

Schulungskonzept zum Datenschutz

Firma

Datum

Inhalt

1. Anforderungen aus der DSGVO
2. Räume
3. Ziel des Schulungskonzeptes
4. Ziele der Datenschutz-Schulung
5. Zielgruppe / Geltungsbereich
6. Inhalte der Schulung
7. Besonderer Schulungsinhalt
8. Methodik
9. Dauer & Ort
10. Evaluierung
11. Wiederholungen
12. Anforderungen aus der DSGVO

Gewährleistung der Grundsätze für die Verarbeitung personenbezogener Daten gem. Art.5 Abs. (1) DSGVO

Gewährleistung einer angemessenen Sicherheit der personenbezogenen Daten gem. Art. 5 Abs. (1) f DSGVO

Nachkommen von Rechenschaftspflichten gem. Art. 5 Abs. (2) DSGVO

Ergreifen von Maßnahmen zur Sicherstellung, dass die Verarbeitung von personenbezogenen Daten gemäß der DSGVO erfolgt. Art.24 Abs. (1) DSGVO

1. Ziel unseres Schulungskonzeptes

Aufklärung unserer Beschäftigten über die DSGVO und deren Begriffe

Sensibilisierung unserer Beschäftigten

Gewährleistung von rechtlichen oder/und vertraglichen Pflichten zum Datenschutz

Minimierung von Risiken für Betroffenen aufgrund datenschutzrechtlicher Verstöße

Minimierung von Risiken für die Organisation aufgrund Sanktionen oder Rufschädigungen

1. Ziele der Datenschutz-Schulungen

Sensibilisierung für Datenschutz: Die Schulungen sollen das Bewusstsein unserer Beschäftigten für den Datenschutz stärken und ihnen helfen, die Bedeutung des Datenschutzes für das Unternehmen und die betroffenen Personen zu verstehen.

Kenntnisse über die DSGVO vermitteln: Die Schulungen sollen die grundlegenden Anforderungen und Bestimmungen der DSGVO vermitteln, damit unsere Beschäftigten verstehen, wie personenbezogene Daten geschützt werden müssen.

Verständnis für Datenschutzrisiken entwickeln: Die Schulungen sollen den Beschäftigten helfen, Datenschutzrisiken zu identifizieren und angemessene Maßnahmen zum Schutz personenbezogener Daten zu ergreifen.

Befähigung zur Umsetzung von Datenschutzmaßnahmen: Die Schulungen sollen den Beschäftigten helfen, angemessene Datenschutzmaßnahmen umzusetzen und damit Datenschutzverletzungen zu vermeiden.

Schulung der IT-Sicherheit: Die Schulungen sollen die Beschäftigten auch in Bezug auf IT-Sicherheit schulen, damit sie in der Lage sind, IT-sicherheitsrelevante Entscheidungen zu treffen und Bedrohungen zu erkennen.

1. Zielgruppe und Geltungsbereich

Die Schulung richtet sich an alle Beschäftigten, die personenbezogene Daten verarbeiten oder mit solchen Daten in Berührung kommen. Abteilungen im Unternehmen, die mit personenbezogenen Daten arbeiten:

Mitgliederverwaltung,

Personalwesen,

das Marketing,

der Kundenservice ,

die Buchhaltung

Qualitätsmanagement

Bitte zählen Sie hier oder in einer Anlage Ihre Abteilungen/Einheiten auf

Bitte führen Sie hier oder in einer Anlage die verschiedenen Lokalitäten auf

Bitte definieren Sie den Begriff „Beschäftigte“ für Ihre Organisation

(Tipp: Sie können hier auf Ihr Organigramm verweisen)

1. Inhalte der Schulung

Eine Datenschutzschulung sollte folgende Inhalte beinhalten:

1. Einführung in die DSGVO: Die Teilnehmerinnen und Teilnehmer sollten grundlegende Informationen zur DSGVO erhalten, wie zum Beispiel die Ziele und Grundsätze der Verordnung.

2. Rechtsgrundlagen für die Verarbeitung personenbezogener Daten: Die Teilnehmerinnen und Teilnehmer sollten lernen, welche Rechtsgrundlagen für die Verarbeitung personenbezogener Daten nach der DSGVO existieren und wie diese angewendet werden.

3. Begriffsdefinitionen: Die Schulung sollte die wichtigsten Begriffe der DSGVO erklären, wie z.B. personenbezogene Daten, Verarbeitung, Auftragsverarbeitung, Datenschutzbeauftragter.

