

Modul M231

Datenschutz und Datensicherheit anwenden

Allgemeine Informationen

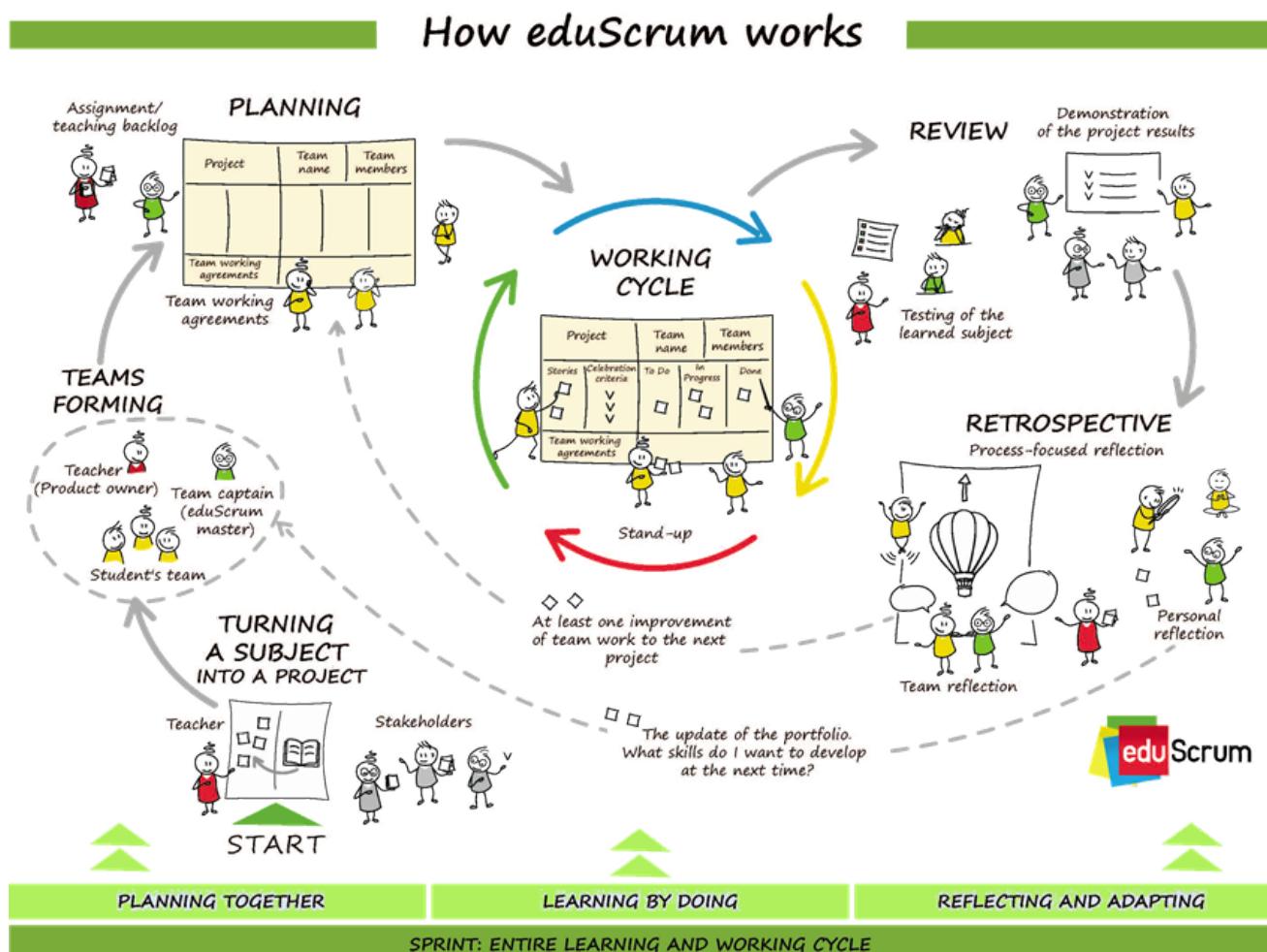
Modulbeschreibung

-  Modulidentifikation

Quartalsübersicht

Woche	Datum	Thema	Leistungsbewertung
Woche 1	27.04.2023	Theory zu eduScrum	
Woche 2	04.05.2023	Sprint 1	
Woche 3	11.05.2023	Sprint 1	
Woche 4	25.05.2023	Sprint 1	Sprint 1 Review
Woche 5	01.06.2023	Sprint 2	
Woche 6	08.06.2023	Sprint 2	
Woche 7	15.06.2023	Sprint 2	Sprint 2 Review
Woche 8	15.06.2023	Sprint 3	
Woche 9	15.06.2023	Sprint 3	Sprint 3 Review

Theory zu eduScrum



Quelle: <https://eduscrum.org/how-eduscrum-works/#how>

Themen

Sprint

Das Herzstück von eduScrum® ist der Sprint, ein zusammengesetzter Satz von Lernmateri...

Planung

Die während eines Sprints auszuführenden Arbeiten werden während der Sprintplanungssit...

Review

Die Sprint Reviews finden während des gesamten Sprints wiederholt statt, damit sich die T...

Retrospektive

Die Sprint Retrospektive ist für das Lernendenteam der Moment, in dem sie auf ihre geleist...

Stand-up (Daily)

Das Stand Up ist eine fünfminütige, zeitlich begrenzte Veranstaltung für das Lernendentea...

Working Cycle

Team Forming

Rollen in eduScrum

Tools

Kanban Board pro Gruppe:

Sprint

Das Herzstück von eduScrum® ist der Sprint, ein zusammengesetzter Satz von Lernmaterialien, die sicherstellen, dass die Lernziele erreicht werden. Ein Sprint kann eine kontextreiche Unterrichtsreihe, ein Projekt, ein Kapitel aus einem Buch usw. sein. Im Allgemeinen fällt ein Sprint mit der Länge eines Semesters oder einer Periode zusammen, obwohl dies keine Voraussetzung ist. Ein Sprint hat in der Regel eine voreingestellte Zeitbox (Periode) von ungefähr sieben Wochen. Das hängt auch von den jeweiligen zeitlichen Rahmenbedingungen ab. Wenn eine längere Sprintdauer verwendet wird, wird es für Lernendenteams schwieriger, die Komplexität zu überblicken und gut zu planen. Einige Teams, insbesondere kürzlich gestartete Teams, haben Schwierigkeiten, den gesamten Sprint im Voraus zu planen. Sie können dann zu Beginn des Sprints Umrisse planen und die Planung während des Sprints detaillierter ergänzen. Der Sprint beginnt mit einer Sprintplanungssitzung und der Teambildung. Die Teams entscheiden selbst, was sie in dieser Zeit tun werden. Das WIE bestimmen die Lernendenteams immer selbst.

Der Sprint besteht aus:

- Sprint Planungsbesprechung mit Teambildung
- Stand Up, zu Beginn jeder Lektion
- Ausführen von Aufträgen und Aufgaben
- Sprint Review
- Retrospektive auf den Sprint und persönliche Reflexion

Während des Sprints:

- bleibt die Zusammensetzung des Lernendenteams gleich
- die Aufgabe bleibt die gleiche.
- kann die Qualität geklärt und zwischen Lehrer- und Schülerteam neu verhandelt werden, wenn mehr gelernt wird.

Der Sprint endet mit einem Review und einer Retrospektive, in der die abgeschlossene Arbeit überprüft und Verbesserungsmaßnahmen festgelegt

werden. Es finden Zwischenüberprüfungen (Reviews) statt, um ihren Teil der Arbeit anzupassen und zu verbessern (falls erforderlich). Während des Sprints überprüft der Lehrer regelmäßig, ob die Teams im Hinblick auf die angestrebten Ergebnisse noch auf Kurs sind. In einigen Fällen wird dafür innerhalb des Sprints ein zusätzlicher fester und wiederkehrender Termin vereinbart. Wie in Scrum haben wir auch in eduScrum® das Motto "Testen im Sprint", was wir als Reviews bezeichnen. Der Dozent betont regelmäßig, dass die gelieferte Arbeit vom Team selbst getestet werden muss. Die Schülerteams können sich dazu nach eigenem Ermessen alle möglichen Methoden ausdenken, indem sie sich

Quelle: <https://art2beagile.slab.com/public/posts/edu-scrum-guides-2-0-fk6r8ill>

Planung

Die während eines Sprints auszuführenden Arbeiten werden während der Sprintplanungssitzung geplant. Die Erstellung dieses Plans ist eine gemeinsame Aufgabe des gesamten Lernendenteams. Zunächst bietet der Lehrende einen Überblick über die Aufgabe, die Anzahl der Stunden, die Anzahl der Stunden, die ein Sprint dauert, die zentralen, gemeinsamen Momente, das Abgabedatum, die Bewertungsmodelle und ähnliches. Er legt also den Rahmen fest, innerhalb dessen die Lernenden ihre Eigenverantwortung ausüben und ihre Planung erstellen können. Das Sprintplanungstreffen ist ein Treffen innerhalb eines Zeitrahmens von zwei Stunden für einen Sprint von etwa 2 Monaten. Dieser Zeitrahmen gilt auch für kürzere Sprints.

Das Sprintplanungstreffen beantwortet jeweils die folgenden Fragen:

- Was wird im nächsten Sprint vom Lernendenteam erwartet; was ist das Lernziel, welche Themen werden behandelt, was sind die Celebration Criteria und welche Planungsabhängigkeiten gibt es?
- Was muss getan werden, um das Lernziel zu erreichen, in welcher Reihenfolge und von wem?

Der Lehrer stellt das/die Lernziel(e) dem Schülerteam vor und erklärt dies so, dass das gesamte Lernendenteam eine gute Vorstellung davon hat, was von ihnen während dieses Sprints erwartet wird. Die Lernziele müssen so erklärt werden, dass das Lernendenteam die Lernziele in einer gemeinsamen Planungssitzung für den kommenden Sprint selbstständig erarbeiten kann. Nachdem der Lehrer die Lernziele erklärt hat, ist es Sache des Lernendenteams, die erforderliche Arbeit abzubilden. Das Team ist in erster Linie für den Umfang der Aufgaben und Komponenten verantwortlich. Sobald bekannt ist, was zu tun ist, beginnt das Lernendenteam damit, die Aufgaben und Teile chronologisch zu ordnen, basierend auf den Erkenntnissen des Lehrers und den Celebration Criteria. Sobald alle Aufgaben und Teile chronologisch geordnet sind, kann die erste Unterteilung der Aktivitäten erfolgen. Während dieser Planungssitzung wird nur ein erster Start gegeben. Schließlich führt der Prozess der Überprüfung und Anpassung zu immer

neuen Erkenntnissen und möglicherweise auch zu Anpassungen in der Planung und Arbeitsverteilung.

Quelle: <https://art2beagile.slab.com/public/posts/edu-scrum-guides-2-0-fk6r8ill>

Review

Die Sprint Reviews finden während des gesamten Sprints wiederholt statt, damit sich die Teams auf die Qualität der Arbeit konzentrieren können, die sie am Ende abliefern müssen. In der Zwischenzeit präsentieren die Teams, was sie während des gesamten Einsatzes erreicht haben. Diese Ergebnisse werden mit den Lernzielen verglichen. Die Form hängt von dem/den Lernziel(en) und den Celebration Criteria ab. Während des Sprints ist es wichtig, so oft wie möglich zu überprüfen (inspizieren) und anzupassen, aber nicht so oft, dass der Lernprozess dadurch beeinträchtigt wird. Generell lässt sich sagen, dass die Erfolgschancen umso größer sind, je öfter man Überprüfungsmomente und Anpassungen anwendet. Wann eine Überprüfung stattfindet und wie sie bewertet wird, wird im Voraus mit dem Lernendenteam zu Beginn des Sprints (während der Sprintplanung) festgelegt. Diese Überprüfungsmomente helfen den Teams, einzuschätzen, wo sie im Hinblick auf den Fortschritt der zu erreichenden Lernziele stehen, und möglichst viel Feedback zu ihren Zwischenergebnissen zu erhalten.

