DS-GVO für Unternehmen und Vereine

schmid datensicherheit

Kontaktdaten auf der vorletzten Seite dieser Folien

Datenschutz / EU-DS-GVO

Bild: pixabay.com (Geralt, IO-Images)

VERORDNUNG (EU) 2016/679

... vom 27. April 2016

Landkreis NEUSTADT an der Waldnaab

Update Dezember 2018

Informationsmaterial aus einer Vortragsreihe für das Landratsamt Neustadt/WN

Datenschutz

schmid datensicherheit

Die DS-GVO ist seit 25.Mai 2018 verpflichtend !!

Europäische Datenschutz-Grundverordnung

VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016

(EU-DS-GVO → pdf-Datei hat 88 Seiten)

Erwägungsteil:

- Beschreibung der Ziele der Verordnung
- Interpretation der Intention
- 173 Erwägungspunkte

Artikelteil:

- 99 Artikel
- 57 Seiten

Inhaltsübersicht

schmid datensicherheit

Datenschutz für Unternehmen –

Basisanforderungen und Spezialfälle

- Datenschutz – woher und warum ?
- Was sind personenbezogene Daten ?
- Welche Begriffe sollten bekannt sein ?
- Welche Dokumentationen sind erforderlich ?
- Wie ist der Umgang mit den Daten zu organisieren ?
- Was ist zu verschiedenen Einzelaspekten zu sagen ?

Datenschutz – Woher kommt das?

schmid datensicherheit

Ursprung der Rechtsprechung zum Datenschutz:

- **Informationelle Selbstbestimmung**
  Das Recht auf informationelle Selbstbestimmung ist im Recht Deutschlands das Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen (Rechtsprechung des Bundesverfassungsgerichts).
- **Europäische Menschenrechtskonvention**
  „Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz."
  – EMRK Art. 8 Abs. 1
- **Unverletzlichkeit der privaten Wohnung**
  Das Grundrecht der Unverletzlichkeit der Wohnung dient als Freiheitsrecht vorrangig der Abwehr hoheitlicher Eingriffe in die Privatsphäre, welche die Wohnung bietet. Daneben gibt es dem Gesetzgeber den Auftrag, die Wohnung vor Privatpersonen zu schützen. Dieser Aufgabe kommt der Statt beispielsweise durch den Schutz der Wohnung im Rahmen des Straf- und Zivilrechts nach.
  – Deutsches Grundgesetz (GG) Art. 13 Abs. 1
- **Persönlichkeitsrecht**
  Das allgemeine Persönlichkeitsrecht (APR) wird mit einem umfassenden Persönlichkeitsschutz aus Art. 2 Abs. 1 GG (freie Entfaltung der Persönlichkeit) in Verbindung mit Art. 1 Abs. 1 GG (Menschenwürde) abgeleitet.
- **Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme**
  Dieses Recht wird im Grundgesetz nicht eigens genannt, sondern wurde als spezielle Ausprägung des allgemeinen Persönlichkeitsrechts 2008 durch das Bundesverfassungsgericht derart formuliert bzw. aus vorhandenen Grundrechtsbestimmungen abgeleitet.

(Bilerd: pixabay.com; Texte sind teilweise Auszüge aus https://de.wikipedia.org/)

schmid datensicherheit

Ziele der EU-DS-GVO:

- EU-weiter einheitlicher wirksamer Schutz personenbezogener Daten (Stärkung und Präzisierung der Rechte der betroffenen Personen);
- Verschärfung der Auflagen für diejenigen, die personenbezogenen Daten verarbeiten und darüber entscheiden;
- EU-weite einheitliche Befugnisse der Mitgliedsstaaten (Vorschriften, Überwachung, Sanktionen);

Worauf bezieht sich "Daten"? [1]

schmid datensicherheit

Personenbezogenen Daten sind:

alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Im Detail:

- **Name und Adresse**
- **Personalausweisnummer**
- **Kundennummer**
- **Mitgliedsnummer**
- **Online-Nutzername**
- **E-Mail-Adresse**
- **Telefonnummer**
- **IP-Adresse (!)**
- **Sprachaufzeichnung**
- **Geburtsdatum, Geburtsort**
- **Porträtfoto, Videoaufzeichnung einer Person**
- **...**

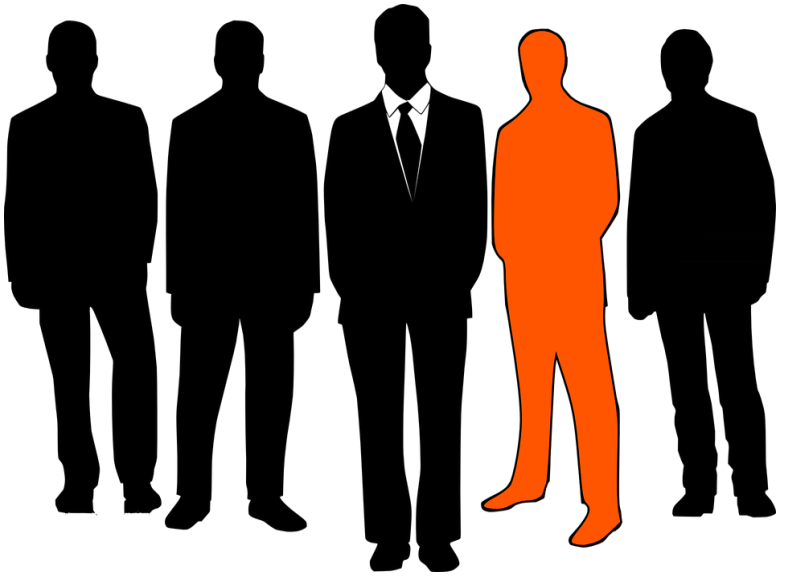


Bild: pixabay.com, OpenClipart-Vectors

Worauf bezieht sich "Daten"? [2]

schmid datensicherheit

Personenbezogenen Daten sind auch:

Daten, über die ein Personenbezug auf eine identifizierbare natürliche Person hergestellt werden kann. Im Detail:

- **Standortdaten**
- **Kontonummer**
- **Kennnummer**
- **Rentenversicherungsnummer**
- **Sozialversicherungsnummer**
- **Kfz-Kennzeichen**
- **...**

Deutsche Rentenversicherung

Bilder: geoportal.bayern.de/bayernatlas/, www.deutsche-rentenversicherung.de

Worauf bezieht sich "Daten"? [3]

schmid datensicherheit

Besondere Arten personenbezogener Daten, die in höherem Maße sensibel sind, unterliegen einem verschärften Schutz. Die Kategorien sind:

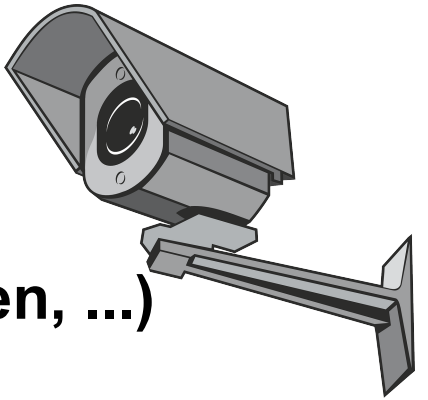
- **Rassische und ethnische Herkunft**
- **Politische Meinungen**
- **Religiöse oder weltanschauliche Überzeugungen**
- **Gewerkschaftszugehörigkeit**
- **Gesundheit und Sexualität**
- **Genetische und biometrische Daten zur eindeutigen Identifizierung einer Person**
- **Vermögens- und Finanzverhältnisse** steht nicht in der DS-Grundverordnung, erfordert aber erhöhten Schutzbedarf

Überblick zu Datenarten

schmid datensicherheit

Arten von personenbezogenen Daten:

