Materialien für den Datenschutz

Perfekte DSGVO-Mitarbeiterschulung für Ihr Unternehmen

Beginnen Sie mit unserem kostenfreien Beispiel. Damit Sie gleich zu Beginn ganz klar wissen, was Sie bekommen. Anhand der Muster-Mitarbeiterschulung erhalten Sie einen ersten Einblick in unser Angebot. Material, dass Sie als Datenschutzbeauftragte oder Verantwortlicher in Ihrem Unternehmen gut gebrauchen können.

Zusätzlich haben Sie die Möglichkeit, 16 weitere und ausführliche Schulungsmaterialien im DIN-A4-Format zu erwerben, die ganz speziell auf die Sensibilisierung für Datenschutz und Datensicherheit zugeschnitten sind. Und gleichzeitig die vorgeschriebene Schulungspflicht in Ihrem Unternehmen abdecken.

Warum Sie „Der DSB“ nutzen sollten

Jeder einzelne Text unseres Materials erstreckt sich auf einer DIN-A4-Seite und ist bewusst so gestaltet, dass er nicht nur informiert, sondern auch sensibilisiert. Das Besondere daran: Die Inhalte beziehen sich auf praktische Beispiele aus dem Privatleben und schlagen so eine Brücke zum Datenschutz im Berufsalltag.

Wie Sie der „Der DSB“ einsetzen können

Wenn Sie unsere Schulungsmaterialien erworben haben, stehen Ihnen durch die spezielle Gestaltung und Form diverse Möglichkeiten zur Verfügung, diese PDF zielgerichtet einzusetzen.
Sie können die PDFs ganz einfach so benutzen:

- Aushang am Schwarzen Brett
- Verteilung per E-Mail
- Beilage zur monatlichen Gehaltsabrechnung
- Veröffentlichung im Intranet
- Schulungsmaterial bei eigenen Veranstaltungen

Ihre Vorteile im Überblick

- Entlastung: Wir haben uns bereits für Sie ausführlich Gedanken gemacht.
- Zeitsparend: Direkt einsatzbereite PDF-Dateien ohne Anpassungsbedarf.
- Erfahrungsbasiert: Die Materialien basieren auf den langjährigen Erfahrungswerten von Lorenz Macke, einem erfahrenen und zertifizierten externen Datenschutzbeauftragten.
- Relevanz: Unsere Themen wie QR-Codes, Urlaubszeit oder Dienstpläne sind praxisnah und für jeden Mitarbeiter verständlich.
- Aktualität: Unsere Texte sind aktuell auf dem Stand von Juli 2023 und werden stets auf dem Laufenden gehalten. Und noch besser: Einige sind sogar zeitlos gültig.

Mehr Bewusstsein für Datenschutz schaffen

Durch den Bezug zu Alltagssituationen wird der Inhalt nicht nur informativ, sondern auch eindrücklich vermittelt. Unsere Erfahrung zeigt, dass eine wohldosierte Sensibilisierung durch alltagsnahe Beispiele mehr bewirkt als reine Faktenvermittlung. Und sollte es zu einem Datenschutzvorfall kommen, ermöglichen unsere Materialien den Nachweis regelmäßiger Schulungen gemäß DSGVO.

Themenübersicht

Einige der behandelten Themen sind beispielsweise „Speicherrichtlinien“, „Fotos im Betrieb“, „Unternehmensdetails erwähnen“ oder in Zeiten der allgegenwärtigen Videokonferenzen der Problempunkt „Bildschirm teilen“.

Einfach per Download!

Holen Sie sich jetzt gleich Ihre Materialien und sorgen Sie für eine effektive und verständliche Sensibilisierung Ihrer Mitarbeiter und Schulung im Bereich Datenschutz und Datensicherheit.

Rechtsgrundlage

Sie haben die Wahl…

… ob Sie Wahlwerbung in Ihren Briefkasten bekommen. Sie wollen keine Wahlwerbung? Dann haben Sie folgende Möglichkeiten.

Hinweis „Keine Werbung“:

Dieser Hinweis bezieht sich auf eine Werbesendung ohne eine Adresse, die konkret Ihrem eigenen Briefkasten zugeordnet werden kann. Eine umstrittene Lücke ist die Adressierung: „An die Bewohner des Hauses Musterstr. 1, 12345 Berlin“.

Parteien:

Die Parteien können Ihre Adresse vom Meldeamt kostenpflichtig anfragen und zum Zwecke der Wahlwerbung vor der Wahl verwenden!

Der Standardwert ist also erstmal; „Ja, die Daten dürfen verwendet werden“. Es sei denn, Sie haben beim Bürgeramt/Ordnungsamt der „Melderegisterauskunft zum Zwecke der Wahlwerbung“ widersprochen.
Dieses Recht können Sie jederzeit kostenfrei für die Zukunft ausüben (danach auch jederzeit wieder ändern). Wahlwerbung per E-Mail ist unzulässig und per Telefon ebenso, es sei denn, Sie haben vorher eingewilligt.