Quelle: <https://art2beagile.slab.com/public/posts/edu-scrum-guides-2-0-fk6r8ill>

Retrospektive

Die Sprint Retrospektive ist für das Lernendenteam der Moment, in dem sie auf ihre geleistete Arbeit und ihre persönliche und Team-Entwicklung zurückblicken. Die Sprint Retrospektive wird so bald wie möglich durchgeführt, nachdem sie ihre Lernarbeiten abgeschlossen haben und die Noten für die Abschlussarbeit bekannt sind. Die Retrospektive muss mit ausreichender Tiefe durchgeführt werden, so dass sowohl das Team als auch die einzelnen Mitglieder sie nutzen können, um einen Plan zu erstellen, wie sie sich beim nächsten Sprint verbessern können. Jede Verzögerung der Retrospektive ist eine potentiell verpasste Gelegenheit, Verbesserungen für die Teams und die Lernenden im nachfolgenden Sprint umzusetzen.

Der Zweck der Sprint Retrospektive ist es:

- eine Retrospektive (Rückblick) auf den Verlauf des letzten Sprints in Bezug auf Menschen, Beziehungen, Prozesse und Werkzeuge zu erhalten;
- Punkte, die gut gelaufen sind, und potenzielle Verbesserungen zu identifizieren und zu organisieren; und,
- einen Plan zur Umsetzung von Verbesserungen in der Art und Weise, wie das Lernendenteam seine Arbeit erledigt, zu erstellen.

Die Sprint-Retrospektive besteht aus drei Teilen;

1. Der Lernende bewertet die vom Team angewandten Methoden und Verfahren und identifiziert Verbesserungspunkte;
2. Der Lernende bewertet dann seine Teamkollegen hinsichtlich möglicher Fähigkeiten und Punkten, die verbessert werden können. Dies erfolgt für jeden Lernenden zunächst in Einzelarbeit.
3. und überlegt, was sie anders machen können. Als Ergebnis lernt das Lernerteam, gemeinsam effektiv und effizient zu lernen. Die Retrospektive ist daher ein sehr wichtiger und wesentlicher Bestandteil von eduScrum® und sollte im eduScrum®-Prozess auf keinen Fall fehlen. Sie findet statt, nachdem der gesamte Auftrag erledigt ist.

Das Lernendenteam beantwortet die folgenden vier Fragen sowohl individuell als auch kollektiv:

- Was ist gut gelaufen?
- Was kann oder muss verbessert werden?
- Was sollten wir nicht mehr tun?
- Welche positiven Aktionen werden wir mit uns in den nächsten Sprint nehmen?

Persönliche Reflexion

Die Lernenden erhalten durch die Retrospektive eine Menge Feedback. Sie erfahren zum Beispiel, wie andere Menschen über ihre Arbeit denken. Oft ist das Feedback gut und motivierend. Aber sie lernen auch, ihr eigenes Handeln kritisch zu betrachten, wo sie sich verbessern können. Mit diesem Feedback können sie anfangen, beim nächsten Mal etwas besser zu machen! Retrospektive und persönliche Reflexion ermöglichen es den Teams, besser zusammenzuarbeiten. Sie sind enorm wichtige Schritte in einem Prozess der ständigen Verbesserung (Kaizen). Am Anfang hat der Lernende viel Freiheit, Reviews, Retrospektiven und persönliche Reflexionen auszufüllen. Der Lehrer wird ihn darin coachen, weiter zu wachsen. Auf diese Weise wird der eduScrum® Prozess nicht nur immer besser und besser, sondern auch der Lernende und sogar der Lehrende und wachsen als Teamplayer und als Person.

Quelle: <https://art2beagile.slab.com/public/posts/edu-scrum-guides-2-0-fk6r8ill>

Stand-up (Daily)

Das Stand Up ist eine fünfminütige, zeitlich begrenzte Veranstaltung für das Lernendenteam, um Aktivitäten zu synchronisieren und einen Plan für aktuell anstehende Unterrichtsstunde/Arbeitseinheit zu erstellen. Das Stand Up findet zum Anfang jeder Einheit statt. Dabei wird die Arbeit seit dem letzten Stand Up überprüft und vorausgesagt, welche Arbeiten bis zum nächsten Stand Up durchgeführt werden können. Das Stand Up wird bei jeder Session und zur gleichen Zeit, nämlich zu Beginn, durchgeführt, um die Komplexität zu reduzieren und Regelmäßigkeit zu schaffen. Während des Treffens erklärt jedes Teammitglied Folgendes:

- Was habe ich seit der letzten Unterrichtsstunde getan, um dem Team zu helfen?
- Was werde ich in dieser Lektion tun, um dem Team zu helfen?
- Was sind die Hindernisse, die mir oder dem Team im Weg stehen?

Das Team nutzt das Stand Up, um den Fortschritt im Hinblick auf das Lernziel zu bewerten und zu überwachen, die Arbeit neu zu planen und Arbeitsvereinbarungen zu treffen. Das Stand Up erhöht die Wahrscheinlichkeit, dass das studentische Team das Lernziel mit dem bestmöglichen Ergebnis erreicht. Das Lernendenteam muss in der Lage sein, dem Lehrer zu erklären, wie es als selbstorganisierendes Team zusammenarbeiten wird, um das Lernziel zu erreichen, und wie die Arbeit im weiteren Verlauf des Sprints aussehen wird. Der Teamkapitän sorgt dafür, dass das Team die Sitzung abhält, aber das Team selbst ist für die Durchführung des Stand Ups verantwortlich. Der Teamkapitän hilft dem Lernendenteam, das Stand Up innerhalb der Fünf-Minuten-Frist durchzuführen. Stand Ups verbessern die Kommunikation, identifizieren und beseitigen Entwicklungshindernisse, betonen und fördern eine schnelle Entscheidungsfindung und verbessern den Wissensstand des Teams in Bezug auf das Projekt. Dies ist ein sehr wichtiges Treffen.

Quelle: <https://art2beagile.slab.com/public/posts/edu-scrum-guides-2-0-fk6r8ill>

Working Cycle

Team Forming

Rollen in eduScrum

Teacher - Product Owner

Der Dozent hat eigentlich eine hybride Rolle als Product Owner und eduScrum®-Master (mit dem Ziel, dies dem studentischen Teamkapitän zu übergeben). Als Product Owner und eduScrum®-Master ist der Dozent verantwortlich für die Festlegung der zu erreichenden Lernziele und deren Bewertung, die Überwachung des eduScrum®-Prozesses und die Erleichterung des Lernprozesses der einzelnen Lernenden der Lernendenteams; wie z.B. Bezugnahme auf den Lernstoff, Beantwortung von Fragen und Bezugnahme auf Beispiele. Darüber hinaus ist der Lehrer auch für die Förderung der teamübergreifenden Zusammenarbeit verantwortlich. Wie genau dies geschieht, ist für verschiedene Organisationen, Teams und Individuen unterschiedlich.

Der/die Lehrende:

1. bestimmt, WAS und WARUM gelernt werden soll
2. überwacht und verbessert die Qualität der dem jeweiligen Curriculum entsprechenden Lernergebnisse
3. testet und bewertet die Lernergebnisse und überwacht die persönliche Entwicklung
4. hat verschiedene Rollen

Team Captain - eduScrum Master

Innerhalb des Lernendenteams spielt eines der Mitglieder die Rolle des Teamkapitäns. Der Teamkapitän ist nicht der Chef, sondern auch ein arbeitendes Mitglied des Teams. Er oder sie sorgt dafür, dass das Team optimale Leistungen erbringen kann - ohne jedoch über dem Team zu stehen, sind sie in erster Linie ein

gleichberechtigtes Teammitglied. Innerhalb von eduScrum® ist der Teamkapitän eine begrenztere Rolle als die Rolle des Scrum Master innerhalb von Scrum. Dies liegt daran, dass dem Dozenten verschiedene Aufgaben und Verantwortlichkeiten zugewiesen werden, die Teil der Rolle des Scrum Masters wären. Wenn die „Teamcaptains“ mehr Erfahrung haben, können sie mehr Verantwortung vom Lehrer übernehmen, was bedeutet, dass die Gesamtverantwortung des Lehrers allmählich abnimmt. Die Rolle des Teamkapitäns wird während der Teambildung zu Beginn des ersten Sprints gewählt. Der Mannschaftskapitän wird vom Lehrer bestimmt oder von den Schülern gewählt. Dann wählen die Teamkapitäne, je nach dem für die Teambildung angewandten Verfahren, ihre Teammitglieder auf der Grundlage sich ergänzender Eigenschaften aus. Innerhalb des Lernendenteams ist der Teamcaptain für den "Flap" verantwortlich. Der "Flap" ist die visuelle Tafel, die die Arbeit und die Vereinbarungen des Teams sichtbar macht. Der Teamkapitän sorgt dafür, dass der "Flap" bei Bedarf zur Verfügung steht und dass er aktualisiert worden ist. Die endgültige Arbeit liegt jedoch in der Verantwortung des gesamten Teams. Darüber hinaus unterstützt der Teamkapitän den Lehrer und das Schülerteam. Die Interpretation der Rolle des Teamkapitäns liegt grundsätzlich in der Verantwortung des Lehrers. Je besser die Teams werden, desto mehr Verantwortung kann jedoch an den Teamkapitän delegiert werden.

Lernendenteam

Das Lernendenteam besteht aus unabhängigen Lernenden, die die Arbeit gemeinsam erledigen, um die gesetzten Lernziele am Ende des Sprints gemäß der Celebration Criteria zu erreichen. Die Mitglieder sind gemeinsam, als Team, für die Erfüllung der Celebration Criteria verantwortlich. Die Schülerteams werden vom Lehrer strukturiert und mit Befugnissen ausgestattet, damit sie ihre Arbeit selbst organisieren und verwalten können. Dieser Vorgehensweise verbessert die Effektivität und Effizienz, aber auch die Lernerfahrung und das persönliche Wachstum (effektiv zu sein bedeutet, die richtigen Dinge zu tun. Effizient zu sein bedeutet, die Dinge gut zu machen).

Lernendenteams haben die Folgenden Merkmale:

- Sie sind selbstorganisierend. Niemand (nicht einmal der Lehrer) sagt dem Lernendenteam, wie die Lernziele erreicht werden sollen.
- Die Lernendenteams sind multidisziplinär und verfügen über alle notwendigen Fähigkeiten und persönlichen Entwicklungsbereiche, um die Lernziele als Team zu erreichen und sich persönlich weiterentwickeln zu können;
- Die Mitglieder des Lernendenteams können spezifische Fähigkeiten oder Schwerpunktbereiche haben, aber die Verantwortung liegt beim Lernendenteam als Ganzes;
- Die Teammitglieder können selbst entscheiden, ob sie ihre Qualitäten nutzen oder neue Bereiche entwickeln wollen;
- Das Lernendenteam überwacht seinen Fortschritt und sein Qualitätsniveau selbst, u.a. auf der Grundlage der Celebration Criteria und der Arbeitsvereinbarungen (Definition of Doing & Definition of Fun).