- **Beschäftigtendaten, Daten der Mitglieder**
- **Kundendaten, Vereinsregister**
- **Lieferantendaten (Ansprechpartner)**
- **Kommunikationsdaten (soz. Netzwerke)**
- **Gesundheitsdaten (Krankentage, Sportgruppen)**
- **Bewegungsprofile (Fahrzeugflotten)**
- **Überwachungsdaten**
- **Daten über gekaufte Produkte (Händler)**
- **Mitgliederprofile (Vereine, Stiftungen, Parteien, ...)**
- **...**



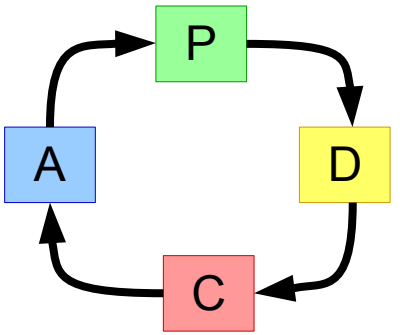
Bilder: pixabay.com, OpenClipart-Vectors, 3dman_eu

Auswirkungen der DS-GVO [1]

schmid datensicherheit

Anforderungen: (verschärft gegenüber BDSG)

- **Transparente Information des Betroffenen**
- **Recht auf Auskunft zu personenbezogenen Daten**
- **Informationspflicht des Verantwortlichen**
- **spezieller Schutzbedarf für digital verarbeitete personenbezogene Daten (→ verstärkter Fokus auf IT-Sicherheit)**
- **für größere Unternehmen und Vereine:**
  - **Datenschutzkonzept (Datenschutz-Mgmt.system)**
  - **Datenschutz als Prozess (PDCA-Zyklus)**
    {Plan → Do → Check → Act → Plan → ..., Audits}
  - **Reifegradmodell** (Kennzahlen zum aktuellen Status)
  - **Zertifizierung der Datenschutzmaßnahmen**



Auswirkungen der DS-GVO [2]

schmid datensicherheit

Reichweite:

- **Auch die Daten von eigenen Kontakten, die in einem anderen Unternehmen** (Muttergesellschaft) **oder in einem anderen Verein** (übergeordneter Verband) **verfügbar sind, sind personenbezogene Daten !!**
- **Kein Unterschied zwischen privat und geschäftlich**
- **Personenbezug in der „Zukunft“ möglich !?!**
  Beispiel: Die IP-Adresse wurde erst vor einigen Jahren als personenbezogenes Datenelement definiert, obwohl IP-Adressen bereits viele Jahre vorher benutzt wurden.
- **Die DS-GVO gilt für "ALLE", die personenbezogene Daten elektronisch oder nicht automatisiert in einer strukturierten Ablage verarbeiten (bzw. nutzen).** Der Aufwand zur Umsetzung der datenschutzrechtlichen Vorgaben soll im Verhältnis zur Unternehmensgröße bzw. zur Vereinsgröße und zu den jeweiligen wirtschaftlichen Möglichkeiten stehen. Die grundsätzlichen Vorgaben und Anforderungen müssen aber von **"jedem"** eingehalten werden, der personenbezogenen Daten erhebt, verarbeitet, speichert, weitergibt oder in irgend einer Weise nutzt.

Personenbezogene Daten [1]

schmid datensicherheit

Begriffsübersicht bei der Datennutzung und -verarbeitung:

- **Verantwortlicher für die Datenverarbeitung, Datenerhebung, u.s.w.**
- **Zwecke der Verarbeitung / Zweckbindung der erhobenen Daten**
- **Kategorien von der Erhebung/Verarbeitung betroffener Personen**
- **Kategorien personenbezogener Daten, die erhoben werden**
- **Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offen gelegt werden**
- **Übermittlung personenbezogener Daten in Drittländer (Datentransfer nur bei Erfüllung aller Anforderungen)**
- **Rechtsgrundlage der Erhebung/Verarbeitung von personenbezogenen Daten**
- **Speicherfristen, denen die Daten unterliegen**

Personenbezogene Daten [2]

schmid datensicherheit

Begriffsübersicht für die Betroffenenrechte:

- **Auskunftsrecht der Betroffenen**
- **Information des Betroffenen vor der Datenerhebung**
- **Recht auf Berichtigung, Löschung, Einschränkung, Widerspruch (Widerruf einer Einwilligung)**
- **Recht auf Vergessen / weitergegebene Daten müssen auch bei Partnern gelöscht werden (gilt auch im Ausland)**
- **Datensparsamkeit und Speicherbegrenzung (zeitlich und bezogen auf Umfang)**
- **Datenportabilität (z. B. Provider, Versicherung, ...)**
- **Notwendigkeit einer Bestätigung zur Einwilligung (für Werbung, Newsletter u.s.w., Double Opt-in)**
- **Nachweis der Herkunft der personenbezogenen Daten, Direkterhebung**

Personenbezogene Daten [3]

schmid datensicherheit

Begriffsübersicht für die Pflichten der Verantwortlichen:

- **Nachweis der Einhaltung von Datenschutzgrundsätzen / Transparenz**
- **Dokumentationspflicht / Verarbeitung und Verwendung von personenbezogenen Daten muss dokumentiert werden**
- **Meldepflicht bei Datenschutzverstößen (72 Std. für Behördenkontakt)**
- **Datenschutzschulungen / Awareness-Maßnahmen – Datenschutz-Verpflichtung aller Zugriffsberechtigten**
- **Datenschutz-Beauftragter / Datenschutz-Audits**
- **Verarbeitung im Auftrag (wechselseitige Haftung/Kontrolle) / AV-Vertrag (Auftragsverarbeitung)**
- **BDSG-neu - Nationale Spielräume**
- **Sanktionsmöglichkeiten sind verschärft / Strafen sind deutlich angehoben**

Personenbezogene Daten [4]

schmid datensicherheit

Begriffsübersicht für die (digitale) Datenverarbeitung:

- **IT-Sicherheit für die Verarbeitung personenbezogener Daten**
- **Schutzziele der Informationssicherheit / Belastbarkeit der Systeme**
- **TOMs - Technisch-organisatorische Maßnahmen**
- **Datensicherung und Löschkonzept**
- **Verhinderung des Missbrauch zu anderen Zwecken**
- **Rechtmäßigkeit, z.B. einer Überwachung** (Objektschutz durch Videoüberwachung)
- **Risikoanalyse / Risikobewertung** (Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen)
- **Datenschutz-Folgenabschätzung (Privacy Impact Assessment)**
- **Privacy-by-Design / Privacy-by-Default**
- **Security-by-Design (Stand der Technik)**

Datenschutz für Unternehmen

schmid datensicherheit

Wichtigste Punkte mit denen sich ein Betrieb beschäftigen muss:

- **Dokumente (Verfahrensverzeichnis, Verarbeitungstätigkeiten)**
- **Texte (Einwilligungen, Informationen für Betroffene)**
- **E-Mails** (Vertraulichkeit personenbezogener Daten)
- **Webauftritt,** Cookies, Online-Analytics
- **Datenschutzerklärung,** Impressum**, Kontaktformular**
- **Soziale Netzwerke – Like-Buttons**
- **Datenschutzbeauftragter**
- **Bilder, Veranstaltungen**
- **Kinder** (kindgerechter Datenschutz, elterliche Einwilligung)
- **...**

Bilder: pixabay.com

Datenschutz für Vereine

schmid datensicherheit

Wichtigste Punkte mit denen sich ein Verein beschäftigen muss:

