutzung von Künstlicher Intelligenz

Fazit

Der Datenschutz bei der Nutzung von KI erfordert eine sorgfältige Planung und die Implementierung robuster Datenschutzmaßnahmen. Organisationen müssen sicherstellen, dass sie nicht nur die gesetzlichen Anforderungen einhalten, sondern auch ethisch und verantwortungsvoll handeln, um das Vertrauen der Nutzer zu gewinnen und zu bewahren.

11. Datenschutz und Künstliche Intelligenz (KI)

Datenschutz im Zusammenhang mit der Nutzung von Künstlicher Intelligenz

Fazit

Der Datenschutz bei der Nutzung von KI erfordert eine sorgfältige Planung und die Implementierung robuster Datenschutzmaßnahmen. Organisationen müssen sicherstellen, dass sie nicht nur die gesetzlichen Anforderungen einhalten, sondern auch ethisch und verantwortungsvoll handeln, um das Vertrauen der Nutzer zu gewinnen und zu bewahren.

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

12. Beispiele für Datenschutzverletzungen

Beispiel 1: H&M

Vorfall:

H&M wurde beschuldigt, systematisch private Informationen über Mitarbeiter gesammelt und gespeichert zu haben. Diese Informationen beinhalteten Details über Familienangelegenheiten, religiöse Überzeugungen und gesundheitliche Probleme.

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

12. Beispiele für Datenschutzverletzungen

Beispiele für Datenschutzverletzungen und deren Strafen

Beispiel 1: H&M

Strafe:

H&M wurde mit einer Geldstrafe von 35,3 Millionen Euro belegt, da die Sammlung und Speicherung dieser sensiblen Daten ohne angemessene rechtliche Grundlage und Transparenz erfolgte.

Gefördert durch:



12. Beispiele für Datenschutzverletzungen

Beispiele für Datenschutzverletzungen und deren Strafen

Beispiel 1: H&M

Beschränkung auf notwendige Daten: Erfassen und speichern Sie nur Daten, die für den Geschäftszweck erforderlich sind.

Transparenz: Informieren Sie die Betroffenen klar und deutlich über die Datenerfassung und -verarbeitung.

Rechtsgrundlage: Stellen Sie sicher, dass eine rechtliche Grundlage für die Verarbeitung sensibler Daten vorhanden ist.

12. Beispiele für Datenschutzverletzungen

Beispiele für Datenschutzverletzungen und deren Strafen

Beispiel 2: British Airways

Vorfall:

British Airways erlitt 2018 eine Datenpanne, bei der die persönlichen Daten von etwa 500.000 Kunden kompromittiert wurden. Die Datenpanne war auf eine unzureichend gesicherte Webseite zurückzuführen, die von Hackern ausgenutzt wurde.

Gefördert durch:



12. Beispiele für Datenschutzverletzungen

Beispiele für Datenschutzverletzungen und deren Strafen

Beispiel 2: British Airways

Strafe:

Die britische Datenschutzbehörde (ICO) verhängte eine Geldstrafe von 20 Millionen Pfund, was die höchste Strafe war, die die ICO zu diesem Zeitpunkt verhängt hatte.

12. Beispiele für Datenschutzverletzungen

Beispiele für Datenschutzverletzungen und deren Strafen

Beispiel 2: British Airways

Sicherheit der IT-Infrastruktur: Investieren Sie in robuste Sicherheitsmaßnahmen und regelmäßige Sicherheitsüberprüfungen.

Schnelle Reaktion: Reagieren Sie schnell auf Sicherheitsvorfälle, um den Schaden zu begrenzen.

Benachrichtigung: Informieren Sie die Betroffenen und die Behörden zeitnah über den Vorfall.

12. Beispiele für Datenschutzverletzungen

Beispiele für Datenschutzverletzungen und deren Strafen

Beispiel 3: 1&1 Telecom GmbH

Vorfall:

Die deutsche Datenschutzbehörde verhängte eine Strafe gegen 1&1 Telecom GmbH, weil deren Kundenservice unzureichende Authentifizierungsmaßnahmen einsetzte. Dadurch konnten unbefugte Personen durch einfache Angaben von Name und Geburtsdatum auf Kundendaten zugreifen.

12. Beispiele für Datenschutzverletzungen

Beispiele für Datenschutzverletzungen und deren Strafen

Beispiel 3: 1&1 Telecom GmbH

Strafe:

1&1 Telecom GmbH wurde mit einer Geldstrafe von 9,55 Millionen Euro belegt.

12. Beispiele für Datenschutzverletzungen

Beispiele für Datenschutzverletzungen und deren Strafen

Beispiel 3: 1&1 Telecom GmbH

Starke Authentifizierung: Implementieren Sie robuste Authentifizierungsmaßnahmen, um den Zugriff auf sensible Daten zu sichern.

Datensicherheit im Kundenservice: Schulen Sie Ihre Mitarbeiter im sicheren Umgang mit Kundendaten und in der Anwendung von Sicherheitsmaßnahmen. **Risikoanalyse:** Führen Sie regelmäßige Risikoanalysen durch, um Schwachstellen im System zu identifizieren und zu beheben.