Grosse des Lernendenteams

Die optimale Teamgröße ist klein genug, um arbeitsfähig zu bleiben, und groß genug, um signifikante Arbeit zu leisten. Als Faustregel gilt: Teams von vier oder fünf Mitgliedern. Weniger als drei Teammitglieder bedeutet, dass die Interaktion abnimmt und Fähigkeiten unzureichend vertreten sind. Mehr als sechs Mitglieder im Team erfordern zu viel Koordination. Große Teams erzeugen zu viel Komplexität, um durch einen empirischen Prozess kontrolliert werden zu können.

Quelle: <https://art2beagile.slab.com/public/posts/edu-scrum-guides-2-0-fk6r8ill>

Tools

Kanban Board pro Gruppe: <https://kanboard.aebi.cloud/>

Sprint - Rechtlicher Rahmen

Epics



Schweiz DSG

Welche Gesetze gibt es in der Schweiz zum Thema Datenschutz und was beeuten diese fü...



EU DSGVO

Welche Gesetze gibt es in der EU zum Thema Datenschutz und was beeuten diese für uns ...



Copyright CH und EU

Was ist ein Urheberrecht?



Lizenzen

Was ist eine Lizenz?



Impressum, Disclaimer, AGBs

Was braucht eine Webseite?

Handlungsziel

- ▼ 5. Zeigt Konsequenzen von Fehlern im Datenschutz und bei der Datensicherheit auf.

Handlungsnotwendige Kenntnisse:

1. Kennt die Problematik von Datenlöschungen über alle Archive und Backups.
2. Kennt wesentliche juristische Voraussetzungen und Eigenheiten von Websites (z.B. Impressum, Disclaimer, AGBs).

Schweiz DSG

ⓘ NOTE

Welche Gesetze gibt es in der Schweiz zum Thema Datenschutz und was beeuten diese für uns als Informatiker.

▼ 🎉 Celebration Criteria

Kategorisiert Daten aufgrund ihres Schutzbedarfs.

Kennt verschiedene Rechtsräume (Schweiz, EU).

Kennt für den jeweiligen Rechtsraum die juristischen Werke (z. B. DSG, DSGVO).

Überprüft eingesetzte Anwendungen auf Einhaltung der Datenschutzgesetze.

Kennt wesentliche Unterschiede in den Datenschutzgesetzen der verschiedenen Rechtsräume.

Zeigt Konsequenzen von Fehlern im Datenschutz und bei der Datensicherheit auf.

Kennt die Problematik von Datenlöschungen über alle Archive und Backups.

▼ 😊 Quellen für die Uninspierierten

- **CH EDÖB:** Datenschutz
- **CH:** DSG
- **CH:** Art. 13 der Bundesverfassung

- [CH: Verordnung zum Bundesgesetz über den Datenschutz](#)
- [CH: Art. 28-28l Zivilgesetzbuches \(ZGB\)](#)
- [KMU CH Admin: revDSG](#)
- [Hostpoint: Blog](#)

Information

Einstieg ins Thema

Was ist Datenschutz?

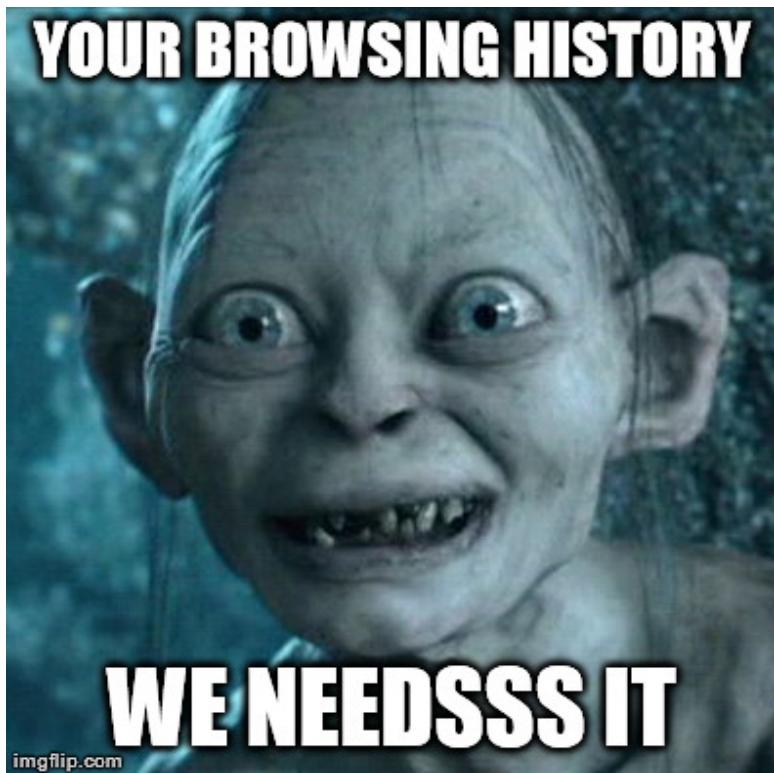
Gesetzliche Vorschriften zum Schutz von personenbezogenen Daten.



 [Bildquelle](#)

Was ist das Ziel des Datenschutzes?

Das die Privatsphäre von Naturlichen Personen bei der Verarbeitung von Daten respektiert wird.



📎 Bildquelle

Was ist "privacy by design"?

Der Datenschutz als Design Grundsatz beim Planen und Umsetzen von Infrastruktur und Software genommen. z.B. werden nur die absolut notwenigen Daten erhoben

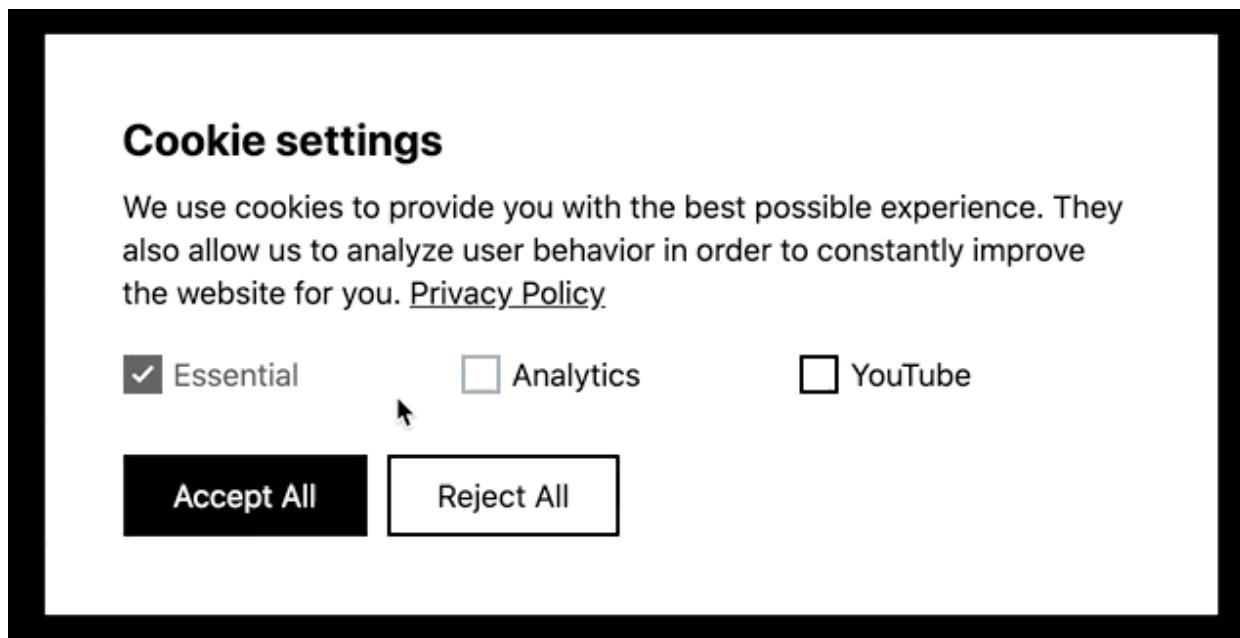
Grundsätze des "Privacy by Design"



Bildquelle

Was ist "privacy by default"?

Wenn es eine Wahl gibt wird die Datenschutz freundlichste Variante als Standard gesetzt. z.B. Cookies etc. bei den Webseiten



[Bildquelle](#)

DSG Kompakt

Gesetzt in der Schweiz

Art. 13 Schutz der Privatsphäre

1 Jede Person hat Anspruch auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihres Brief-, Post- und Fernmeldeverkehrs. 2 Jede Person hat Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten.

CH: Art. 13 der Bundesverfassung

Datenschutz Gesetz

Art. 1 Zweck Dieses Gesetz bezweckt den Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen, über die Personendaten bearbeitet werden.

CH: DSG

Rechte von Betroffenen

- Art. 25 Auskunftsrecht

1. Jede Person kann vom Verantwortlichen Auskunft darüber verlangen, ob Personendaten über sie bearbeitet werden. ...
 - Art. 26 Einschränkungen des Auskunftsrechts
 - Art. 27 Einschränkungen des Auskunftsrechts für Medien
 - Art. 28 Recht auf Datenherausgabe oder -übertragung

1. Jede Person kann vom Verantwortlichen die Herausgabe ihrer Personendaten, die sie ihm bekanntgegeben hat, in einem gängigen elektronischen Format verlangen, wenn:
 - a. der Verantwortliche die Daten automatisiert bearbeitet; und
 - b. die Daten mit der Einwilligung der betroffenen Person oder in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags zwischen dem Verantwortlichen und der betroffenen Person bearbeitet werden.

- Art. 29 Einschränkungen des Rechts auf Datenherausgabe oder -übertragung

Pflicht von Unternehmen

- Art. 6 Grundsätze
 1. Personendaten müssen rechtmässig bearbeitet werden.
 2. Die Bearbeitung muss nach Treu und Glauben erfolgen und verhältnismässig sein.
 3. Personendaten dürfen nur zu einem bestimmten und für die betroffene Person erkennbaren Zweck beschafft werden; sie dürfen nur so bearbeitet werden, dass es mit diesem Zweck vereinbar ist. ...

- Art. 7 Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

- Art. 8 Datensicherheit

- Art. 12 Verzeichnis der Bearbeitungstätigkeiten

1. Die Verantwortlichen und Auftragsbearbeiter führen je ein Verzeichnis ihrer Bearbeitungstätigkeiten. ...
 - Art. 19 Informationspflicht bei der Beschaffung von Personendaten

1. Der Verantwortliche informiert die betroffene Person angemessen über die Beschaffung von Personendaten; diese Informationspflicht gilt auch, wenn die Daten nicht bei der betroffenen Person beschafft werden. ...
 - Art. 20 Ausnahmen von der Informationspflicht und Einschränkungen
 - Art. 21 Informationspflicht bei einer automatisierten Einzelentscheidung

1. Der Verantwortliche informiert die betroffene Person über eine Entscheidung, die ausschliesslich auf einer automatisierten Bearbeitung beruht und die für sie mit einer Rechtsfolge verbunden ist oder sie erheblich beeinträchtigt (automatisierte Einzelentscheidung). ...
 - Art. 22 Datenschutz-Folgenabschätzung

1. Der Verantwortliche erstellt vorgängig eine Datenschutz-Folgenabschätzung, wenn eine Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann. Sind mehrere ähnliche Bearbeitungsvorgänge geplant, so kann eine gemeinsame Abschätzung erstellt werden. ...
 - Art. 24 Meldung von Verletzungen der Datensicherheit

1. Der Verantwortliche meldet dem EDÖB so rasch als möglich eine Verletzung der Datensicherheit, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt. ...