- **Dokumente (Verfahrensverzeichnis, Verarbeitungstätigkeiten)**
- **Texte (Einwilligungen, Informationen für Betroffene)**
- **Daten im Vereinsregister, Bilder, Veranstaltungen**
- **E-Mails** (Vertraulichkeit personenbezogener Daten)
- **Webauftritt,** Cookies, Online-Analytics
- **Datenschutzerklärung,** Impressum**, Kontaktformular**
- **Soziale Netzwerke – Like-Buttons**
- **Kinder** (kindgerechter Datenschutz, elterliche Einwilligung)
- **Datenschutzbeauftragter** (In der Regel für bayerische Vereine nicht erforderlich.)
- **...**

Bilder: pixabay.com

Erlaubte Verarbeitung

schmid datensicherheit

Voraussetzungen für eine erlaubte Datenverarbeitung:

- **Einwilligung der betroffenen Person**
- **Es gibt ein berechtigtes Interesse an der Datenverarbeitung und schutzwürdige Interessen des Betroffenen stehen dem nicht entgegen**
- **Die Datenverarbeitung ist erforderlich**
  - zur Erfüllung eines Vertrages
  - für vorvertragliche Maßnahmen auf eine Anfrage hin (z.B. für Versicherung)
  - zur Erfüllung einer rechtlichen Verpflichtung des Verantwortlichen
  - zum Schutz lebenswichtiger Interessen der betroffenen oder einen anderen natürlich Person
  - im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt

Datenschutz = Verbot mit Erlaubnisvorbehalt

Datenerhebung, Datenvermeidung und Datensparsamkeit

schmid datensicherheit

Die rechtlichen Grundlagen sind in der DS-GVO geregelt:

- **Datenerhebung ist erlaubt,**
  - wenn dieses Gesetz oder andere Vorschriften das erlauben oder anordnen, oder
  - der Betroffene eingewilligt hat.
  - Einwilligung des Betroffenen nur wirksam, wenn freie Entscheidung möglich.
  - Für Kinder (Grenze 16 Jahre) gelten besondere Voraussetzungen.
- **Der Betroffene ist über**
  - die Identität der verantwortlichen Stelle,
  - die Zweckbestimmung, sowie
  - über die Empfänger der Daten zu unterrichten
- **Erhebung, Verarbeitung und Nutzung von Daten muss mit dem Ziel erfolgen,**
  - so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen,
  - die Daten müssen für den Zweck der Datenerhebung erforderlich sein.

Dokumente und Texte

schmid datensicherheit

Wichtigste Unterlagen, Vorlagen und Erklärungen:

- Verfahrensverzeichnis
  (klare einfache Sprache, wirksame datenschutzrechtliche Klauseln, Text zur Veröffentlichung {auf Anfrage})
- Datenschutzerklärung auf Webseite und für soziale Netzwerke
- Geheimhaltungsverpflichtung für Mitarbeiter oder Vereinsmitglieder, die Zugriff auf personenbezogene Daten haben
- Verhaltensregeln für Mitarbeiter definieren (Dienstanweisung, Verpflichtung)
- Vorlage für Einwilligungserklärung(en) (Papier oder Online,
  für Mitarbeiter, für Bilder auf Webseiten o. Unternehmenszeitung, ...)
- Vorlage für Informationen für Betroffene

- Datenschutzleitlinie (Verpflichtung der Geschäftsleitung bei großen Unternehmen bzw. des Vorstands bei großen Vereinen)
- Dokumentation mittels Datenschutz-Managementsystem (ideal),
  Dokumentationsmanagement (nur bei großen Unternehmen oder großen Vereinen)

schmid datensicherheit

Inhalt eines Verfahrensverzeichnisses:

- **Name und Kontaktdaten der verantwortlichen Stelle**
- **Name und Kontaktdaten des Datenschutzbeauftragten**
- **Zwecke der Verarbeitung (Zweckbindung)**
- **Beschreibung der Kategorien betroffener Personen**
- **Beschreibung der Kategorien personenbezogener Daten**
- **Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind / Datenweitergabe**
- **Übermittlungen an ein Drittland (samt Name des Landes)**
- **Dauer der Datenspeicherung / Löschfristen für Datenkategorien**
- **Rechtsgrundlagen / Risikobewertung**
- **Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen**
- **Darlegung der Umsetzung einer uneingeschränkten Kommunikation der Betroffenenrechte / Widerspruchsrecht / Beschwerderecht**

Vorlagen für Verfahrensverzeichnisse

schmid datensicherheit

Beispiele verschiedener Verfahrensverzeichnisse sind auf der Webseite des Bayerischen Landesamts für Datenschutzaufsicht zu finden:

Handreichungen für kleine Unternehmen und Vereine:

https://www.lda.bayern.de/de/kleine-unternehmen.html

Weitere Links sind am Ende des Dokuments aufgelistet.

Ergänzungen zu den Verfahrensvzn.

schmid datensicherheit

Anmerkungen zu den einzelnen Elementen:

- **Ansprechpartner → Verantwortlicher** (Es gibt immer einen Verantwortlichen!)
- **Datum der Einführung → Datum der Aufnahme der Tätigkeit**
  (ideal sind 2 Datumsangaben) → **Datum d. letzt. Änderung im Verfahrensverzeichnis**
- **Kategorie von Empfängern → Empfänger intern**
  → Empfänger extern
  → Übertragung in Drittland oder an internationale Organisation
  → Nennung der konkreten Datenempfänger
  → Dokumentation geeigneter Garantien

  (Die Unterscheidung zwischen intern und extern vereinfacht das Verständnis der Datenverarbeitung.)
- **Rechtsgrundlage** (In der Regel ist es möglich, die rechtliche Grundlage klar und einfach zu definieren, auf der die jeweilige Verarbeitungstätigkeit beruht.)

nicht vergessen:

- **Risikobewertung bei besonderen personenbezogenen Daten** (z.B. Gesundheit)

Datenschutzerklärung

schmid datensicherheit

Anforderungen an die Datenschutzerklärung auf der Webseite/Webseiten:

- **Die Datenschutzerklärung soll alle datenschutzrechtlichen Aspekte des Betriebs der Website (= Webauftritt) abdecken.**
- **Die Datenschutzerklärung darf keine unrichtigen Angaben enthalten (keine Pauschalaussagen).**
- **Die Datenschutzerklärung kann Informationen weiterer digitaler Kommunikationswege enthalten (Umgang mit E-Mails, Datenschutzerklärung für soziale Netzwerke, ...).**
- **Datenschutzerklärung und Impressum müssen immer mit einem Klick von jeder Webseite aus ("Zwei-Klick-Regel") erreichbar sein.**

- **siehe "Datenschutzerklärung" auf einer nachfolgenden Folie**

Einwilligungen

schmid datensicherheit

Inhalte einer Einwilligungserklärung (Nachweis):

- **Betroffene Person und Gegenstand der Einwilligung**
- **Verantwortlicher, Verantwortliche Stelle (hat die Rechenschaftspflicht)**
- **Freiwilligkeit der Einwilligung / Kopplungsverbot**
- **Verwendungszweck**
- **Empfänger der Daten / Reichweite der Nutzung**
- **Rechte des Betroffenen / Rechtsgrundlage**
- **Widerrufbarkeit / Widerspruchsrecht / Datenübertragbarkeit**
- **Zustimmung für die einzelnen Verwendungszwecke so differenziert wie möglich:**
  - □ **Bilder auf dem Webauftritt**
  - □ **Name bei den Bildern auf dem Webauftritt**
  - □ **Bilder auf dem Facebook-Auftritt**
  - □ **Name bei den Bildern auf dem Facebook-Auftritt**
- **Keine aktivierten Voreinstellungen (Privacy-by-Default)**

Arbeitnehmer

schmid datensicherheit

Neue Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DS-GVO ! (§5 BDSG gibt es nicht mehr)

Fälle des Arbeitnehmerdatenschutzes:

- **Überwachung des Surfverhaltens** (Mitarbeitervereinbarungen)
- **Elektronische Zeiterfassung / Krankmeldungen**
- **Videoüberwachung am Arbeitsplatz**
- **Speicherung und Löschung von Bewerberdaten**
- **Veröffentlichung interner Daten (Unternehmenszeitung, Newsletter, Bilder, Geburtstage)**

Kinder unter 16 Jahren [1]

schmid datensicherheit

Umgang mit personenbezogenen Daten von Kindern:

- **Immer schriftliche Einwilligung einholen (idealerweise von beiden Elternteilen)**
- **Empfehlungen der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit für einen kindgerechten Datenschutz im Umgang mit digitalen Medienangeboten:**
  - Empfehlung 1:
    Anbieter digitaler Medien und Dienste, die insbesondere auch Minderjährige ansprechen, sind aufgefordert, die Datenschutzbelange dieser Zielgruppe in besonderem Maße zu berücksichtigen.
  - Empfehlung 2:
    Der besonderen Schutzbedürftigkeit Minderjähriger ist durch eine entsprechende Gestaltung von Produkten und Dienstleistungen besonders Rechnung zu tragen. Informationspflichten sind kindgerecht verständlich darzustellen.