4. Datenschutzorganisation im Unternehmen: Die Teilnehmerinnen und Teilnehmer sollten lernen, wie das Unternehmen sicherstellt, dass Datenschutzbestimmungen eingehalten werden, z.B. welche Prozesse und Verfahren im Unternehmen existieren, um personenbezogene Daten zu schützen.

5. Technischer Datenschutz: Hier geht es darum, technische Maßnahmen zu erläutern, die zum Schutz personenbezogener Daten eingesetzt werden können, wie z.B. Verschlüsselung, Passwortregelungen und Netzwerksicherheit.

6. Umgang mit personenbezogenen Daten: Die Schulung sollte vermitteln, wie die Teilnehmerinnen und Teilnehmer verantwortungsvoll mit personenbezogenen Daten umgehen können, wie z.B. die Vermeidung von Datenpannen und die ordnungsgemäße Löschung von personenbezogenen Daten.

7. Rechte der betroffenen Personen: Die Teilnehmerinnen und Teilnehmer sollten lernen, welche Rechte betroffenen Personen zustehen und wie diese wahrgenommen werden können, wie z.B. Auskunftsrecht, Recht auf Löschung, Recht auf Widerspruch.

8. Sanktionen und Bußgelder: Die Schulung sollte auch die möglichen Konsequenzen von Verstößen gegen die DSGVO erläutern, wie z.B. Sanktionen und Bußgelder.

1. Besonderer Schulungsinhalt   
   Sensibilisierung für Social Media Angriffe

Social Engineering bezeichnet eine Methode, bei der Angreifer gezielt menschliche Schwächen ausnutzen, um Zugang zu vertraulichen Informationen zu erhalten. Hierbei können beispielsweise Phishing-E-Mails, gefälschte Websites oder manipulierte Telefonate eingesetzt werden.

In der Datenschutzschulung sollten die Teilnehmerinnen und Teilnehmer daher darauf geschult werden, wie sie solche Angriffe erkennen und sich davor schützen können. Hierzu gehört beispielsweise die Überprüfung der Echtheit von E-Mails oder Websites, das Vermeiden von unbekannten Links und das Verwenden von sicheren Passwörtern.

Durch die Sensibilisierung für Social Engineering Angriffe können Unternehmen das Risiko von Datenpannen und Cyberangriffen reduzieren und einen wichtigen Beitrag zur Sicherheit personenbezogener Daten leisten.

Die Sensibilisierung für Social Engineering Angriffe kann in einer Datenschutzschulung auf verschiedene Weise geschult werden.

1. **Theoretische Schulung:** In einem Vortrag oder Seminar sollen die Grundlagen von Social Engineering erklärt werden, wie beispielsweise die verschiedenen Arten von Angriffen, die Techniken, die von Angreifern eingesetzt werden, um Vertrauen zu gewinnen, sowie die möglichen Folgen eines erfolgreichen Angriffs.
2. **Praktische Schulung:** Durch die Durchführung von Übungen und Simulationen sollen die Beschäftigten lernen, wie sie auf Social Engineering Angriffe reagieren und sich davor schützen können. Beispielsweise kann ein Phishing-Test durchgeführt werden, bei dem den Beschäftigten eine gefälschte E-Mail geschickt wird, um zu testen, ob sie den Betrug erkennen und richtig reagieren.
3. **Schulung durch interne Richtlinien:** Die Sensibilisierung für Social Engineering Angriffe soll auch durch interne Richtlinien und Verfahrensweisen erreicht werden, die den Beschäftigten helfen, solche Angriffe zu erkennen und darauf zu reagieren. Beispielsweise können Richtlinien für das Öffnen von E-Mails oder das Herunterladen von Dateien aus dem Internet erstellt werden, um das Risiko von Angriffen zu minimieren.

Diese Schulungsmaßnahme und Sensibilisierung sollen in unserer Organisation dazu beitragen, dass unsere Beschäftigten besser in der Lage sind, auf Social Engineering Angriffe zu reagieren und personenbezogene Daten zu schützen.

1. Methodik

Die Schulung wird interaktiv und praxisorientiert durchgeführt. Es werden Fallbeispiele aus dem Unternehmenskontext verwendet, um die Anforderungen der DSGVO konkret zu vermitteln. Die Teilnehmerinnen und Teilnehmer werden aktiv in die Schulung eingebunden und haben die Möglichkeit, Fragen zu stellen und ihre Erfahrungen zu teilen.