Besonders Schutzenswert Daten

- Art. 5 Begriffe

- a-b. ...

- c. besonders schutzenswerte Personendaten:

1. Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten,
 2. Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie,
 3. genetische Daten,
 4. biometrische Daten, die eine natürliche Person eindeutig identifizieren,
 5. Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen,
 6. Daten über Massnahmen der sozialen Hilfe;
-

EU DSGVO

ⓘ NOTE

Welche Gesetze gibt es in der EU zum Thema Datenschutz und was bedeuten diese für uns als Informatiker.

▼ 🎉 Celebration Criteria

Kategorisiert Daten aufgrund ihres Schutzbedarfs.

Kennt verschiedene Rechtsräume (Schweiz, EU).

Kennt für den jeweiligen Rechtsraum die juristischen Werke (z. B. DSG, DSGVO).

Überprüft eingesetzte Anwendungen auf Einhaltung der Datenschutzgesetze.

Kennt wesentliche Unterschiede in den Datenschutzgesetzen der verschiedenen Rechtsräume.

Zeigt Konsequenzen von Fehlern im Datenschutz und bei der Datensicherheit auf.

Kennt die Problematik von Datenlöschungen über alle Archive und Backups.

▼ 😊 Quellen für die Uninspirierten

- **CH Admin EDÖB: DSGVO**
- **EU: DSGVO**

- [**PWC: EU-DatenschutzGrundverordnung \(GDPR\)**](#)
- [**BARC GmbH: Vergleich Schweiz vs. EU**](#)

Information

Gesetz der EU

Datenschutz Grundverordnung

Rechte von Betroffenen

Art. 15 Auskunftsrecht

Verarbeitungszweck; Kategorien der verarbeiteten Daten; (beabsichtigte) Empfänger der Daten; geplante Speicherdauer oder die Kriterien, wie diese festgelegt wird; Bestehen eines Rechts auf Berichtigung/Lösung der Daten sowie auf Einschränkung/Widerspruch der Verarbeitung; Herkunft der Daten, wenn sie nicht bei dem Betroffenen erhoben wurden; Bestehen eines automatisierten Entscheidungsverfahrens (inkl. Profiling) sowie dessen Logik und Zweck. Geeignete Garantien (z. B. Zertifizierungen), wenn Daten an Drittland oder internationale Organisation übermittelt werden.

- Art. 16 Recht auf Berichtigung
- Art. 17 Recht auf Lösung
- Art. 18 Recht auf Einschränkung der Verarbeitung
- Art. 20 Recht auf Datenübertragbarkeit
- Art. 21 Widerspruchsrecht
- Art. 22 Automatisierte Entscheidungen im Einzelfall einschließlich Profiling
- Art. 23 Beschränkungen

Pflicht von Unternehmen

- Art. 5 Grundsätze für die Verarbeitung personenbezogener Daten
- Art. 6 Rechtmäßigkeit der Verarbeitung

- Art. 7 Bedingungen für die Einwilligung
- Art. 8 Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft
- Art. 9 Verarbeitung besonderer Kategorien personenbezogener Daten
- Art. 10 Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten
- Art. 11 Verarbeitung, für die eine Identifizierung der betroffenen Person nicht erforderlich ist

Vergleich CH vs. EU

	rDSG	DSGVO
 Ernennung Datenschutzbeauftragte(r)	Freiwillig aber empfohlen	Pflicht
 Meldepflicht bei Datenschutzverletzungen	Umgehend	Innerhalb 72h
 Sanktionen	Bis CHF 250'000.- gegen natürliche Personen oder Unternehmen	Bis EUR 20 Mio oder 4% des globalen Umsatzes gegen Unternehmen
 Grenzüberschreitende Datenbearbeitung	Standardvertragsklauseln und interne Richtlinien	Standardvertragsklauseln und interne Richtlinien
 Datenschutzfolgenabschätzung	Verpflichtend bei bestimmter, risikoreicher Datenbearbeitung	Verpflichtend bei risikoreicher Datenbearbeitung mit detaillierten Anforderungen (Art. 35 DSGVO)
 Verzeichnis der Verarbeitungstätigkeiten	Verpflichtend (mit einzelnen Ausnahmen)	Verpflichtend mit Formvorschriften (Art. 30 DSGVO)

 [Bildquelle](#)

Copyright CH und EU

ⓘ NOTE

Was ist ein Urheberrecht?

▼ 🎉 Celebration Criteria

Wählt Software für die Einhaltung von Datenschutz und Datensicherheit aufgrund der Lizenzmodelle aus.

Kennt verschiedene Lizenzmodelle (z.B. für Software, Texte, Bilder).

▼ 😊 Quellen für die Uninspierierten

- **IGE:** Urheberrecht – was ist das?
- **IGE:** Wie darf ich eine Fotografie nutzen?
- **Creative Commons:** Was ist Creative Commons?

Information

Urheberrecht

Was ist Urheberrecht?

- Schützt den Ersteller eines Werkes und gibt ihm Rechte darüber

- In der Schweiz ist es zeitlich begrenzt auf 70 respektive bei Computersoftware 50 Jahre
- Es entsteht automatisch nach erstellen eines Werks
- Es gibt in der Schweiz kein Register

Was gilt als Werk?

- literarische Werke jeglicher Art (Texte) von Roman bis wissenschaftliche Werke, Zeitungsartikel, Inhalt von Webseiten
- visuelle oder audiovisuelle Werke wie Fotografien und Filme
- Werke der Musik und andere akustische Werke
- Werke der bildenden Kunst (Malerei, Bildhauerei, Grafik)
- Werke der angewandten Kunst (Gegenstände mit Gebrauchswert)
- Werke mit wissenschaftlichem oder technischem Inhalt wie Zeichnungen, Pläne, Karten oder plastische Darstellungen
- Werke der Baukunst (Architektur)

Quelle: <https://www.ige.ch/de/etwas-schuetzen/urheberrecht/grundlegendes>

bei Software

Urheberrechtlich geschützt ist insbesondere der Quelltext von Computerprogrammen. Davon ausgeschlossen sind beispielsweise Algorithmen, die einer Software zugrunde liegen.

Quelle: <https://www.ige.ch/de/etwas-schuetzen/urheberrecht/grundlegendes>

Was ist Public Domain ?

Public Domain (eigentlich «öffentlicher Grund», «Allmend») steht für diejenigen Inhalte, die nicht oder nicht mehr urheberrechtlich geschützt und damit frei verfügbar sind. Diese Inhalte sind gemeinfrei. Der Zugang zu ihnen kann nicht durch das Urheberrecht begrenzt oder kostenpflichtig ausgestaltet werden.

Quelle:

https://www.ige.ch/fileadmin/user_upload/schuetzen/urheberrecht/d/Public_Domain_Fact_Sheet_DE_04.2020.pdf

Lizenzen

NOTE

Was ist eine Lizenz?

▼ Celebration Criteria

Wählt Software für die Einhaltung von Datenschutz und Datensicherheit aufgrund der Lizenzmodelle aus.

Kennt verschiedene Lizenzmodelle (z.B. für Software, Texte, Bilder).

▼ Quellen für die Uninspierierten

Allgemein

- **Business Systemhaus AG:** Was ist eine Lizenz?

Bilder

- **Schweizerische Kriminalprävention:** Das eigene Bild
- **ifolor:** Bildrechte in der Schweiz
- **VERTRAGSHILFE:** Das Recht am eigenen Bild in der Schweiz
- **beobachter:** Jedes Foto ist geschützt
- **IGE:** Wie darf ich eine Fotografie nutzen?
- **Creative Commons:** Was ist Creative Commons?

Software

- **Thales:** Software-Lizenzmodelle

- **Institut für Rechtsfragen der Freien und Open Source Software:**
Welches sind die wichtigsten Open Source Lizenzen und welchem Lizenztyp gehören sie an?
- **BREKOM:** Softwarelizenz
- **Rentsch Partner AG:** Schutz Software

Information

Bilder

Sind Bilder Urheberrechtlich geschützt?

Das Urheberrecht schützt sämtliche Fotografien und ähnlich wie Fotografien hergestellte Abbildungen, die physisch vorhandene dreidimensionale Objekte abbilden und von Menschen gemacht wurden.

Der Schutz besteht unabhängig davon, ob die Fotografien individuellen Charakter aufweisen oder nicht. Geschützt sind sowohl Fotografien von professionellen Fotografen als auch die Fotografien von Laien, also beispielsweise Presse- und Produktbilder ebenso wie alltägliche Familien- und Urlaubsfotos.

Quelle: <https://www.ige.ch/de/etwas-schuetzen/urheberrecht/ein-werk-nutzen/fotografienschutz>

Welche Kommerziellen Lizenzen gibt es?

- Klassische Lizenzverträge (Rights-Managed Lizenz) Der Nutzen des Bilds wird definiert und einen entsprechenden Preis für diese Nutzung Abgemacht.
- “lizenzfreie Bilder” (Royalty-Free Lizenz) Üblicherweise bei Online Agenturen, das Bild darf dann auch nur für einen bestimmten Zweck und Auflage verwendet werden. Oft auf ein Projekt beschränkt. Die Bilder sind auch nicht exklusiv und durch die höhere Auflage dann auch günstiger.

Welche freien Lizenzen gibt es?

CREATIVE COMMONS LICENSES		COPY & PUBLISH	ATTRIBUTION REQUIRED	COMMERCIAL USE	MODIFY & ADAPT	CHANGE LICENSE
	PUBLIC DOMAIN	✓	✗	✓	✓	✓
	CC BY	✓	✓	✓	✓	✗
	CC BY-SA	✓	✓	✓	✓	✗
	CC BY-ND	✓	✓	✓	✗	✓
	CC BY-NC	✓	✓	✗	✓	✓
	CC BY-NC-SA	✓	✓	✗	✓	✗
	CC BY-NC-ND	✓	✓	✗	✗	✓

You can redistribute (copy, publish, display, communicate, etc.)

You have to attribute the original work

You can use the work commercially

You can modify and adapt the original work

You can choose license type for your adaptations of the work.

Recht am eigenen Bild

Ein Bild mit einer klar erkennbaren Person, welche im Fokus steht, darf nicht ohne Einwilligung veröffentlicht werden. Wen das Öffentliche Interesse überwiegt, gibt es Ausnahmen.