Kinder unter 16 Jahren [2]

schmid datensicherheit

Umgang mit personenbezogenen Daten von Kindern:

- **Empfehlungen der Bundesbeauftragten für den Datenschutz .....:**
  - Empfehlung 4:
    Datenschutzhinweise einschließlich Informationen zu den erforderlichen Einwilligungen sind in einfacher und für Minderjährige leicht verständlicher Sprache abzufassen und an exponierter Stelle zu platzieren.
  - Empfehlung 5:
    Erziehungsberechtigte, Lehrkräfte und alle sonstigen in die Betreuung von Kindern und Jugendlichen eingebundenen gesellschaftlichen Kräfte sind aufgerufen, gerade in Zeiten der durch die Digitalisierung ermöglichten Freiheiten sowohl für den besonderen Wert personenbezogener Informationen als auch für das Risiko der hohen Verletzbarkeit der eigenen Persönlichkeit zu sensibilisieren.

Datenschutzverletzungen

schmid datensicherheit

Bei Datenschutzverletzungen existiert eine gesetzliche Meldepflicht bei der Aufsichtsbehörde.
Beispiele für Meldepflicht:

- **Hacking von IT-Systemen**
- **Verlust von Daten**
- **Diebstahl von papiergebundenen oder digitalen Daten**
- **Fehlversand**
- **Softwarefehler**
- **Schadcode, Trojaner (Daten sind fremdverschlüsselt)**
- **Fehlentsorgung**
- **Vernichtung (versehentliches oder absichtliches Löschen)**
- **Sonstiges ?**

Bilderer: pixabay.com

Transparente Verarbeitung

schmid datensicherheit

Aus Erwägungsgrund Nr. 39 der DS-GVO ergibt sich der Grundsatz der Transparenz (für das öffentliche Verfahrensverzeichnis und die Datenschutzerklärung):

- **Dieser setzt voraus, dass alle Informationen und Mitteilungen zur Verarbeitung dieser personenbezogenen Daten leicht zugänglich und verständlich und in klarer und einfacher Sprache abgefasst sind.**
- **Dieser Grundsatz betrifft insbesondere die Informationen über die Identität des Verantwortlichen und die Zwecke der Verarbeitung und sonstige Informationen, die eine faire und transparente Verarbeitung im Hinblick auf die betroffenen natürlichen Personen gewährleisten, sowie deren Recht, eine Bestätigung und Auskunft darüber zu erhalten, welche sie betreffende personenbezogene Daten verarbeitet werden.**
- **Information plus Bildsymbole können für Transparenz (und transparente Texte) verwendet werden.**
- **Es muss eine Bewertung erfolgen, ob in Texten evtl. unwirksame datenschutzrelevante Klauseln enthalten sind.**

Informationspflichten des Verantwortlichen

schmid datensicherheit

Bei der Erhebung oder Verarbeitung personenbezogener Daten muss der Betroffene geeignet informiert werden. Dies ergibt sich aus Abschnitt 2 der DS-GVO (Informationspflicht und Recht auf Auskunft), insbesondere aus den Artikeln 13, 14 und 15. Die folgende Liste beschreibt Angaben, über die der Betroffene fallbezogen in Kenntnis gesetzt werden soll*: * (ohne Anspruch auf Vollständigkeit)

- **Bezeichnung der Tätigkeit, die mit der Verarbeitung in Zusammenhang steht.**
- **Name und Kontaktdaten des Verantwortlichen.**
- **Kontaktdaten der/des betrieblichen Datenschutzbeauftragten (**soweit vorhanden**).**
- **Zwecke und Rechtsgrundlagen der Verarbeitung.**
- **Kategorien der personenbezogenen Daten, die verarbeitet werden.**
- **Herkunft und/oder Erhebungsform der Daten.**
- **Empfänger oder Kategorien von Empfängern der personenbezogenen Daten.**
- **Übermittlung von personenbezogenen Daten an ein Drittland (**soweit zutreffend**).**
- **Dauer der Speicherung der personenbezogenen Daten.**
- **Rechte des Betroffenen (**gegenüber dem Verantwortlichen und der Aufsichtsbehörde**).**

Datenschutzbeauftragter

schmid datensicherheit

Eine Pflicht zur Benennung eines Datenschutzbeauftragten (DSB) kann sich sowohl aus der DS-GVO als auch aus nationalem Recht ergeben.

- **Ein DSB ist zu benennen, wenn 1 der folgenden Voraussetzungen gegeben ist:**
  - Kerntätigkeit mit umfangreicher oder systematischer Überwachung von Personen;
  - Kerntätigkeit mit umfangreicher Verarbeitung besonders sensibler Daten;
- **Faktoren für die Definition des Begriffs "umfangreich":**
  - Menge der verarbeiteten personenbezogenen Daten (Volumen),
  - Verarbeitung auf regionaler, nationaler o. supranationaler Ebene (geografischer Aspekt),
  - Anzahl der betroffenen Personen (absolute Zahl oder in Prozent zur relevanten Bezugsgröße) und
  - Dauer der Verarbeitung (zeitlicher Aspekt).
- **Benennung eines DSB ist auch in folgenden Fällen erforderlich:**
  - es werden in der Regel mindestens zehn Personen ständig (= überwiegend) mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt;
  - es werden Verarbeitungen vorgenommen, die einer Datenschutz-Folgenabschätzung unterliegen, oder es werden personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeitet;

Werbung

schmid datensicherheit

Die DS-GVO definiert ein berechtigtes Interesse eines Verantwortlichen (= keine Behinderung der Werbetreibenden), aber auch ein Widerspruchsrecht gegen Direktwerbung:

- **Werden personenbezogene Daten verarbeitet, um Direktwerbung zu betreiben, so hat die betroffene Person das Recht, jederzeit Widerspruch gegen die Verarbeitung sie betreffender personenbezogener Daten zum Zwecke derartiger Werbung einzulegen; dies gilt auch für das Profiling.**
- **E-Mail-Werbung, Newsletter u. ähnl. erfordert Double Opt-in Zustimmung.**
- **Die Verarbeitung muss „zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich“ sein, und eine Interessenabwägung darf nicht zu dem Ergebnis führen, dass die Verarbeitung unzulässig ist.**
- **Aus Erwägungsgrund Nr. 47 der DSGVO ergibt sich, dass Direktwerbung in der Regel ein solches berechtigtes Interesse darstellt.**

Direktwerbung

schmid datensicherheit

Direktwerbung mit automatisiertem Email-Versand:

