KROES

ZERTIFIZIERTER DATENSCHUTZ

inklusive DSFA-Fragebogen

PRAXIS-LEITFADEN:

DSGVO & KI - 10 Praxis Tipps zur datenschutzkonformen KI - Nutzung im Unternehmen.

So nutzen Sie personenbezogene Daten rechtssicher für KI-Projekte. Ohne Angst vor Datenschutzverstößen und Bußgeldern.

Version: August 2025

KROES

ZERTIFIZIERTER DATENSCHUTZ

Herzlich Willkommen!

Es freut mich, dass Sie sich für meinen Praxis-Leitfaden **“DSGVO & KI - 10 Praxis Tipps zur datenschutzkonformen KI-Nutzung im Unternehmen**” interessieren.

Mit der zunehmenden Nutzung von KI-Tools wie zB ChatGPT, Claude oder Copilot steigen auch die rechtlichen Risiken.

Jeder Datenschutzbeauftragter in Unternehmen steht vor der zunehmenden Herausforderung, die technischen Innovationen einerseits zu ermöglichen und andererseits dem Thema DSGVO & Co. zu 100% gerecht werden zu müssen.

Dieser Praxis-Leitfaden zeigt Ihnen in 10 konkrete umsetzbare Tipps, wie Sie rechtssichere KI-Projekte realisieren können und dass ohne Angst vor Schatten-KI, Datenpannen oder empflindlichen Bußgeldern haben zu müssen.

Ich wünsche Ihnen viel Erfolg bei der Umsetzung und stehe Ihnen für Fragen gerne zur Verfügung.

Alexander Kroes

externer zertifizierter Datenschutzbeauftragter

”

In meiner Tätigkeit als externer DSB begleite ich Unternehmen bei der Einführung von KI-Systemen in Unternehmen. Von StartUp bis zum KMU.

Meine Erfahrungen dabei sind, dass die rechtlichen Anforderungen und der praktische rechtliche Umgang mit den KI-Systemen oft unklar ist.

Es fehlt zumeist an einer Struktur, um den Einsatz von KI datenschutzkonform zu planen, zu bewerten und rechtskonform umzusetzen.

Es fehlt zumeist an einer Struktur, um den Einsatz von KI datenschutzkonform zu planen, zu bewerten und rechtskonform umzusetzen.

Dieser Leitfaden unterstützt dabei, die Anforderungen bei Einsatz von KI-Systemen Schritt für Schritt sicher zu erfüllen.

Datenschutz und KI - warum das ein relevantes Thema ist und wen es betrifft

KROES
ZERTIFIZIERTER DATENSCHUTZ

Der Einsatz von künstlicher Intelligienz (KI) ist bei vielen Unternehmen mittlerweile tägliche gängige Praxis und das quer durch alle Branchen. Mit dem vermehrten Einsatz von KI-Systemem steigen auch die datenschutzrechtlichen Anforderungen deutlich.

EU AI Act vs. DSGVO: Die wichtigsten Unterschiede und Gemeinsamkeiten

Die Datenschutz-Grundverordnung (DSGVO) hat seit ihrem Inkrafttreten 2018 Maßstäbe für den Schutz personenbezogener Daten gesetzt. Der EU AI Act zielt nun auf die Regulierung von KI-Systemen ab. Beide Rahmenwerke entspringen demselben europäischen Werteverständnis: Technologie soll dem Menschen dienen, nicht umgekehrt. Dennoch bestehen markante Unterschiede.

EU AI Act vs. DSGVO: Die wichtigsten Unterschiede

Die DSGVO konzentriert sich primär auf den Schutz und die Verarbeitung personenbezogener Daten. Sie legt fest, wie Unternehmen Daten sammeln, speichern und nutzen dürfen. Der EU AI Act hingegen betrachtet KI-Systeme als Ganzes. Er schreibt vor, wie KI entwickelt, getestet, eingesetzt und kontrolliert werden sollte, um sicherzustellen, dass sie rechtskonform, sicher, fair und diskriminierungsfrei agiert. Während die DSGVO **alle Technologien** umfasst, ist der EU AI Act **ausdrücklich auf KI-Anwendungen** zugeschnitten.