Quelle: <https://www.skppsc.ch/de/wp-content/uploads/sites/2/2016/12/rechteigenesbild.pdf>

Software

Open Source

	 Free software	 Open-source software	 FREE Freeware	 Public-domain software
Definition	"FREE" is a matter of liberty, not price	"OPEN" doesn't just mean access to the source code	"FREE" refers to price, while freedom of the use is restricted by creator	"PUBLIC DOMAIN" belongs to the public as a whole
Ground philosophy	Social movement	Development methodology	Marketing goals	Copyright disclaimation
Ground rules	Four Freedoms https://www.gnu.org/philosophy/free-sw.html	Open Software initiative https://opensource.org/osd		Creative Common Organization https://creativecommons.org
Free of charge	Not necessary	Not necessary	✓ YES	✓ YES
Covered by copyright law	✓ YES	✓ YES	✓ YES	✗ NO
Examples	   	 		

	 C Copyright	 Copyleft	 Permissive	 Creative Commons
What is a user allowed to do with the code?	What creator dictates	What user wants under certain rules	What user wants with a few restrictions	What user wants without restrictions
Clause of the use	As creator dictates	Derivative work must be attributed to creator, open-source and copyleft	Derivative work must be attributed to a creator	Derivative work must be attributed to a creator
Source code	As creator dictates	Must be open	Don't have to be open	No specific terms about the distribution of source code
Is creator liable for bugs?	✓ YES	✓ YES	✗ NO	✗ NO
Re-licensing	As creator dictates	Derivative work cannot be released as proprietary software	Derivative work can be released under another license or as proprietary software	Derivative work can be released under another license or as proprietary software
Commercial restrictions	As creator dictates	Permitted	Permitted	Permitted

							
Type	Permissive	Permissive	Permissive	Copyleft	Copyleft	Copyleft	
Provides copyright protection	✓ TRUE	✓ TRUE					
Can be used in commercial applications	✓ TRUE	✓ TRUE					
Provides an explicit patent license	✓ TRUE	✗ FALSE	✗ FALSE	✗ FALSE	✗ FALSE	✗ FALSE	
Can be used in proprietary (closed source) projects	✓ TRUE	✓ TRUE	✓ TRUE	✗ FALSE	✗ FALSE partially	✗ FALSE for web	
Popular open-source and free projects	Kubernetes Swift Firebase	Django React Flutter	Angular.js JQuery, .NET Core Laravel	Joomla Notepad++ MySQL	Qt SharpDevelop	SugarCRM Launchpad	

Quelle: <https://moqod-software.medium.com/understanding-open-source-and-free-software-licensing-c0fa600106c9>

Kommerzielle Lizenzen

- Unbefristete Lizenzierung -> Kunde die Software einmalig
- Concurrent-User-Lizenzen -> mehrere Benutzer einen Lizenzcode
- Abonnement-basierte Lizenzierung
- Proprietäre Lizenzierungsmodelle -> z.B. Microsoft Windows oder Office
- Floating-Feature-Lizenzmodell -> gleichzeitige Nutzung bestimmter Features durch Benutzer einschränken
- Feature-basiertes Lizenzierungsmodell
- Netzwerk Lizenzierung -> Lizenz wird an einem Lizenz Server im Netzwerk geprüft
- Cloud-basierte Lizenzierung -> Paas Dienste z.B. Salesforce Quelle:
<https://cpl.thalesgroup.com/de/software-monetization/software-license-models>

Impressum, Disclaimer, AGBs

NOTE

Was braucht eine Webseite?

▼ Celebration Criteria

Zeigt Konsequenzen von Fehlern im Datenschutz und bei der Datensicherheit auf. Kennt wesentliche juristische Voraussetzungen und Eigenheiten von Websites (z.B. Impressum, Disclaimer, AGBs).

▼ Quellen für die Uninspierierten

- [**Hostpoint:** Impressumspflicht ab Frühling in der Schweiz](#)
- [**cyon:** Websites: Wer benötigt ein Impressum und was muss darin stehen?](#)
- [**beobachter.ch:** EIGENE WEBSITE ERSTELLEN: Das müssen Sie rechtlich beachten](#)
- [**weka:** Impressumspflicht Schweiz: So erstellen Sie rechtssichere Websites](#)
- [**020webdesign.ch:** Checkliste zur rechtlich sicheren Website in der Schweiz](#)

Information

Vermerk über Verlag, Druckerei, Redaktion u. a. in Büchern, Zeitungen und Zeitschriften

Quelle: <https://www.duden.de/rechtschreibung/Impressum>

Impressum

Privatpersonen

- Vorname und Name
- Postadresse
- E-Mail-Adresse

Juristische Personen

- Firmenname
- Postadresse
- E-Mail-Adresse
- Unternehmens-Identifikationsnummer (UID)

Disclaimer

Erklärung, in der sich jemand (besonders der Inhaber einer Website) von bestimmten Inhalten (besonders den Inhalten fremder, aber mit der eigenen verlinkter Websites) distanziert

Quelle: <https://www.duden.de/rechtschreibung/Disclaimer>

Bsp:

- <https://www.basel.ch/politik-und-behorden/besondere-behorden/landeskanzlei/disclaimer>
- <https://www.blkb.ch/rechtliches/rechtliche-hinweise.html>

- https://www.roche.ch/legal_statement.html
-

AGBs

- **Gewährleistung** Garantiebestimmungen für die bei der Transaktion verkauften Waren oder Dienstleistungen.
- **Datenschutz** Verwendung der gesammelten Daten, Verschlüsselungstechnik usw.
- **Bestellungen** Rechnungs- und Zahlungsbedingungen, Mehrwertsteuer usw.
- **Lieferung** Versandgebiete, Lieferfristen usw.
- **Haftung** Beispielsweise im Falle einer Beschädigung der Ware während des Versands.
- **Retouren** Umtausch- und Rücknahmeregelungen.
- **Anwendbares Recht und Gerichtsstand** Im Streitfall zuständiges Gericht und anwendbares Recht (Verweis auf schweizerisches Recht).

Quelle: [KMU Admin](#)

Sprint - Konzeptionelles

Epics

Sicherheit und Risiko

Was ist Sicherheit und Risiko?

Informationssicherheit

Was ist Informationssicherheit ?

Datensicherheit

Was ist Datensicherheit?

Identity und Access Management

Wer darf was machen?

Sicherheit und Risiko

ⓘ NOTE

Was ist Sicherheit und Risiko?

▼ 🎉 Celebration Criteria

Sie kennen die Unterschiede zwischen Security und Safety.

Sie kennen die Grundlagen vom Risikomanagement.

▼ 😊 Quellen für die Uninspierierten

- [**Sichere Industrie:** Safety vs. Security...](#)
- [**CH Admin:** Risikomanagement](#)
- [**CH Admin:** Risikoidentifikation und Risikobewertung](#)

Sicherheit

Was ist Sicherheit?

«Sicherheit bezeichnet einen Zustand, der frei von unvertretbaren Risiken der Beeinträchtigung ist oder als gefahrenfrei angesehen wird.»

(DIN EN 61508)

Was ist der Unterschied zwischen Security und Safety?

Safety

Primäres Schutzziel = Lebewesen

Security

Primäres Schutzziel = Objekte

Risiko

Das Risiko ist ein Mass für die Grösse einer Gefährdung und beinhaltet die Häufigkeit bzw. Wahrscheinlichkeit und das Schadensausmass eines unerwünschten Ereignisses.

- Eintrittswahrscheinlichkeit (auch Schadenswahrscheinlichkeit, Schadenshäufigkeit)
- Schadenspotenzial, Schadensausmass

Eintrittswahrscheinlichkeit * Schadensausmass = Risiko

Eintrittswahrscheinlichkeit	Schadensausmaß			
	ohne Arbeitsunfall (keine Rechtsfolgen)	leicht, Erste Hilfe (Rechtsfolgen möglich)	schwer, reversibel (Rechtsfolgen wahrscheinlich)	sehr schwer, Tod (dramatische Rechtsfolgen)
sehr wahrscheinlich, oft				
sehr wahrscheinlich, gelegentlich				
möglich, selten				
praktisch, unmöglich				

Quelle: https://www.dominabau.de/blog/risikomanagement/risikomatrix.html
Illustrationen: adobeStock.com/ylestekir



Eintrittshäufigkeit

Eintrittshäufigkeit	Beschreibung
selten	Ereignis könnte nach heutigem Kenntnisstand höchstens alle 5 Jahre eintreten.
mittel	Ereignis tritt einmal alle fünf Jahre bis einmal im Jahr ein.
häufig	Ereignis tritt einmal im Jahr bis einmal pro Monat ein.
sehr häufig	Ereignis tritt mehrmals im Monat ein.

Schadenshöhe

Schadenshöhe	Schadensauswirkungen
vernachlässigbar	Die Schadensauswirkungen sind gering und können vernachlässigt werden.
begrenzt	Die Schadensauswirkungen sind begrenzt und überschaubar
beträchtlich	Die Schadensauswirkungen können beträchtlich sein.
existenzbedrohend	Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmass erreichen.

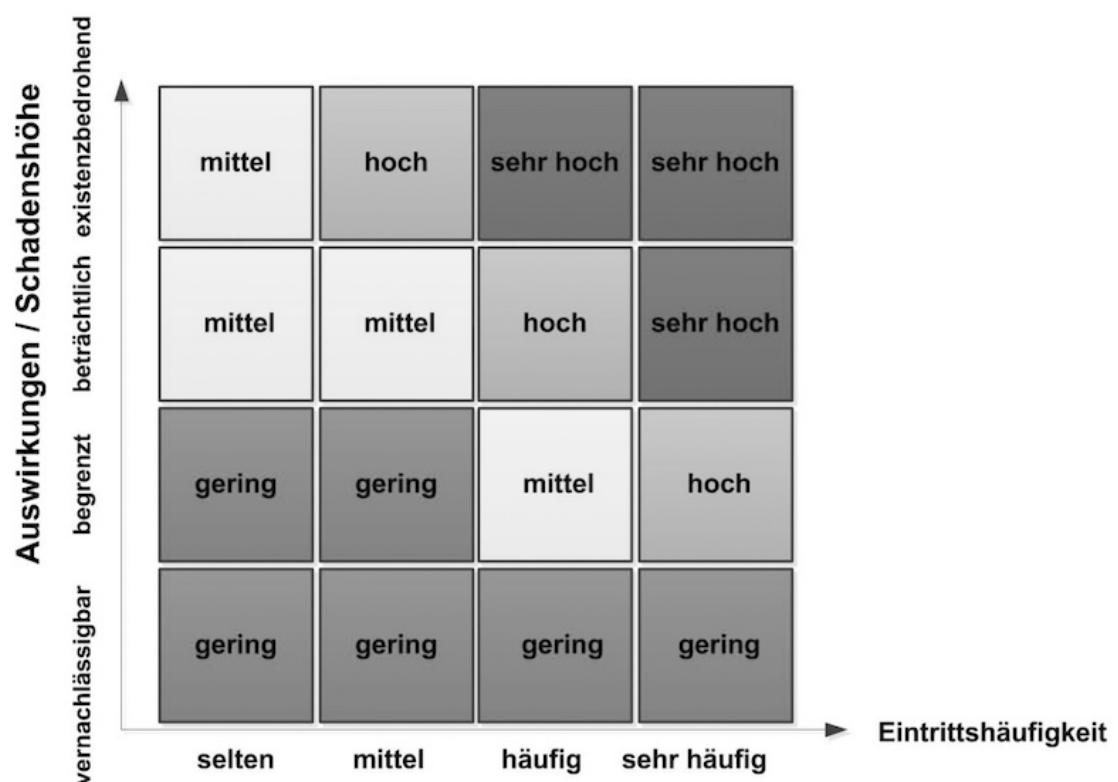


Abbildung 3: Matrix zur Einstufung von Risiken

Risikokategorien

Risikokategorien	Beschreibung
gering	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten einen ausreichenden Schutz. In der Praxis ist es üblich, geringe Risiken zu akzeptieren und die Gefährdung dennoch zu beobachten.
mittel	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen reichen möglicherweise nicht aus.
hoch	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz vor der jeweiligen Gefährdung.
sehr hoch	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz vor der jeweiligen Gefährdung. In der Praxis werden sehr hohe Risiken selten akzeptiert.