- **Der Betroffene darf der Direktwerbung nicht widersprochen haben, und seine Interessen dürfen in einer Abwägung nicht überwiegen.**
- **Der Werbende muss nachweisen, dass er diese Interessenabwägung tatsächlich durchgeführt hat und das Ergebnis zu seinen Gunsten ausfällt.**
- **Um die Transparenz der Interessenabwägung herzustellen, muss die verarbeitende Stelle die in die Abwägung einfließenden Interessen gegenüber dem Betroffenen benennen.**
- **Die Einwilligung zur Datennutzung zu Werbezwecken darf nicht derart erzwungen werden, dass sie mit anderen Dienstleistungen für den Betroffenen fest verbunden ist (Kopplungsverbot).**
- **Ist die Einwilligung für die Dienstleistung (oder allgemein Vertragserfüllung) nicht erforderlich, darf sie auch nicht einfach verlangt werden. Es muss klar und deutlich auf die geplante Nutzung zu Werbezwecken hingewiesen werden (kostenloser Newsletter, Prinzip „Service gegen Daten“ muss erklärt werden).**

Datenschutzerklärung

schmid datensicherheit

Jeder Online-Auftritt braucht eine Erklärung zum Datenschutz:

- **Erklärung welche Daten zu welchem Zweck verarbeitet werden**
- **Erklärung welche Daten beim Besuch der Webseite generiert oder erfasst werden**
  - Webserver-Logging, Aufzeichnungen in Schutzsystemen des Providers
  - Cookies
  - Webtracking / Web-Analytics
- **Speicherfristen beschreiben**
- **Erklärung welche Rechte der Benutzer hat**
- **Kontaktmöglichkeit zum Betreiber des Webauftritts**

Bilder: pixabay.com, Einladung_zum_Essen

- **Link zur Plattform für Online-Streitbeilegung "https://ec.europa.eu/consumers/odr/" im Impressum bereitstellen**

Cookies [1]

schmid datensicherheit

Die EU-Vorgaben zu Cookies sind in der Verordnung 2009/136/EC des Europäischen Parlaments und des Rates geregelt: Cookie-Richtlinie

- **Die Cookie-Richtlinie der EU:**
  - Diese Richtlinie ist in Europa völlig uneinheitlich umgesetzt.
  - Richtlinie mit Opt-in implementiert: Dänemark, Frankreich, Großbritannien, Litauen, Niederlande, Österreich, Schweden und Spanien;
  - Richtlinie mit Opt-out implementiert: Bulgarien, Finnland, Luxemburg, Polen, Slovakei, Tschechien und Ungarn
  - Richtlinie nicht implementiert: Belgien, Deutschland, Estland, Griechenland, Italien, Lettland, Norwegen, Malta, Portugal und Zypern.
- **Cookies werden nach Anbieter unterschieden:**
  - First-Party-Cookies (Direktanbieter-Cookies): die Webseite muss den Benutzer informieren;
  - Third-Party-Cookies (Drittanbieter-Cookies): Werbeeinblendungen müssen direkt informieren (Icons).

Cookies [2]

schmid datensicherheit

Die rechtlichen Grundlagen sind im **TMG** (= Telemediengesetz) geregelt:

- **Oft ist die Information des Benutzers über Cookies durch ein pop-up-Fenster gelöst.**
  - Aktuell ist der Einsatz von pop-up-Fenstern mit Cookie-Hinweisen in Deutschland nicht notwendig, wenn die Verwendung von Cookies in der Datenschutzerklärung erläutert wird.
  - Strenge, zwingende Richtlinien für pop-ups gelten z.B. in Großbritannien.
- **Die Cookie-Policy kann generell als opt-out implementiert werden.**
  - Meistens kann man nur die Cookie-Information abnicken → Cookie-Behandlung kann durch Browser-plug-ins erfolgen.
  - Manchmal kann man Cookies "akzeptieren" oder "ablehnen". Die Besucher einer Webseite wollen aber, dass die Webseite funktioniert.
- **Empfänger, Funktionsweise, Zweck und Nutzung der Cookies (auch Ausschlussaspekte), Widerspruchsrecht des Benutzers beschreiben.**

Cookies [3]

schmid datensicherheit

Neue europäische Regelwerke sind im Genehmigungsprozess:

- **VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/**
  - **e-Privacy**-Richtlinie (Verordnung über Privatsphäre und elektronische Kommunikation)
- **Die Ausgestaltung der Cookie-Richtlinie steht erst fest, wenn die e-Privacy-Richtlinie der EU verabschiedet (geplant in 2019) und interpretiert ist.**
- **Es sollte eine allgemeine Diskussion angestoßen werden, ob die generelle Implementierung von pop-up-Fenstern auf allen Webseiten, die Cookies verwenden, dazu führt, Cookie-Hinweise grundsätzlich abzunicken. Für den Nutzer wäre dies kontraproduktiv für Fälle, in denen spezielle Hinweise zu beachten sind.**

Webtracking / Analytics

schmid datensicherheit

Webtracking, Web-Analytics und Software-Patch-Status (SW-Updates) werden von der Datenschutzaufsicht beobachtet:

- **Web-Analytics ist möglich mit Anonymisierung der IP-Adresse.**
- **Datenerfassung, Kategorien von Daten und Empfänger von Daten müssen explizit beschrieben werden.**
- **Die Aufsichtsbehörden arbeiten mit Tools, um Cookies und Tracking-, Analytics- und Fingerprinting-Aktivitäten auf Webseiten automatisiert untersuchen zu können.**
- **Die Aufsichtsbehörden werden sich auch die Patch-Aktivitäten der Webseiten-Betreiber (Verantwortliche Stelle (Unternehmen oder Verein) oder Hosting-Provider) ansehen, ob die den Webseiten zugrunde liegende Software (z.B. Wordpress, Apache, NGINX, ...) auf dem aktuellen Update-Stand betrieben wird.**

Email-Tracking

schmid datensicherheit

Email-Tracking wird von der Datenschutzaufsicht stark missbilligt:

- **Email-Tracking benutzt versteckte Tracking-Pixel (“web bugs,” “web beacons,” “pixel tags,” “clear GIFs” oder andere Bezeichnungen) um das Benutzerverhalten zu beobachten.**
- **In der Konferenz der europäischen Datenschutzbeauftragten wurde diese Praxis strikt abgelehnt.**
- **Nur eine eindeutige Einwilligung des Email-Empfängers rechtfertigt dieses Tracking.**
- **Es gibt noch keine abschließende Aussage der europäischen Datenschutzbehörde.**

Sichere Kommunikation [1]

schmid datensicherheit

Webauftritt*, Kontaktformular, Onlineshop, Bezahlvorgänge, u.s.w. generell mit https (X.509-Zertifikat für Webserver: Let's encrypt kostenlos, EV-Zertifikate (EV = extended Validation) bei Schmid Datensicherheit {Browserzeile wird grün}).

Verschlüsselter Datenaustausch zwischen einzelnen Anwendern und einem Anbieter für:

- **Versand einer digitalen Rechnung (mit digitaler Signatur)**
- **Einsendung von Daten und Dokumenten**
- **Beantwortung von konkreten Fragen mit Personenbezug**
- **...**

*** Wenn einzelne Seiten mit https arbeiten, sollte der ganze Webauftritt auf https umgestellt werden.**

Sichere Kommunikation [2]

schmid datensicherheit

Verschlüsselter Datenaustausch / Email-Verschlüsselung:

Gemäß dem BayLDA gelten für die Kommunikation zwischen einem Anbieter oder Dienstleister (z.B. Rechtsanwälte, Steuerberater) und seinen Klienten die folgenden Aussagen. Die Klienten sind in der Regel über 18 und für die sichere Übertragung ihrer Daten zum Dienstleister selbst verantwortlich. Aber: Anbieter und Dienstleister, die mit Klienten kommunizieren, müssen mindestens eine Lösung anbieten, Daten über einen gesicherten Kanal auszutauschen, wenn personenbezogene Daten eine nennenswerte Rolle spielen.

