



Aktueller Stand: NIS2-Umsetzungsgesetz (NIS2UmsuCG)

Ende Juli 2025 mag für viele bereits viele Monate her sein. Seitdem hat sich jedoch nichts Neues beim Gesetzesentwurf zur Umsetzung der NIS-2-Richtlinie im Bundeskabinett ergeben. Die Sommerpause des Deutschen Bundestags mag dafür ursächlich sein.

Das Bundesamt für Sicherheit in der Informationstechnik blieb in dieser Zeit nicht untätig und veröffentlichte Ende September 2025 eine Hilfestellung für die Schulungspflicht für Geschäftsleitungen für besonders wichtige und wichtige Einrichtungen. Hierbei handelt es sich allerdings nicht um eine rechtliche Vorgabe, sondern es soll Schulungsanbietern als Orientierung dienen, das notwendige Wissen für die Führungsebene aufzubereiten.

Handreichung:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/NIS-2/nis-2-geschaeftsleitungsschulung.pdf?__blob=publicationFile&v=3

Thema 1

**Schon ein
Berechtigungs-
konzept erstellt?**

Seite 1

Thema 2

**Heute schon das
Passwort
vergessen?**

Seite 2

Thema 3

**Das Risiko der
Gestensteuerung**

Seite 3





Mobilität der Zukunft – Herausforderungen smarter Technologien

Die Zukunft der Mobilität ist digital: Autos fahren zunehmend vernetzt, Sprachassistenten helfen bei der Navigation, unsere Smartphones begleiten uns bei jeder Fahrt, und biometrische Systeme wie Gesichtserkennung oder Fingerabdruckscanner machen die Nutzung noch komfortabler. Doch mit all diesen Innovationen entstehen auch neue Herausforderungen – vor allem, wenn es um den Schutz unserer persönlichen Daten geht.

Seit 2018 gilt die **DSGVO**. Sie soll sicherstellen, dass unsere persönlichen Daten nur mit unserer Zustimmung und auf transparente Weise verarbeitet werden. Doch während die Technik sich ständig weiterentwickelt, kommt der Datenschutz oft nicht hinterher. Gerade im Bereich Mobilität zeigt sich, wie schnell Innovationen datenschutzrechtliche Grenzen überschreiten.

Ein besonders wichtiges Beispiel sind **Connected Cars** – also Autos, die mit dem Internet verbunden sind. Sie sammeln unzählige Daten, z. B. zum Standort, zum Fahrverhalten oder zur Anzahl der Insassen. Diese Daten sollen helfen, den Verkehr sicherer zu machen bzw. Staus zu vermeiden. Gleichzeitig stellt sich die Frage: Wer bekommt diese Daten eigentlich? Und wer darf sie verwenden?

Auch **smarte Endgeräte** wie Smartphones oder Bordcomputer liefern viele Informationen – z. B. wohin wir fahren, wie schnell wir uns bewegen oder welche Apps wir nutzen. Diese Informationen können Nutzerprofile erstellen und landen bei Firmen außerhalb der EU – außerhalb des Anwendungsbereichs der DSGVO.

Sprachassistenten wie Siri oder Alexa machen das Autofahren bequemer, weil man, ohne Knöpfe drücken zu müssen, z. B. Musik abspielen oder Nachrichten verschicken kann. Doch sie hören ständig zu – nicht nur dem Fahrer, sondern allen Passagieren oder Telefonpartnern. Das wirft Fragen zur **Rechtmäßigkeit** auf.