Informationssicherheit

ⓘ NOTE

Was ist Informationssicherheit ?

▼ 🎉 Celebration Criteria

Sie kennen die unterschiedlichen Arten von Informationen.

Sie kennen die Grundlage vom Informationssicherheit.

▼ 😊 Quellen für die Uninspierierten

- [**Security Insider:** Was ist Informationssicherheit?](#)
- [**BREKOM:** Informationssicherheit](#)
- [**NCSC:** Bundesinterne Kampagne](#)
- [**MATRIX IT development GmbH:** Begriffe und Definitionen](#)

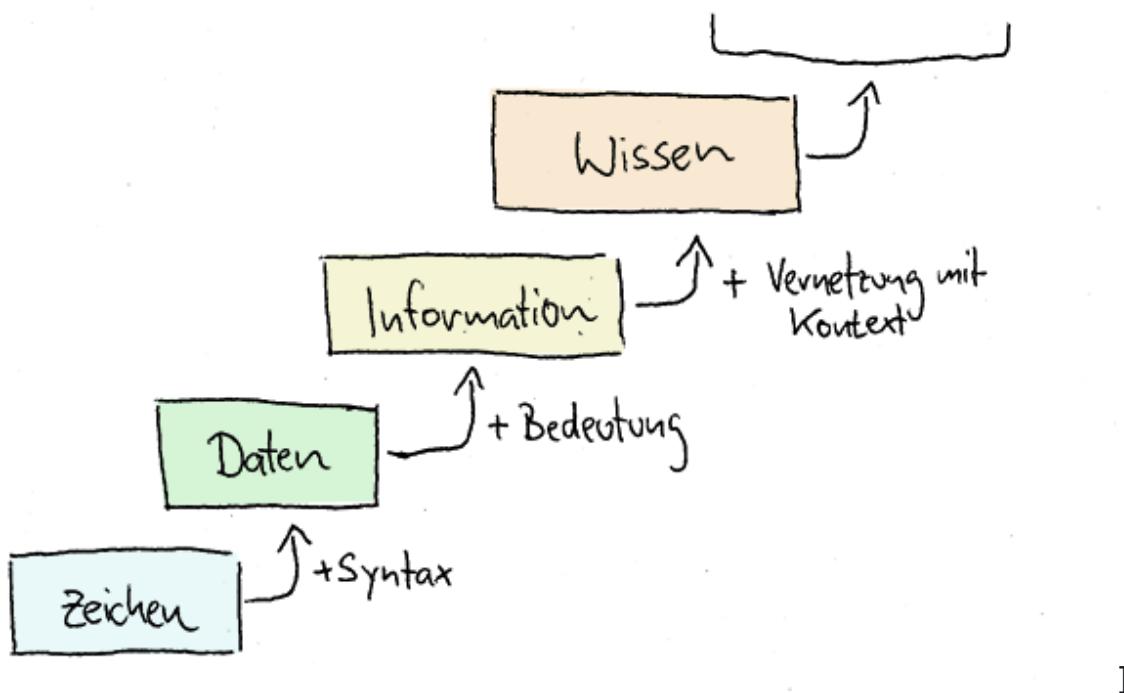
Einstieg in Informationssicherheit

Was sind Informationen?

„Informationen stellen Kenntnisse über Sachverhalte oder Personen dar.“

artegic AG: Wo liegt der Unterschied zwischen Daten, Informationen und Wissen?

Daten und Informationen im Kontext



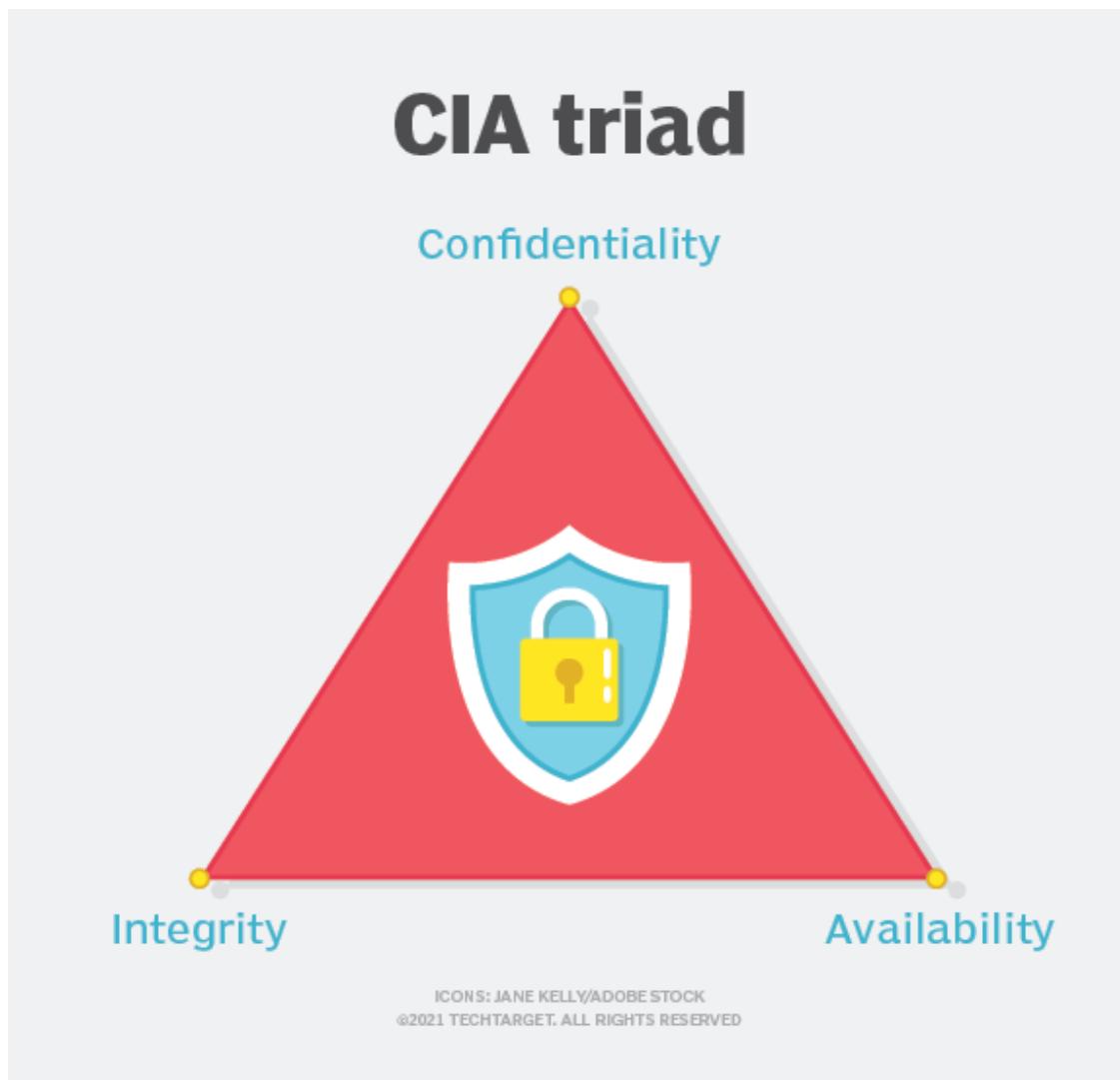
vis4.net: Datavis vs. Infovis - Zwischen Kunst und Journalismus

Was ist Informationssicherheit?

Schutz von Informationen in jeder Form, egal ob auf Papier oder digital.

CIA

- Confidentiality (Vertraulichkeit)
- Integrity (Integrität)
- Availability (Verfügbarkeit)



Vertraulichkeit

- Daten sind vertraulich zu behandeln
- Nur autorisierte Personen haben Zugriff
- Das ist bei Daten im Zugriff, im Transfair und im Ruhezustand zu gewährleisten

Integrität

- Datenintegrität: Daten sind korrekt, vollständig und konsistent
- Systemintegrität: System funktioniert zu jedem Zeitpunkt wie vorgesehen

Verfügbarkeit

- Daten sind verfügbar

- Üblicherweise in Service-Level-Agreements geregelt

Datensicherheit

ⓘ NOTE

Was ist Datensicherheit?

▼ 🎉 Celebration Criteria

Kategorisiert Daten aufgrund ihres Schutzbedarfs.

Kennt verschiedene Kategorien der Schutzwürdigkeit von Daten und deren Kriterien.

- Sie können die Daten Anhand ihres Schutzbedarf klassifizieren.

Kennt den Unterschied von Datenschutz und Datensicherheit.

Setzt verschiedene Möglichkeiten der Datenspeicherung ein.

Kennt Verfahren zur Speicherung von Daten und bewusst redundanter Datenhaltung (z.B. lokal, Server, Cloud).

Kennt verschiedene Gefahren, denen Daten ausgesetzt sind (z.B. Diebstahl, Ransomware, Integritätsverletzung).

- Sie kennen verschiedene Gefahren für Datensicherheit.
- Sie kennen können den Begriff Bedrohung, Schwachstelle, Risiko und Asset einordnen.
- Sie wissen die Wahl des korrekt Speicher Medium zum Schutzziel beitragen kann.

▼ 😊 Quellen für die Uninspierierten

- [**Profi AG** Datensicherheit](#)
- [**datenschutz.org:** Datenschutz: Maßnahmen für den Schutz von Daten](#)
- [**Oracle** Was ist Datensicherheit?](#)
- [**ISARI CONSULT Stefanie Schmidt:** Risiken im Risikomanagement bewerten und beurteilen](#)
- [**NCSC:** Schwachstelle](#)
- [**NCSC** Cyberbedrohungen](#)
- [**BSI-Standard:** 200.2 - Kapitel 8.2 Schutzbedarf feststellung](#)

Einstieg in Datensicherheit

Was ist Datensicherheit?

- Schutz der Daten egal ob Personenbezogen oder nicht
- Fokus auf Technischen und Organisatorischen Massnahmen

Was ist das Ziel des Datensicherheit?

Jegliche Daten gegen mögliche Bedrohungen zu Schützen und so die 3 Schutzziele (CIA) umzusetzten.