- **Online-Portal** (https) **/ Cloud-Lösung zum Upload und Download für individuellen Benutzer**
  - Vorteil: Läuft über den jeweiligen Provider, keine weiteren Kosten
  - Nachteil: Keine Historie im Email-Postfach welche Daten wann kommuniziert wurden, Zugriffsregelungen mit Authentisierung sind notwendig

Sichere Kommunikation [3]

schmid datensicherheit

Verschlüsselter Datenaustausch / Email-Verschlüsselung:

- **De-Mail – Dieser sichere elektronische Postfach- und Versanddienst für digitale Nachrichten basiert auf dem De-Mail-Gesetz, gültig seit 3.5.2011**
  - De-Mail-Dienste sind Dienste auf einer elektronischen Kommunikationsplattform, die einen sicheren, vertraulichen und nachweisbaren Geschäftsverkehr für jedermann im Internet sicherstellen sollen.
  - Ein De-Mail-Dienst muss eine sichere Anmeldung, die Nutzung eines Postfach- und Versanddienstes für sichere elektronische Post sowie die Nutzung eines Verzeichnisdienstes und kann zusätzlich auch Identitätsbestätigungs- und Dokumentenablagedienste ermöglichen.
  - Vorteil: De-Mail-Dienste werden ausschließlich von akkreditierten Anbietern erbracht. Die Diensteanbieter unterliegen der Aufsicht durch das BSI.
  - Nachteil: Der Kommunikationsraum De-Mail ist nicht kompatibel zu herkömmlichen E-Mail-Diensten.

Sichere Kommunikation [4]

schmid datensicherheit

Verschlüsselter Datenaustausch / Email-Verschlüsselung:

- **S/MIME** (X.509-Zertifikate für Email-Verschlüsselung und Email-Signatur)
  - Vorteil: Betriebssysteme unterstützen X.509, Zertifikate für Abteilungen möglich
  - Nachteil: Unterstützung auf Mobilgeräten nur mit speziellen Apps, Zertifikatverwaltung (1x) für jeden Empfänger
  - Die Schmid Datensicherheit GmbH bietet Ihnen Zertifikate für Email-Verschlüsselung und Email-Signatur mit unterschiedlicher Verifikationstiefe gegenüber dem Zertifikat-Inhaber der europäischen Zertifikat-Authority GlobalSign. Fragen Sie jederzeit unverbindlich an.

Sichere Kommunikation [5]

schmid datensicherheit

Verschlüsselter Datenaustausch / Email-Verschlüsselung:

- **Webmail-Portal mit Pull-Verfahren** (Empfänger holt sich Daten)
  - Nachteil: Empfänger muss sich authentisieren → Benutzername & Passwort, One-way-Transfer
- **Webmail-Portal mit Push-Verfahren** (Jede Email wird in ein anderes, geschütztes Format konvertiert)
  - Nachteil: Benutzerpasswort muss ausgetauscht werden, Benutzer benötigt Entschlüsselungs-Software, One-way-Transfer

Sichere Kommunikation [6]

schmid datensicherheit

Verschlüsselter Datenaustausch / Email-Verschlüsselung:

- **PGP** (Pretty Good Privacy, Signatur und Verschlüsselung von Emails, Verschlüsselung von Dateien und Verzeichnissen)
  - Nachteil: in die kostenpflichtige Security Suite von Symantec eingebunden, U.S. Firma
- **OpenPGP, GnuPG, GPG** (Freie PGP-Version)
  - Vorteil: Freeware, Shareware
  - Nachteil: kaum verbreitet, Stabilität der Software nicht immer gewährleistet
- **7-zip** (zip-Archiv mit AES-128 und Passwort, https://www.7-zip.org/)
  - Vorteil: 7-zip ist kostenlos; Open-Source-basierte freie Software, GNU LGPL license und andere Lizenzen
  - Nachteil: es muss ein Passwort über einen sicheren Drittkanal ausgetauscht werden
- **VPN, OpenVPN** (Virtual Private Network)
  - Probleme: verbindet Netzwerke auf IP-Ebene, macht nur Sinn bei "well-known" Kommunikationspartnern, komplexe Konfiguration

Emails mit S/MIME

schmid datensicherheit

S/MIME (Secure / Multipurpose Internet Mail Extensions) hat den Vorteil, dass alle gesendeten Emails digital signiert sind und damit eine höhere Vertrauenswürdigkeit aufweisen.

- **Durch die Signatur ist die Authentizität des Absenders gesichert.**
- **Der Empfänger kann das Zertifikat zur Verschlüsselung an den Absender benutzen.**
- **Es gibt keine Spam-Mails oder Fake-Mails, die digital signiert sind.**

Behörden identifizieren S/MIME mit einer entsprechenden Kennzeichnung, siehe Email an die Stadt Weiden:

Sicherheit bei Empfang unbekannter Mails mit Anhang:

Email-Client in einer virtuellen Maschine installieren. Es genügt ein System im Betrieb, auf dem man Anhänge "testen" kann. VMs: VMWare (VMWare), Virtual Box (Oracle), HyperV (Microsoft)

Digitale Identitäten

schmid datensicherheit

Management von Zugriffs-Berechtigungen erfordert Identifizierung:

- **Benutzername, Passwort** **(ist Standard bei fast allen Zugriffskontrollen)**
- **2-Faktor-Authentisierung mit Chipkarten oder Token**
- **Biometrie**
- **eID-Service mit elektronischem Personalausweis (nur) zur Authentisierung**
  - Ab 2021 sollte jeder Bundesbürger einen elektronischem Personalausweis (ePerso) haben
  - Es muss ein Lesegerät angeschafft werden, auch Smartphone (mit NFC) nutzbar
  - Der eID-Server muss von 1 Anbieter bezogen werden, das Zertifikat muss gekauft werden
  - Über ePerso abgesicherte Kommunikation benötigt Server mit https
  - Portale mit eID werden für öffentliche Stellen zunehmend verfügbar, im privatwirtschaftlichen Bereich ??

Authentisierung und Identifizierung im Web, für Cloud-Zugang, für Datenbank-Zugriff, für Soziale Netzwerke, für E-Mail-Anmeldung

Cloud-Dienste [1]

schmid datensicherheit

Die Auswahl von Cloud-Diensten sollte sich nach den Anforderungen der EU-Datenschutzgrundverordnung (Art. 5, 25, 32 DS-GVO), nach der Schutzklasse des Cloud-Dienstes und nach dem Standort der Rechenzentren richten.

- **Anbieter mit Zertifizierung auswählen:**
  - Welches Informationssicherheits-Managementsystem (ISMS) betreibt der Dienstleister?
  - Welche Datenschutz-Zertifizierung kann der Cloud-Dienst vorweisen?
    - Zertifizierung nach ISO27001, insbesondere ISO27018;
    - Trusted Cloud Datenschutz-Profil für Cloud-Dienste (TCDP);
      Die Bundesregierung hat das Projekt „Datenschutz-Zertifizierung für Cloud-Dienste“ gestartet. Das Ergebnis des Projekts ist ein „Trusted Cloud Datenschutzprofil, TCDP“ genannter Standard ("https://tcdp.de/").
  - Von wem ist die Zertifizierung bestätigt, wer führt die Audits durch?
- **Standort des Rechenzentrums:**
  - Wo sind die Standorte der Rechenzentren und wieviele davon betreibt der Anbieter?
  - Von wo erfolgt die Wartung und die Administration der Server im Rechenzentrum?

Cloud-Dienste [2]

schmid datensicherheit

Der Umgang mit Daten, die in einer Cloud gespeichert werden, sollte dem allgemeinen Datenschutzkonzept des Nutzers eines Cloud-Dienstes folgen und dem Schutzbedarf der Daten entsprechen.

