

2. ZW Modul 231 Lernziele

Inhalt

1. AGB kommt vor, was gehört dazu und was gehört nicht dazu	1
2. Was versteht man unter der Option Opt-In. Was bedeutet die Option: Opt-in?	1
3. Löschpflicht, was droht Firmen, wenn sie ihre Daten nicht löschen	2
(Vertraulichkeit, Integrität, Verfügbarkeit definieren und wissen).....	2
(Risikoanalyse wissen, erstellen und bewerten).....	4
Eckdaten	4

1. AGB kommt vor, was gehört dazu und was gehört nicht dazu

Beim Verfassen der AGB sollten alle Schritte des Verkaufsprozesses bedacht werden. Hier einige Punkte, die es zu berücksichtigen gilt:

- 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).¹

2. Was versteht man unter der Option Opt-In. Was bedeutet die Option: Opt-in?

Die Option "Opt-in" bezieht sich auf die Zustimmung oder Einwilligung einer Person oder eines Benutzers zu einer bestimmten Handlung oder einer bestimmten Verwendung ihrer Daten. Es wird häufig in den Bereichen Datenschutz, Marketing und Kommunikation verwendet. Hier sind einige wichtige Aspekte des Opt-in:

1. **Zustimmung:** Opt-in bedeutet, dass eine Person aktiv zustimmt oder ihre Einwilligung gibt, bevor bestimmte Aktionen durchgeführt werden. Dies kann beispielsweise bedeuten, dass jemand seine E-Mail-Adresse für den Erhalt von Werbe-E-Mails zur Verfügung stellt, indem er ein Anmeldeformular ausfüllt und auf einen "Abonnieren" oder "Zustimmen" Button klickt.
2. **Datenschutz:** Im Kontext des Datenschutzes ist Opt-in eine wichtige Voraussetzung, um sicherzustellen, dass personenbezogene Daten nur verwendet werden, wenn der Benutzer ausdrücklich zugestimmt hat. Dies ist insbesondere in Regionen mit strengen

¹ (ChatGPT, kein Datum)

Datenschutzgesetzen wie der Europäischen Union (EU) im Rahmen der Datenschutz-Grundverordnung (DSGVO) von Bedeutung.

3. **Anti-Spam-Gesetze:** Opt-in-Verfahren sind oft erforderlich, um die Einhaltung von Anti-Spam-Gesetzen sicherzustellen. Beispielsweise erfordern Gesetze wie der CAN-SPAM Act in den USA, dass E-Mail-Marketing-Empfänger die Möglichkeit haben, sich für den Erhalt von E-Mails anzumelden (Opt-in), und dass sie sich leicht abmelden können (Opt-out).
4. **Marketing:** Im Marketing bezieht sich Opt-in auf die Zustimmung von Verbrauchern oder Interessenten, Marketingmaterialien wie E-Mails, SMS-Nachrichten oder Telefonanrufe zu erhalten. Unternehmen müssen sicherstellen, dass sie die Zustimmung ihrer Zielgruppe einholen, anstatt unaufgefordert Nachrichten zu senden, um den Datenschutz und die Kundenbeziehung zu respektieren.
5. **Double Opt-in:** In einigen Fällen wird ein "Double Opt-in" verwendet, um sicherzustellen, dass die Zustimmung gültig ist. Nachdem jemand sich für etwas angemeldet hat (z. B. einen Newsletter), erhält er eine Bestätigungs-E-Mail und muss auf einen Link klicken, um die Anmeldung zu bestätigen. Dies bietet eine zusätzliche Schutzschicht gegen unberechtigte Anmeldungen.

Zusammengefasst bedeutet Opt-in, dass Personen aktiv zustimmen müssen, bevor bestimmte Aktionen durchgeführt werden können, sei es im Bereich Datenschutz, Marketing oder anderen Kontexten. Dies fördert den Schutz der Privatsphäre und das Einhalten von gesetzlichen Vorschriften.²

3. Löschpflicht, was droht Firmen, wenn sie ihre Daten nicht löschen

Unternehmen müssen personenbezogene Daten löschen, wenn der Zweck ihrer Verarbeitung nicht mehr besteht, auf Anfrage einer betroffenen Person oder wenn gesetzliche Löschpflichten bestehen.³ Es gibt Daten, die nach dem Gesetz Aufbewahrungsfristen haben wie z.B. Steuerdaten und Kontodaten. Die Fristen können je nach Land, Branche und Art der Daten variieren.⁴

Bei Nichterfüllung der Datenschutzanforderungen und der Datenlöschpflichten können rechtliche und finanzielle Konsequenzen drohen, darunter Geldstrafen und Bussgelder gemäss dem geltenden Datenschutzgesetz.⁵

Die genauen Konsequenzen können je nach Land und Gesetzgebung variieren. Doch grundsätzlich sieht hier die Datenschutz-Grundverordnung bei einem Verstoß gegen den Datenschutz Bussgelder bis zu 20 Millionen Euro oder aber bis 4% Prozent des weltweiten Jahresumsatzes eines Unternehmens vor.⁶