Datenschutz vs. Datensicherheit

Datenschutz

- Gesetzte zum Schutz von personenbezogen Daten

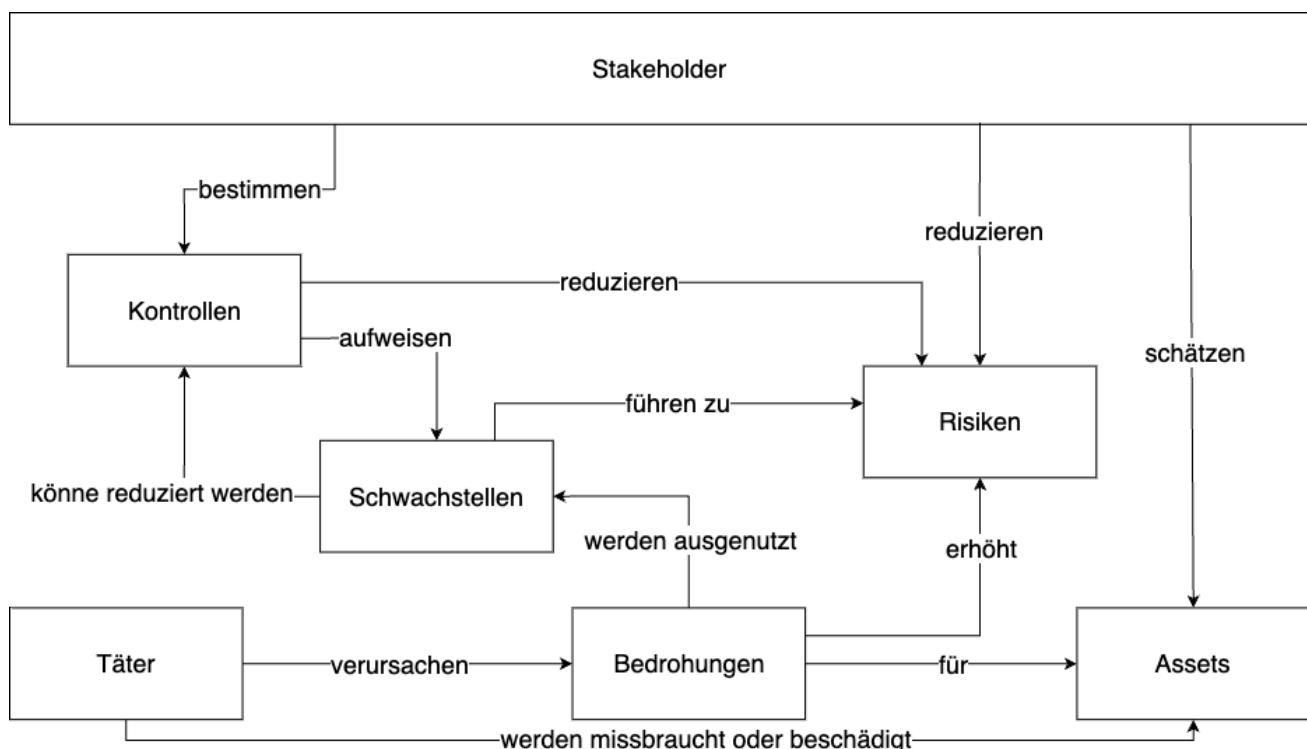
- Vorschriften zum Schutz von personenbezogenen Daten
- "Legislative" (gesetzgebende Gewalt, Gesetzgebung)

Datensicherheit

- Massnahmen zum Schutz von Daten (nicht nur personenbezogenen Daten)
- "Exekutive" (vollziehende Gewalt)

Begriffe

Übersicht der Begriffe



Begriff	Beschreibung
Asset	Vermögenswert eines Unternehmens
Schwachstelle	Schwachstellen (vulnerability, bug)
Bedrohung	Ereignis das die Verfügbarkeit, Integrität oder Vertraulichkeit

Begriff	Beschreibung
	von Informationen beeinträchtigen
Exploit	Ein Exploit ist das ausnutzen einer Schwachstelle.
Täter	Person welche Schwachstelle ausnutzt und so eine Bedrohung für die Assets darstellt.

Klassifizierung nach CIA

- Confidentiality (Vertraulichkeit)
- Integrity (Integrität)
- Availability (Verfügbarkeit)



Übersicht der Kategorien

Schutzziel				
Vertraulichkeit	Öffentlich	Intern	Vertraulich	Streng Vertraulich
Integrität		normal	hoch	sehr hoch
Verfügbarkeit		normal	hoch	sehr hoch

Vertraulichkeit

Klassifizierung	Beschreibung
Öffentlich	Daten sind für jedermann, auch außerhalb der Firma, zugänglich.
Intern	Interne Daten werden lediglich den eigenen Mitarbeitern zugänglich gemacht.
Vertraulich	Vertraulich definierte Daten sind lediglich einer begrenzten Anzahl an Mitarbeitern zugänglich, z.B Personaldaten, Kundenliste
Streng Vertraulich	Streng vertrauliche Daten sind punktuell und ausschließlich bestimmten definierten Personen zugänglich.

www.sec4you.com: Klassifizierung ISO 27001

Integrität, Verfügbarkeit

Klassifizierung	Beschreibung
normal	Die Schadensauswirkungen sind begrenzt und überschaubar.
hoch	Die Schadensauswirkungen können beträchtlich sein.
sehr hoch	Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmass erreichen.

[Klassifizierung nach BSI](#) ab Seite 104

Identity und Access Management

ⓘ NOTE

Wer darf was machen?

▼ 🎉 Celebration Criteria

Überprüft und verbessert gegebenenfalls die Datensicherheit der eigenen Infrastruktur.

Kennt Techniken des Zugriffsschutzes, Passwordmanager und Prinzipien der Passwortverwaltung.

- Sie wissen was ein "sicheres Passwort" ausmacht.
- Sie kennen alternativen und ergänzungen zu Passwörter.
- Sie kennen die Limitationen von Passwörter und MFA.
- Sie kennen die Grundlagen von RBAC.
- Sie wissen wo RBAC in IAM Einzuordnen ist.
- Sie wissen was Least Privileged Access (LPA) ist.

Kennt den Unterschied von Authentifizierung und Autorisierung.

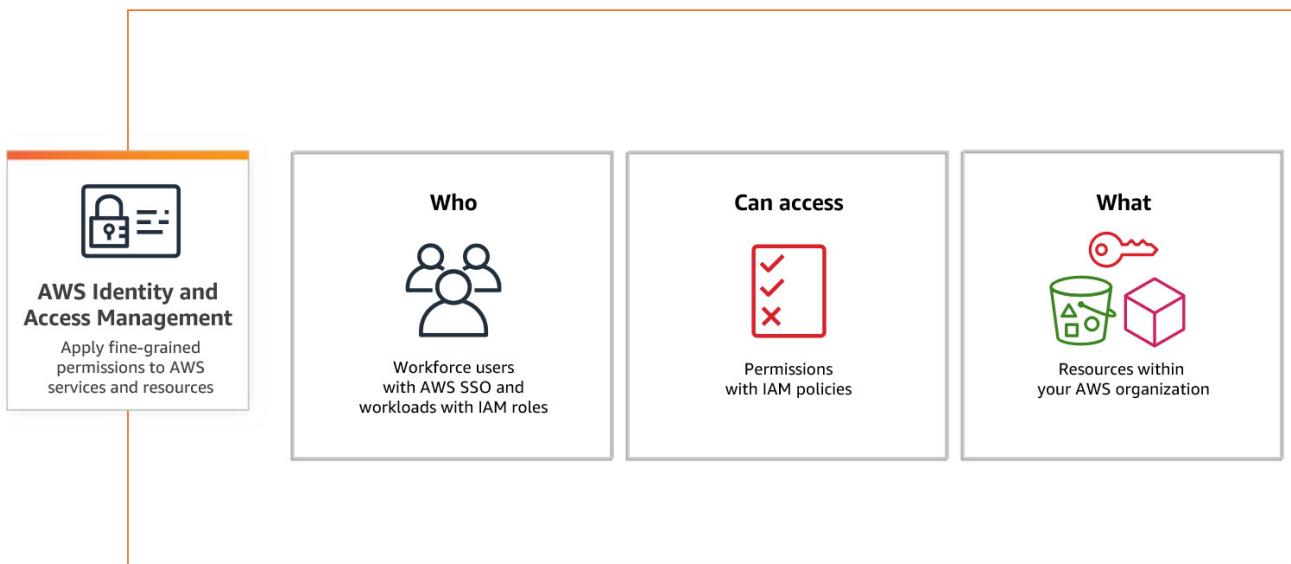
▼ 🧐 Quellen für die Uninspierierten

- [**ComputerWeekly.de:** Identity Access Management \(IAM\) -Systeme](#)
- [**Microsoft** Was ist Identity & Access Management \(IAM\)?](#)
- [**Okta:** Vergleich von Authentifizierung und Autorisierung](#)

- [**auth0:** Authentication vs. Authorization](#)
- [**CH Admin bit:** How To Choose a Strong Password](#)
- [**TechTarget:** strong password](#)
- [**Boston University:** How To Choose a Strong Password](#)
- [**tools4ever** Was ist Multi-Faktor-Authentifizierung?](#)
- [**securityinsider** Was ist Multi-Faktor-Authentifizierung \(MFA\)?](#)
- [**ionos:** Role Based Access Control \(RBAC\): Wie funktioniert die rollenbasierte Zugriffskontrolle?](#)
- [**youtube.com:** Role-Based Access Control \(RBAC\) Explained: How it works and when to use it](#)
- [**microsoft:** Azure Role-Based Access Control, Azure RBAC\)?](#)

Einstieg in Identity und Access Management

Was ist IAM?



Identity

- Identität
- Wer?
 - ein Person welches sich via User, Password und MFA Authentifiziert
 - ein System das sich via Zertifikat oder Key Authentifiziert

Access

- Zugriff
- Was?
 - legt fest auf was, wie zugegriffen werden darf oder eben nicht

Berechtigungen

Identity	Resource	Access
Hans Müller	Internet	allowed to google.ch
FC_read	\FileServer001\Finanzen\$	read
FC_write	\FileServer001\Finanzen\$	write
HR_read	\FileServer001\HR\$	read

Identity	Resource	Access
HR_write	\FileServer001\HR\$	read

Least Privileged Access

User und System haben nur Zugriff auf das was Notwendig ist um ihren Job zuerledigen. z.B. Der/ Die Service Desk Mitarbeiter:in hat keinen Domain Admin, sondern nur Password Reset Rechte.

ohne

Identity	Resource	Access
FC	\FileServer001\Finanzen\$	full
HR	\FileServer001\HR\$	full

mit

Identity	Resource	Access
FC_Debitoren_read	\FileServer001\Finanzen\$\Debitoren	read
FC_Debitoren_write	\FileServer001\Finanzen\$\Debitoren	write
FC_Kreditoren_read	\FileServer001\Finanzen\$\Kreditoren	read
FC_Kreditoren_write	\FileServer001\Finanzen\$\Kreditoren	write
HR_Loehne_read	\FileServer001\HR\$\Löhne	read
HR_Loehne_write	\FileServer001\HR\$\Löhne	write
HR_Bewerbungen_read	\FileServer001\HR\$\Bewerbungen	read

Identity	Resource	Access
HR_Bewerbungen_HR_write	\FileServer001\HR\$\Bewerbungen	write

Verzeichnis Dienst

The screenshot shows the Windows Active Directory Users and Computers (ADUC) management console. The left pane features a navigation tree with nodes like 'Active Directory Users and Computers', 'Saved Queries', and 'com' (which is expanded to show 'Builtin', 'Computers', 'Domain Controllers', 'ForeignSecurityPrincipal', 'Managed Service Account', and 'Users'). The right pane contains a table with two columns: 'Name' and 'Description'. A message at the top of the table area says 'There are no items to display'.

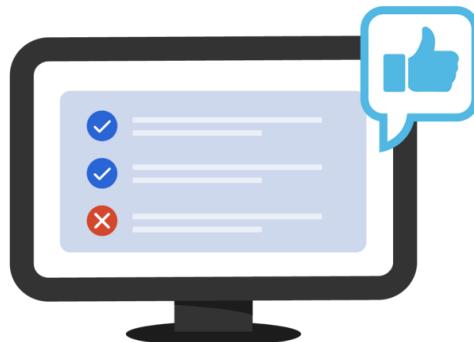
Authentifizierung und Autorisierung

Authentication



Confirms users are who they say they are.

Authorization



Gives users permission to access a resource.

okta

Authentifizierung: Identität nachweisen

- Prüft Anmeldeinformation
- Passwörter
- Biometrische Daten
- Pin
- MFA APP
- Hardware Token

Autorisierung: Rechte Vergabe

- Ordnet bestimmte Rechte einer Identität zu
 - Server
 - Admin Rechte
 - FileShare
 - Zugriff auf bestimmtes APP

Passwörter und MFA

Was ist eine sicheres Passwort?