- **Datenspeicherung in der Cloud mit Verschlüsselung:**
  - Vollverschlüsselung für Speicherung, Applikations-Server arbeiten mit offenen Daten;
  - Zugriff auf Datenspeicher in der Cloud sollte über offene Protokolle wie WebDAV erfolgen, client-seitige Software sollte unabhängig sein;
  - Duplicati ist eine freie populäre (LPGL) Software für verschlüsseltes, inkrementelles Backup;
  - Hintergrund: Der Anwender selbst ist das einfachste Angriffsziel, um Zugriff auf den Cloud-Speicher zu erschleichen → Phishing;
  - Risiko: Wenn der Zugang zum Cloud-Dienst kompromittiert ist, hat der Angreifer üblicherweise vollen Zugriff auf alle Daten, die gespeichert sind.

Biometrische Daten

schmid datensicherheit

Die DS-GVO enthält einige Erwägungspunkte zu biometrischen Daten, eine explizite datenschutzrechtliche Erweiterung auf Länderebene ist vorgesehen. Diskussionspunkte:

- **Passfotos sind ideale Ausgangsbilder zum Missbrauch biometrischer Identifikationssysteme.**
- **Passfotos fallen folglich unter die besonderen personenbezogenen Daten.**
- **Aber: Die Anzahl der Überwachungskameras steigt kontinuierlich und man hinterlässt auch täglich an unzähligen Stellen Fingerabdrücke.**
- **Fotografie-basierte Biometrie fängt erst da an, wo man beginnt, Merkmale aus einem Bild zu identifizieren.**
- **Biometrische Bildidentifikationssysteme arbeiten auf Basis sogenannter "local feature analysis".**
- **Mit guten Bildern und passender Hardware können solche Systeme (theoretisch) überlistet werden.**
- **Informationen siehe "https://facedetection.com/", "https://www.bioid.com/"**

Videoüberwachung

schmid datensicherheit

Videoüberwachung öffentlich zugänglicher Räume ist im BDSG-NEU geregelt.

- **Die Beobachtung ist nur zulässig, soweit sie für folgende Fälle erforderlich ist:**
  - zur Aufgabenerfüllung öffentlicher Stellen,
  - zur Wahrnehmung des Hausrechts oder
  - zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke (Abwägung der Interessen).
- **Umstand der Beobachtung und verantwortliche Stelle sind aufzuzeigen.**
- **Schutz von Leben, Gesundheit oder Freiheit, Abwehr von Gefahren**
- **Bei Zuordnung von Videoaufnehmen zu bestimmten Personen müssen diese informiert werden.**
- **Daten müssen nach Erreichen des Zwecks gelöscht werden.**

Risikobehandlung

schmid datensicherheit

Maßnahmenbeispiele (Risikobewertung, evtl. Datenschutz-Folgenabschätzung):

- **Datenminimierung**
- **Verschlüsselung**
- **Pseudonymisierung / Anonymisierung**
- **Rollen-/Rechtekonzepte**
- **Zugangs-, Zutritts- und Zugriffskontrolle**
- **Datenschutzmanagementsystem / (ISMS)**
- **Awareness / Datenschutzschulungen**
- **Trennung von Test-/Produktivsystemen**
- **Mandantentrennung**
- **Nicht-Verkettbarkeit**
- **Identifikationsprozesse**
- **Lösch-/Sperrkonzepte**

Bilder: pixabay.com, 3dman_eu

Verarbeitung im Auftrag

schmid datensicherheit

Beispiele für Datenweitergabe:

- **Externe Dienstleister**
- **Vermittler**
- **Berater**
- **Provider**
- **weitere .....**

Wichtig: Rollen-/Rechtekonzepte

→ **in der Regel DV-Vertrag notwendig, Auftraggeber haftet auch für den Auftragnehmer, Auftragnehmer haftet für Daten vom Auftraggeber**

→ **Prüfung der Datenverarbeitung vor der Durchführung der Verarbeitung (Vorabkontrolle, bei DV im Auftrag auch wechselseitig)**

Lohnabrechnung (als Beispiel)

schmid datensicherheit

Lohnabrechnung, Finanzbuchhaltung, Webhosting, Datenlöschung oder externe Callcenter sind typische Beispiele für Datenweitergabe und Auftragsverarbeitung:

- **Der Auftragnehmer verarbeitet personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO auf Grundlage eines Vertrages.**
- **Die Datenweitergabe erfordert eine Vorabkontrolle und einen Auftragsverarbeitungsvertrag.**
- **Der aufgrund eines Auftrages tätige Dienstleister ist weisungsgebunden. Er führt die Verarbeitung für den Auftraggeber nicht als Dritter durch. Es besteht ein "Innenverhältnis".**
- **Der Verwendungszweck der Daten sollte mit dem Auftragsverarbeiter vertraglich geregelt sein, damit keine Daten zusammenführt werden, um z.B. Personenprofile oder Gebietsprofile zu erstellen.**
- **Hier gab es zuletzt einige Änderungen, aktuelle Informationen einholen!**

Paketversand (als Beispiel)

schmid datensicherheit

Die Inanspruchnahme fremder Fachleistungen bei einem eigenständig Verantwortlichen und bei geeigneter Rechtsgrundlage stellt keine Auftragsverarbeitung dar:

- **Ein Paketversand und Online-Marktplätze, die selbstständig die Daten der Kunden verarbeiten, sind keine Auftragsverarbeiter.**
- **Die Datenweitergabe an den Versanddienstleister oder Dropshipper ist zur Vertragserfüllung erforderlich. Der Versanddienstleister gilt als ein Dritter (zur Auftragsabarbeitung) und ist kein Auftragsverarbeiter. Der Versanddienstleister arbeitet im Auftrag des Versenders und auf dessen Weisung.**
- **Bestimmte Dienstleistungen stellen eine Inanspruchnahme fremder Fachleistung bei einem eigenständig Verantwortlichen dar und bedürfen keines Auftragsverarbeitungsvertrages. Dies ist beispielsweise in der Regel die Einbeziehung eines:**

  Berufsgeheimnisträgers, Inkassobüros, Bankinstituts, Postdienstes

Veranstaltungen und Bilder

schmid datensicherheit

Datenschutz sinnvoll umsetzen:

- **Bei öffentlichen Veranstaltungen eine Kennzeichnung anbringen, dass Fotos für Unternehmenszwecke oder Vereinszwecke aufgenommen werden**
  Inhalt: Verantwortlicher, Kontaktmöglichkeit, Verwendungszweck, Widerspruchsrecht (Opt-out)
- **Dokumentation der Bildauswahl für die Veröffentlichung auf dem Webauftritt, ... Mitarbeiter oder Vereinsmitglieder bei Einwilligung ok, abgebildete Partner fragen, Personen im Hintergrund oder bei Panoramabilder sind Beiwerk** (meistens)
- **Vorlagenblatt anfertigen und für die Dokumentation ausfüllen und abheften (Archiv für die Zukunft)**
  - **Welche Veranstaltung, Datum**
  - **Welche Vereinsmitglieder waren anwesend (für evtl. Nachfragen)**
  - **Welche Fotografen haben Bilder aufgenommen (Bildnachweise im Impressum)**
  - **Wer hat an der Bildauswahl teilgenommen**
  - **Kompromittierende Bilder aussortieren**
  - **Bilder auswählen (und im Dokument festhalten)**

Spezialfälle

schmid datensicherheit

Weitere spezielle Punkte im Datenschutz:

- **Grenzüberschreitende Verarbeitung, Marktortprinzip**
- **One Stop Shop** (Federführende Aufsichtsbehörde bei grenzüberschreitender Verarbeitung)
- **Speicherfristen** (was darf konkret wie lange gespeichert werden?)
- **Löschkonzept** (Löschen/Vernichten von Speichermedien, Papier-Shredder) (wie gestaltet man ein rechtssicheres Lösch- und Backup-Konzept?)
- **Datenschutzanforderungen an App-Entwickler und App-Anbieter** (Mobile Endgeräte)
- **Einhaltung von Rechtsvorschriften zur Kreditvergabe** (Basel III), **Reputation des Unternehmens**

Es gibt inzwischen Vorlagen für "**Quälbriefe**" zur Datenabfrage !!!