Ob eine E-Learning-Schulung oder eine Präsenz-Schulung geeigneter ist, hängt von verschiedenen Faktoren ab. Beide Schulungsarten haben Vor- und Nachteile.

Die [Firma] wird ihre Beschäftigten sowohl in Präsenz-Schulungen als auch über E-Learning Angebote und Richtlinien zum Datenschutz sensibilisieren und aufklären.

Nähere Details finden Sie in der Anlage Schulungsplanung.

1. Präsenz-Schulung

Eine Präsenz-Schulung bietet den Vorteil, dass die Teilnehmerinnen und Teilnehmer die Möglichkeit haben, Fragen zu stellen und sich aktiv mit anderen Teilnehmern auszutauschen. Insbesondere bei komplexen Themen wie Datenschutz kann dies von Vorteil sein.

Auch können praxisnahe Beispiele besser vermittelt werden, wenn sie direkt vor Ort

gezeigt werden können. Zudem kann eine Präsenz-Schulung auch dazu beitragen, das Gemeinschaftsgefühl im Unternehmen zu stärken.

Nähere Details finden Sie in der Anlage Schulungsplanung.

1. E-Learning

Eine E-Learning-Schulung bietet den Vorteil, dass die Beschäftigten die Schulung zeit- und ortsunabhängig durchführen können.

Nähere Details finden Sie in der Anlage Schulungsplanung.

1. Dauer & Ort

Für die Schulungen stellen wir folgende Räumlichkeiten bereit…/ Die Schulungen können in folgenden Räumlichkeiten stattfinden:…

Nähere Details finden Sie in der Anlage Schulungsplanung.

1. Evaluierung

Im Anschluss an die Schulung wird eine Evaluierung durchgeführt, um die Effektivität der Schulung zu überprüfen. Dabei werden die Teilnehmerinnen und Teilnehmer gebeten, einen Fragebogen auszufüllen, um ihre Zufriedenheit mit der Schulung zu bewerten und ihr erworbenes Wissen zu testen. Die Ergebnisse der Evaluierung werden anonym ausgewertet und dienen als Grundlage für die Weiterentwicklung des Schulungskonzepts.

1. Wiederholungen

Regelmäßig Schulungen sollen sicherstellen, dass die Beschäftigen stets auf dem aktuellen Stand sind und das Bewusstsein für Datenschutz im Unternehmen aufrechterhalten wird.

Nähere Details finden Sie in der Anlage Schulungsplanung.

Wenn es größere Veränderungen im Datenschutzrecht gibt, wie zum Beispiel eine Änderung der DSGVO oder eine wichtige Gerichtsentscheidung, kann es notwendig sein, zusätzliche Schulungen durchzuführen. Auch bei der Einführung neuer Technologien oder Prozesse, die mit der Verarbeitung personenbezogener Daten verbunden sind, sollten die Beschäftigten entsprechend geschult werden.

1. 100% Schutz ist nicht möglich

Es gibt keinen 100%igen Schutz vor Datenschutzverletzungen oder Cyberangriffen. Es ist immer möglich, dass ein Angreifer eine Schwachstelle im System oder menschliche Fehler ausnutzt, um Zugang zu vertraulichen Informationen zu erhalten.

Dennoch wollen wir durch angemessene Sicherheitsmaßnahmen und Schulungen das Risiko von Datenschutzverletzungen und Cyberangriffen minimieren. Dazu gehört beispielsweise die Implementierung von IT-Sicherheitsmaßnahmen wie Firewalls, Antivirensoftware und regelmäßige Sicherheitsupdates sowie die Schulung der Beschäftigten in Bezug auf Datenschutz und Informationssicherheit.

Ein wichtiger Aspekt ist auch das regelmäßige Überprüfen und Verbessern der Sicherheitsmaßnahmen, um Schwachstellen zu identifizieren und zu beheben. In diesem Zusammenhang kann auch ein Notfallplan für den Umgang mit Datenschutzverletzungen und Cyberangriffen erstellt werden, um im Ernstfall schnell und effektiv handeln zu können.

Letztendlich ist es wichtig, ein Bewusstsein bei allen Beschäftigten dafür zu schaffen, dass es keine absolute Sicherheit gibt und dass jeder Einzelne seinen Teil dazu beitragen muss, um Datenschutz und Informationssicherheit zu gewährleisten.