Was ist MFA?



Kuze Zusammenfassung



Sprint - Technische und Organisatorische Massnahmen

Epics



Technische Massnahmen

Who the F* is TOM? 😬



Organisatorische Massnahmen

OMMMMM.... 🧘



Physische Sicherheit

Keep your hands out of the cookie jar!!

Technische Massnahmen

ⓘ NOTE

Who the F*** is TOM? 😱

▼ 🎉 Celebration Criteria

Sie kennen Technische Massnahmen zum Schutz der Daten.

▼ 😊 Quellen für die Uninspierierten

- [**Swiss Infosec:** Technische und organisatorische Massnahmen \(TOM\)](#)
- [**Toshiba Tec Switzerland AG** Allgemeine Beschreibung der technischen und organisatorischen Massnahmen](#)
- [**Swisscom:** 10 Tipps, wie sich KMU vor Cyberattacken schützen](#)
- [**ComputerWeekly:** Physische Sicherheit \(Objektschutz\)](#)
- [**security insider:** Was ist physische IT-Sicherheit?](#)
- [**green** Schutz im Datacenter](#)

Einstieg in Technische Massnahmen

Was sind Technische Massnahmen?

Spezialisten setzen diese Massnahmen üblicherweise um.

- Hardware (Netzsicherheit) z.B. Firewall
- Sicherheit des Arbeitsplatzes (Sperrbildschirm, Antiviren-Programme)
- Zugriffssicherheit (Access Management, Rollenmodell)

Welche Technische Massnahmen gibt es ?

- Hardware (Virtuelle Appliances)
 - Firewall
 - Loadbalancer
 - Verschlüsselung
- Sicherheit des Arbeitsplatzes
 - Sperrbildschirm
 - Antivierus Software
 - VPN
 - Bitlocker
 - MFA
- Zugriffssicherheit
 - RBAC
 - Netztwerk Segmentierung (VLANs)
 - MAC Filter
 - ACLs

Wie verbessern Technische Massnahmen die IT Sicherheit?

- Eine Firewall begrenzt den Zugriff auf Netzwerk Ressourcen von Unbefugten.
- Ein Loadbalancer kann die Last auf mehrere Server verteilen um die Performance zu verbessern und bei einem Ausfall Server ausschliessen um die Verfügbarkeit gewährleisten zu können.

- Das Sperren von Bildschirm sorgt dafür das Niemand auf Resourcen Zugriffen kann die er nicht sollte.
- Ein VPN sorgt dafür das im Homeoffice einen sicher Zugriff auf Resourcen im Geschäft gewährleistet werden kann.
- Mac Filtering auf den Switches sorg dafür das nur Authorisierte Geräte Zugriff ins Netzwerk erhalten.

Organisatorische Massnahmen

ⓘ NOTE

OMMMMM.... 

▼ 🎉 Celebration Criteria

Sie kennen Organisatorische Massnahmen zur Umsetzung der Informationssicherheit.

▼ 😊 Quellen für die Uninspierierten

- [**Swiss Infosec:** Technische und organisatorische Massnahmen \(TOM\)](#)
- [**Toshiba Tec Switzerland AG** Allgemeine Beschreibung der technischen und organisatorischen Massnahmen](#)
- [**Swisscom:** 10 Tipps, wie sich KMU vor Cyberattacken schützen](#)

Einstieg in Organisatorische Massnahmen

Was sind Organisatorische Massnahmen?

Organisatorische Massnahmen richten sich an die Personen

- Mitarbeiterersensibilisierung (Awareness)
- interne Guidelines
- ...

Welche Organisatorische Massnahmen gibt es?

- Nutzungsrichtlinien für IT
- Schulungen der Mitarbeiter
- 4 Augen Prinzip
- NDA
- Firmen Kultur
- Organisationsstruktur der Firma
- Prozessdokumentation
- ...

Wie tragen Organisatorische Massnahmen zur Umsetzung der Informationssicherheit bei?

- Die Schulung der MA z.b. führ zu Korekten Umgang z.B. bei Spam oder sonstigen Gefahren.
- Das 4 Augen Prinzip reduziert das Fehler Risiko bei Kritischen Task.
- NDA helfen bei der Einhaltung der Geheimhaltung bei der Zusammenarbeit mit externen.
- Eine Firmen Kultur welche Fehler zulässt, Motiviert Mitarbeiter zum Melden von zwischen Fällen.
- ...

Wo sind die Organisatorische Massnahmen in CIA einzuordnen? (erstellen Sie eine Tabelle)

Massnahme	Zuordnung
Nutzungsrichtlinien für IT	Vertraulichkeit

Massnahme	Zuordnung
Schulungen der Mitarbeiter	Vertraulichkeit
4 Augen Prinzip	Verfügbarkeit
NDA	Vertraulichkeit

Physische Sicherheit

ⓘ NOTE

Keep your hands out of the cookie jar!!

▼ 🎉 Celebration Criteria

Sie kennen Physische Massnahmen zum Schutz von Daten und IT Systemen.

▼ 💬 Quellen für die Uninspierierten

- [**ComputerWeekly:** Physische Sicherheit \(Objektschutz\)](#)
- [**security insider:** Was ist physische IT-Sicherheit?](#)
- [**green** Schutz im Datacenter](#)

Einstieg in Physische Sicherheit / Objekt Schutz im IT Kontext

Was sind Physische Massnahmen?

Schutz der Assets auch Personen von äussern Gefahren und Ereignissen.
Mann redet auch von Objektschutz.

Gefahren:

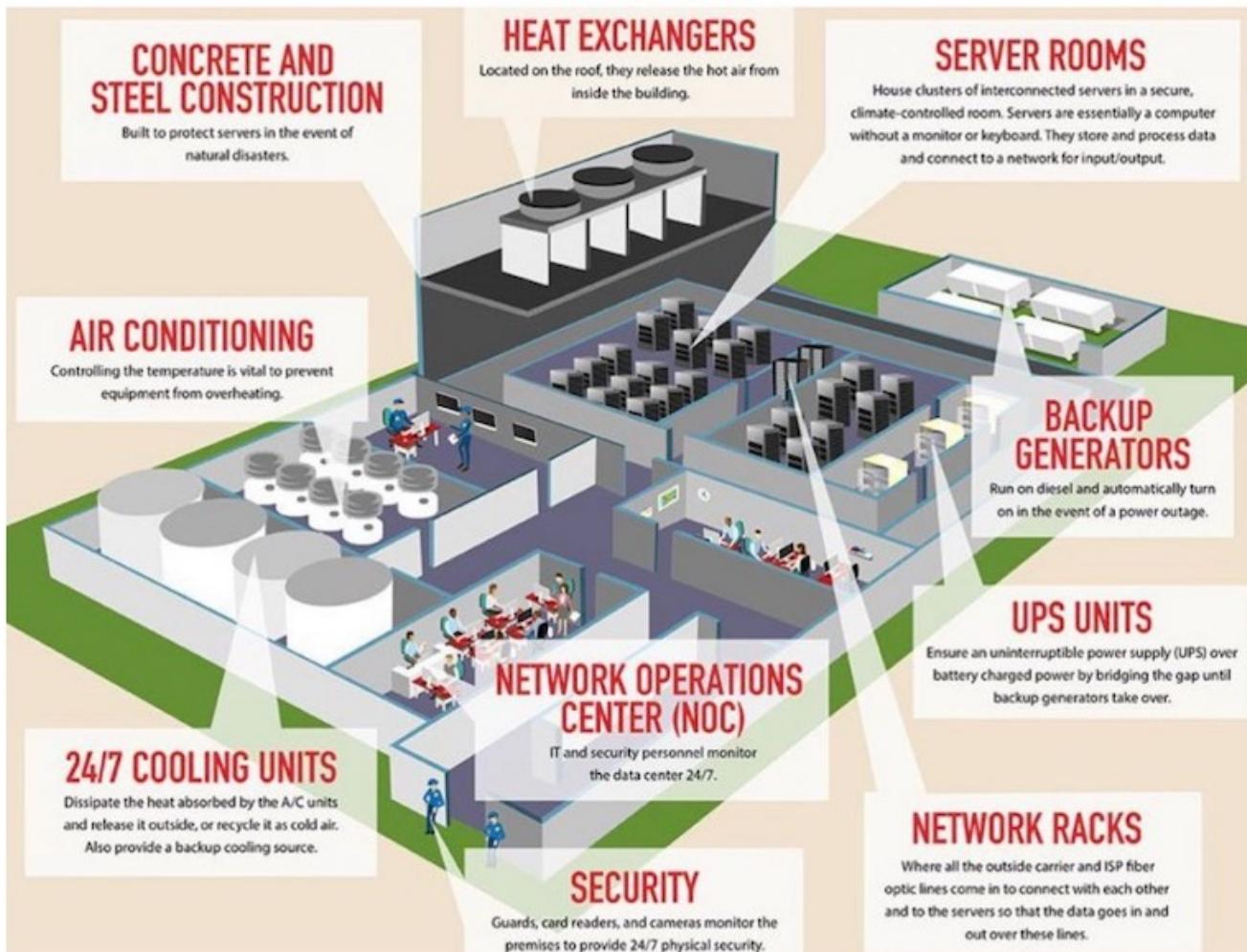
- Schutz vor Feuer

- Naturkatastrophen (Blitzschlag, Wasser, Erdbeben)
- Einbrüchen, Diebstahl
- Sabotage, Vandalismus und Terrorismus

Massnahmen

- Löschanlage mit Wasser oder GAS
- USV Batterie oder Generator
- Kühlung
- Zutrittskontrolle mit Bag, Iris, Fingerprint, Schlüssel
 - Vereinzelungsschleuse
 - Protokollierung
- Überwachungskameras
- Alarmanlage
- Abschliessbar Racks
- Geo Redundanz

Bsp. Daten Center



Sprint - SicherheitsFrameworks

Epics

NIST

Was ist NIST?

BSI

Was ist BSI?

COBIT

Was ist COBIT?

ITIL

Was ist ITIL?

NIST

NOTE

Was ist NIST?

▼ Celebration Criteria

Sie kennen die Grundbausteine von NIST.

Sie können das Framework in seinen Grundzügen jemanden erklären.

Sie kennen Stärken und Schwächen des Frameworks.

▼ Quellen für die Uninspierierten

- [NIST](#)

BSI

NOTE

Was ist BSI?

▼ Celebration Criteria

Sie kennen die Grundbausteine von BSI.

Sie können das Framework in seinen Grundzügen jemanden erklären.

Sie kennen Stärken und Schwächen des Frameworks.

▼ Quellen für die Uninspierierten

- [BSI](#)

COBIT

NOTE

Was ist COBIT?

▼ Celebration Criteria

Sie kennen die Grundbausteine von COBIT.

Sie können das Framework in seinen Grundzügen jemanden erklären.

Sie kennen Stärken und Schwächen des Frameworks.

▼ Quellen für die Uninspierierten

- **COBIT**

ITIL

NOTE

Was ist ITIL?

▼ Celebration Criteria

Sie kennen die Grundbausteine von ITIL.

Sie können das Framework in seinen Grundzügen jemanden erklären.

Sie kennen Stärken und Schwächen des Frameworks.

▼ Quellen für die Uninspierierten

- [ITIL Video](#)