Rechtsgrundlage:

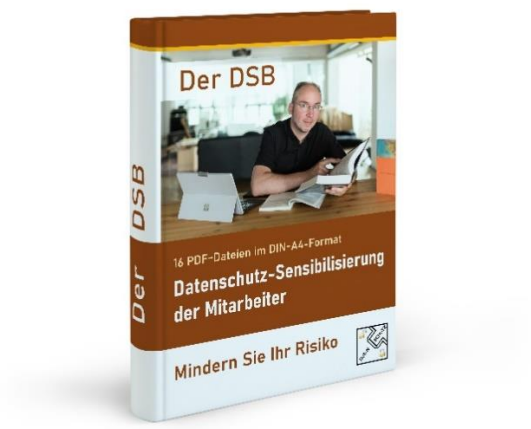
Bevor Sie Personen kontaktieren, brauchen Sie eine Rechtsgrundlage. Diese ergibt sich aus der DSGVO, aber auch aus dem Gesetz gegen den unlauteren Wettbewerb (UWG) und weiteren Spezialgesetzen.

Marketingabteilung & Datenschutz:

Marketing möchte machen -> Datenschutz drosselt
Marketing macht‘s -> Datenschutz drückt die Daumen

Fazit:

Bevor Sie Marketingaktionen starten, muss die Rechtmäßigkeit geprüft und sichergestellt sein.



DerDSB Themenübersicht

Datenschutz mal anders:

Die Verbindung von Privatem und Geschäftlichen.

Mögliche Fehler der Mitarbeitenden am PC

Hinweis:

Bisher wurden alle Texte von Lorenz Macke persönlich erstellt. So soll es auch bleiben. Dieses kostenfreie Muster ist eine Ausnahme.
Da ChatGPT (künstliche Intelligenz) nun mehr und mehr verwendet wird und auch in den Medien diskutiert wird, habe ich ChatGPT gefragt „Was sind die größten Fehler, die Mitarbeitende bei der Arbeit am Computer machen?“ [Kostenfreies Muster als Bonus: KI-Richtlinie auf https://www.dtnschtz.de]

Verwendung schwacher Passwörter:

Schwache Passwörter sind eine große Sicherheitslücke. Mitarbeiter sollten starke Passwörter verwenden, die schwer zu erraten sind, und vermeiden, dasselbe Passwort für mehrere Konten zu verwenden. (Anmerkung: Es muss Richtlinien bzw. Vorgaben seitens der IT geben.)

Keine Sicherung wichtiger Daten:

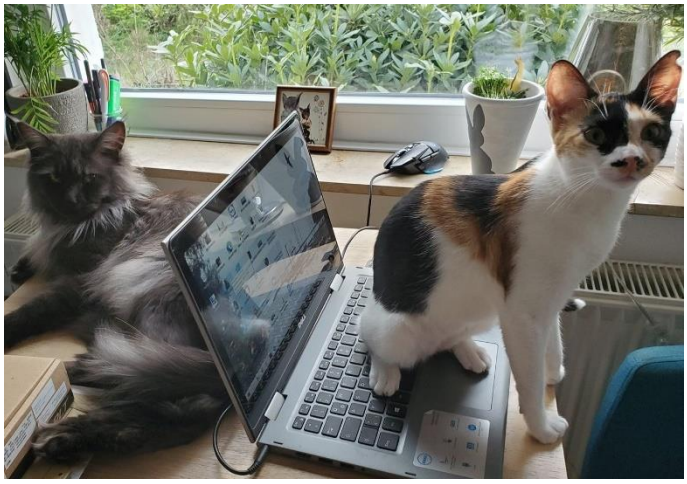
Datenverlust kann aufgrund von Hardwarefehlern, menschlichen Versagens oder Cyberangriffen auftreten. Mitarbeiter sollten wichtige Daten regelmäßig sichern, um dauerhaften Verlust zu vermeiden. *(Anmerkung: Speichern Sie die Daten an festgelegten Speicherorten, damit diese gesichert werden.)*

Vernachlässigung von Software-Updates:

Software-Updates enthalten oft kritische Sicherheitspatches, die vor bekannten Schwachstellen schützen. Die Vernachlässigung der Softwareaktualisierung kann Systeme und Daten anfällig für Cyberangriffe machen. *(Anmerkung: Trifft hoffentlich mehr auf das mobile Arbeiten zu)*

Computer nicht sperren, wenn sie sich nicht am Schreibtisch befinden:

Computer entsperrt und unbeaufsichtigt zu lassen, kann unbefugten Zugriff auf vertrauliche Daten ermöglichen. Mitarbeiter sollten ihre Computer immer sperren, wenn sie ihren Schreibtisch verlassen, auch wenn es nur für kurze Zeit ist.



Herunterladen nicht genehmigter Software:

Das Herunterladen nicht genehmigter Software kann zu Sicherheitslücken führen oder die Netzwerkleistung beeinträchtigen. Mitarbeiter sollten nur Software herunterladen, die von der IT-Abteilung ihrer Organisation genehmigt wurde.

Sicherheitsvorfälle nicht melden:

Sicherheitsvorfälle wie verlorene oder gestohlene Geräte, verdächtige Aktivitäten oder Datenschutzverletzungen sollten unverzüglich dem IT- oder Sicherheitspersonal gemeldet werden. Das Versäumnis, Vorfälle zu melden, kann das Risiko weiterer Schäden erhöhen.

Fazit:

Jetzt sind Sie sich möglicher Auswirkungen bewusst. Achten Sie bitte weiterhin auf die Einhaltung der Vorgaben und denken Sie mit.

Bezugsmöglichkeit:

Weitere 16 Materialien können Sie unter www.derdsb.de kostenpflichtig erwerben.

Bestellen Sie jetzt im Digistore24