Erweiterte Anforderungen

schmid datensicherheit

Spezielle Erwartungen und Maßnahmen im Datenschutz:

- **Verständliche, klare und einfache Sprache → Transparenz**
- **Verschlüsselung personenbezogener Daten in öffentlichen Netzen: https, VPN, E-Mail-Verschlüsselung, passwort-gesicherte Dateien**
- **Umsetzung erhöhter Anforderungen im Umgang mit Gesundheitsdaten**
- **Verschlüsselte Datenträger für personenbezogene Daten, wenn die Datenträger im öffentlichen Raum transportiert werden, oder exklusive Datenverarbeitung über gesicherte Remote-Verbindungen auf internen Serversystemen der verantwortlichen Stelle. Anfragen dazu können Sie jederzeit an die Schmid Datensicherheit GmbH richten.**
- **Festplattenverschlüsselung und inhouse-https im Netzwerk (z.B.) bei "besonderen" personenbezogenen Daten (oder vergleichbares Sicherheitsniveau)** (Crypto-Speicher, ...)
- **Patch-Management zur Sicherstellung der Aktualität der benutzten IT-Systeme, geordnete Software-Updates der Betriebssysteme und Anwendungen**
- **Einhaltung der länderspezifischen Anpassungen:**
  → Datenschutz-Anpassungs- und Umsetzungsgesetz (EU DSAnpUG-EU)
  auch: BDSG-NEU

Zusammenfassung

schmid datensicherheit

Die wichtigsten Schritte in Kürze:

- **Anlegen eines Verfahrensverzeichnisses**
- **Datenschutzerklärung / Social Media**
- **Anpassung Internetseite / Webshop**
- **Prüfung der Vereinssatzung und ggf. diese ergänzen**
- **Texte für die Information von Betroffenen und für mögliche Auskunftsersuchen erstellen**
- **soweit erforderlich gesonderte Einholung von Einwilligungen (Mitarbeiter, Mitglieder, Newsletter, Direkterhebung, Messeakquise)**
- **soweit erforderlich Verpflichtungserklärungen und Dienstvereinbarungen unterzeichnen (Mitarbeiter)**

Hinweise [1]

schmid datensicherheit

Bayerisches Landesamt für Datenschutzaufsicht (BayLDA)

Datenschutz in Bayern für den nicht-öffentlichen Bereich

Promenade 27 (Schloss), 91522 Ansbach

https://www.lda.bayern.de/

Der Bayerische Landesbeauftragte für den Datenschutz (BayLfD)

Zuständigkeit für bayerische öffentliche Stellen

Wagmüllerstraße 18, 80538 München

https://www.datenschutz-bayern.de/

Hinweise [2]

schmid datensicherheit

Hinweise zu gesetzlichen Informationen:

- **Gesetzliche Grundlagen:**
  Datenschutz-Grundverordnung (EU DS-GVO) ab 25. Mai 2018 anwendbar
  – https://dsgvo-gesetz.de/
- **Bundesdatenschutzgesetz:**
  – https://dsgvo-gesetz.de/bdsg-neu/
- **Bayerisches Datenschutzgesetz (BayDSG)** vom 15. Mai 2018:
  – http://www.gesetze-bayern.de/Content/Document/BayDSG
- **Weg zur DS-GVO – Selbsteinschätzung:**
  – https://www.lda.bayern.de/tool/start.html

Hinweise [3]

schmid datensicherheit

Spezifische Informationen:

- **Handreichungen für kleine Unternehmen und Vereine:**
  – https://www.lda.bayern.de/de/kleine-unternehmen.html
- **Verzeichnis von Verarbeitungstätigkeiten:**
  Bayerisches Landesamt für Datenschutzaufsicht (Vorlage)
  – https://www.lda.bayern.de/media/dsk_muster_vov_verantwortlicher.pdf
- **Fragebogen zur Umsetzung der DS-GVO:**
  – https://www.lda.bayern.de/media/dsgvo_fragebogen.pdf
- **Häufig gefragt - FAQ für Vereine** (Bayerisches Landesamt)**:**
  Das BayLDA beantwortet 10 Fragen zur Umsetzung der DS-GVO bei Vereinen und Ehrenamtlichen
  – https://www.lda.bayern.de/de/faq.html

Hinweise [4]

schmid datensicherheit

- **Webauftritt der Datenschutzkonferenz (DSK):**
  Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder
  – https://www.datenschutzkonferenz-online.de/
- **Anforderungen an Datenschutzbeauftragte (Aufsichtsbehörde Bayern) / (Wenn zu bestellen):**
  – https://www.lda.bayern.de/media/dk_mindestanforderungen_dsb.pdf
- **Meldung des Datenschutzbeauftragten an die Aufsichtsbehörde (Bayern) / (Wenn bestellt):**
  – https://www.lda.bayern.de/de/dsb-meldung.html
- **Meldung Datenschutzverletzung (Bayern) Innerhalb von 72 Stunden! (Art. 33 DS-GVO):**
  – https://www.lda.bayern.de/de/datenpanne.html

Hinweise [5]

schmid datensicherheit

- **Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit:**
  – https://www.bfdi.bund.de/DE/Home/home_node.html
- **Gesetz zur Regelung des Zugangs zu Informationen des Bundes** (Informationsfreiheitsgesetz - IFG)**:**
  – https://www.gesetze-im-internet.de/ifg/IFG.pdf
- **Datenschutzgeneratoren für Internetseiten:**
  Bund der Selbständigen - Gewerbeverband Bayern e.V
  – https://www.bds-bayern.de/datenschutzgenerator/
- **Rechtsanwaltskanzlei Dr. Thomas Schwenke:**
  – https://datenschutz-generator.de/
- **Generator für kostenlose Datenschutzerklärung – eRecht24 GmbH & Co. KG:**
  – https://www.e-recht24.de/muster-datenschutzerklaerung.html

Hinweise [6]

schmid datensicherheit

Datenarme Konfiguration von Windows 10:

- **Hinweise zur datenschutzfreundlichen Nutzung von Windows 10 des Landesbeauftragten für den Datenschutz in Baden-Württemberg:**
  – https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2016/04/2016-04_leitfaden_win10.pdf#
- **Orientierungshilfe des Arbeitskreises Informationssicherheit der deutschen Forschungseinrichtungen (AKIF):**
  – https://www.it-sicherheit.mpg.de/Orientierungshilfe_Windows10.pdf

Hinweise [7]

schmid datensicherheit

EU-U.S. and Swiss-U.S. Privacy Shield Frameworks

https://www.privacyshield.gov/welcome

https://www.privacyshield.gov/European-Businesses

NOYB – European Center for Digital Rights – Wien

"*Privacy is none of your business*"

https://noyb.eu/

Mag. Max Schrems, Dr. Petra Leupold, Dr. Christof Tschohl

Kontakt

schmid datensicherheit

Dipl.-Ing. (Univ.) Lutz J. Schmid

Schmid Datensicherheit GmbH

Heidestraße 4

92637 Weiden / Opf.

Tel.: 0961-4712941

Mobil: 0160-98492962

Email: info@schmid-datensicherheit.de

URL: www.schmid-datensicherheit.de

ENDE

schmid datensicherheit

Vielen Dank für das Interesse!