Besonders sensibel sind **biometrische Daten** wie Fingerabdrücke oder Gesichtserkennung. Sie gehören laut DSGVO zu den „besonderen Kategorien personenbezogener Daten“ und dürfen nur in Ausnahmefällen verarbeitet werden – etwa aufgrund einer ausdrücklichen Zustimmung. Trotzdem werden sie immer öfter eingesetzt, zum Beispiel beim Öffnen von Autotüren oder in Fahrerüberwachungssystemen (DMS)

Die Mobilität der Zukunft bringt viele Vorteile mit sich – sie wird sicherer, effizienter und komfortabler. Doch all das hat seinen Preis: Unsere persönlichen Daten werden immer mehr zum Rohstoff dieser digitalen Welt. Deshalb ist es wichtig, dass der Datenschutz mit der technischen Entwicklung Schritt hält. Die DSGVO ist ein guter Anfang, aber sie muss konsequent angewendet und weiterentwickelt werden. Nur so kann die Mobilität von morgen nicht nur smart, sondern auch sicher für die Privatsphäre sein.

Das Risiko der Gestensteuerung

Die Gestensteuerung hat sich als moderne, berührungslose Form der Interaktion mit digitalen Geräten etabliert. Ob auf dem Smartphone, Tablet, Smart-TV oder Notebook – durch einfache Handbewegungen lassen sich Funktionen ausführen, Anwendungen steuern oder visuelle Effekte erzeugen. Dabei werden Gesten erkannt und in animierte Reaktionen umgesetzt – z. B. erscheinen beim Daumen-hoch-Gestenzeichen animierte „Likes“ auf dem Bildschirm. Gestensteuerung kann aber den Arbeitsalltag von körperlich beeinträchtigten Mitarbeitenden erheblich erleichtern, indem sie die Nutzung des Gerätes aktiv unterstützt. Zum Beispiel Programme starten oder Texte verfassen und bearbeiten.

So faszinierend diese Technologie ist, so wichtig ist auch ihre datenschutzrechtliche Betrachtung – insbesondere im Hinblick auf die Verarbeitung personenbezogener und biometrischer Daten im Sinne der Datenschutz-Grundverordnung (DSGVO). Systeme zur Gestenerkennung analysieren mithilfe integrierter Kameras (z. B. FaceTime-Kamera bei Apple) oder spezieller Sensorik (z. B. Infrarot, Tiefensensoren) kontinuierlich die Körperbewegungen der Nutzer. Dabei können insbesondere folgende Daten verarbeitet werden:

- Bewegungsprofile von Händen, Armen, Gesicht oder Körperhaltung
- Bilder oder Videos der Umgebung (z. B. durch die Webcam)
- Kontextbezogene Daten wie Zeitpunkt, Ort, Bildschirmaktivität

Um eine vom System interpretierbare Geste zu erkennen, ist eine kontinuierliche Überwachung der Sensorumgebung notwendig. Ähnlich wie Sprachassistenten, die uns ständig zuhören, um das Aktivierungswort zu erkennen, beobachten uns die optischen Sensoren kontinuierlich, um eine Geste zu erkennen. Durch das Verarbeiten der Lippenbewegungen ist es dem Betreiber möglich, zu erkennen, was ge- bzw. gesprochen wird, und aus dem Kontext der menschlichen Bewegungen lassen sich weitere Sachverhalte ableiten. Dadurch ist es dem Hersteller der Geräte oder einem Angreifer möglich, nicht nur Personenbezug herzustellen, sondern auch Unternehmenssachverhalte (Betriebsgeheimnisse) zu erfassen auszuwerten.

Aus den oben genannten Gründen ist es angezeigt, Mitarbeitende in Bezug auf die Nutzung der Gestensteuerung zu sensibilisieren, auch dann, wenn die Gestensteuerung selbst nicht genutzt wird.

Impressum

complimant AG, Edt 4, 84558 Kirchweidach

Vorstand: Franz Obermayer, Ann-Karina Wrede

Vorsitzender des Aufsichtsrates: Christian Volkmer

Telefon: +49 8683 99390-40

E-Mail: info@complimant.de / datenschutz@complimant.de

www.complimant.de

Eintragung im Handelsregister: Amtsgericht: Traunstein

Registernummer: HRB 20500 Steuernummer: 141/120/07009

Umsatzsteuer-Identifikationsnummer gemäß §27a

Umsatzsteuergesetz: DE274380239

Verantwortlich für den Inhalt nach §18 Abs. 2 MStV Franz Obermayer