(Vertraulichkeit, Integrität, Verfügbarkeit definieren und wissen)

1. Vertraulichkeit

Unter Vertraulichkeit versteht man, dass Daten nur von den Personen eingesehen oder offengelegt werden dürfen, die dazu auch berechtigt sind. Will man Daten vertraulich behandeln, muss klar festgelegt werden, wer in welcher Art und Weise Zugriff auf diese Daten hat. Doch man muss noch einen weiteren Aspekt beachten, den viele gerne vergessen: Zur Vertraulichkeit von Daten gehört

² (ChatGPT, kein Datum)

³ (231_SPICK)

⁴ (Spick_MainQuest_2_231)

⁵ (MainQuest Spicker_KD 28.09.2023)

⁶ (OneNote Modul 231, kein Datum)

auch, dass diese bei der Übertragung nicht von unautorisierten Personen gelesen werden! Das heisst, es muss dafür gesorgt sein, dass die Daten bei einer Übertragung in geeigneter Weise verschlüsselt werden. Zu den verschiedenen Verschlüsselungsverfahren erfahren Sie hier mehr.

Ein gutes Beispiel aus der Praxis stellt hier vor allem Ihr E-Mail-Verkehr dar. Vermutlich umfasst dieser wöchentlich mehrere tausend E-Mails. Darunter befinden sich mit Sicherheit Informationen, die vertraulich zu behandeln sind. Aber können Sie auch garantieren, dass diese Informationen nur die Augen erreichen, für die sie bestimmt sind? Ihr E-Mail-Verkehr muss verschlüsselt sein! Andernfalls können Sie die Vertraulichkeit Ihrer Daten, die per E-Mail versendet wurden, nicht mehr garantieren!

Und hier noch ein weniger technisches Beispiel: Auch Räumlichkeiten, in denen vertrauliche Datenbestände wie. z.B. die Lohnbuchhaltung verarbeitet oder gelagert werden, müssen entsprechend gesichert sein. Wenn solche Räume frei zugänglich sind, kann man die Vertraulichkeit der dort befindlichen Daten vergessen!

2. Integrität

Viele verwechseln Integrität mit Vertraulichkeit. Integrität bedeutet allerdings, dass es nicht möglich sein darf, Daten unerkant bzw. unbemerkt zu ändern. Es geht hierbei also um das Erkennen von Datenänderungen, wohingegen bei Vertraulichkeit der Fokus auf der Berechtigung liegt. Oft wird mit Integrität (man spricht dann von starker Integrität) sogar gefordert, dass Daten überhaupt nicht unberechtigt verändert werden können. Da sich dies aber selten sinnvoll umsetzen lässt, empfehle ich die erste Definition. Nehmen wir einmal Forschungs- und Entwicklungsdaten. Wenn die Integrität solcher Daten zerstört ist, weil eine winzige Änderung unerkant vorgenommen wurde, können Sie sämtlichen Daten nicht mehr trauen! Man muss niemandem erklären, dass dies eine Katastrophe wäre.

3. Verfügbarkeit

Die Verfügbarkeit eines Systems beschreibt ganz einfach die Zeit, in der das System funktioniert. Im Sinne der Schutzziele geht es hier selbstverständlich darum, die Verfügbarkeit möglichst hoch zu halten. Anders gesagt: Es gilt, das Risiko Systemausfälle zu minimieren!

Sie sollten sich also einen Überblick über die im Unternehmen vorhandenen Systeme und damit auch Datenbestände verschaffen. Anschliessend müssen Sie analysieren, welche Systeme und Datenbestände unbedingt notwendig sind, damit die Arbeitsabläufe im Unternehmen funktionieren können. Diese sollten Sie entsprechend gegen Ausfälle schützen! Eine Art Risikoanalyse, in der man Ausfallwahrscheinlichkeit, Ausfallzeit und Schadenspotenzial auflistet, ist hierbei zu empfehlen. Zudem sollte die Geschäftsleitung bzw. eine Fachabteilung festlegen, welche Ausfallzeiten jeweils tolerierbar sind. Diese können nämlich von Unternehmen zu Unternehmen variieren. Beispielsweise kann es durchaus sein, dass der Ausfall des Mailservers für einen Tag verkraftbar ist; in anderen Unternehmen ist das der Super-GAU.⁷

⁷ (OneNote Modul 231, kein Datum)

(Risikoanalyse wissen, erstellen und bewerten)

— Risikoanalyse Bsp.

Besitzer	Szenario	Beschreibung	Ursache	Schadensklasse	Eintrittswahrscheinlichkeit
IT	Stromausfall	Serverfarmen können nicht mehr betrieben werden. Dienste stehen nicht mehr zur Verfügung.	kein Redundanz	hoch	mittel

Eckdaten

8 Antworten zu je einer Frage, insgesamt 24 Punkte

Aufgabe 231-3A bis Aufgabe 231-4B