EU AI Act vs. DSGVO: Die Gemeinsamkeiten

Gemeinsam ist beiden Verordnungen die Intention, **Grundrechte zu schützen**. Die DSGVO wahrt das Recht auf Datenschutz, der AI Act adressiert indirekt auch Rechte wie Gleichbehandlung und Nichtdiskriminierung. Außerdem setzen beide auf Bußgelder und Sanktionen, um die Einhaltung der Vorgaben durchzusetzen. Diese möglichen Sanktionen der Regulierung sollen sicherstellen, dass Unternehmen die Regelwerke auch ernst nehmen und umsetzen.

Gemeinsam für eine ethisch, digital vertretbare Zukunft

Insgesamt ergänzen sich DSGVO und EU AI Act: Die DSGVO schützt Daten, der AI Act reguliert die Funktionsweise der KI, die diese Daten nutzt. Zusammen bilden sie ein europäisches Fundament für eine sichere, vertrauenswürdige und ethische digitale Zukunft, in der Fortschritt und Schutz der Bürgerinnen und Bürger in Balance stehen.

info@datenschutz-kroes.at https://datenschutz-kroes.at

KROES
ZERTIFIZIERTER DATENSCHUTZ

Die Bedeutung für Unternehmen

Alle Unternehmen - unabhängig von Größe und Branche - müssen sich auf klare Spielregeln einstellen, wenn sie KI-Systeme implementieren und nutzen. Insbesondere dann, wenn dabei personenbezogene Daten verarbeitet werden.

Zentrale wesentliche Fragen hierbei sind:

- den rechtsicheren Umgang mit Trainings-und Eingabedaten
- die Pflicht zur Transparenz über Funktionslogiken und Datenverwendung
- die Abgrenzung von Verantwortlichen zwischen Anbieter, Betreiber und Nutzer
- und die Einschätzung, ob eine Datenschutz-Folgenabschätzung (DSFA) erforderlich ist

Welche Art von Unternehmen sind betroffen?

Jedes Unternehmen, welche KI-gestützte-Systeme in der Europäischen Union (EU) einsetzen oder bereitstellen und das unabhängig von Größe und Branche. Es betrifft ein Einzelunternehmen genau so wie es einen Mittelständler oder Konzern betrifft - ohne Ausnahme.

Besonders relevant ist das Thema für folgende Unternehmen:

1. IT-und Softwareunternehmen
2. Personalabteilungen mit KI im Recruting, Matching oder Skill-Profiling
3. Marketingteams, die mit Predictive Analytics oder User-Tracking arbeiten
4. Customer-Support mit automatisierten Antwortsystemen
5. Industriebetriebe mit KI-basierter Qualitätssicherung oder Steuerung
6. sowie **alle** Dienstleister, die KI-Systeme für andere entwicklen oder betreiben

Künstliche Intelligenz trifft auf Datenschutzverordnungen

KROES
ZERTIFIZIERTER DATENSCHUTZ

Rechtsgrundlagen & Zweckbindung

Durch den Einsatz von KI wird das Recht auf informationelle Selbstbestimmung als Teil des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG gefährdet.
Dies zeigt sich aktuell in vielerlei Diskussionen rund um Google Home, Amazon Echo und ähnliche intelligente Sprachassistenten. Diese zeichnen teilweise auch Gespräche und Situationen auf, wenn dies von den Nutzern gerade nicht beabsichtigt oder gewünscht wird.

Dies ist datenschutzrechtlich besonders bedenklich. Beispielsweise ist eine Datenschutzfolgenabschätzung (DSFA), sofern notwendig, kaum bis gar nicht erstellbar, da der Algorithmus selbst entscheidet und es für den Verwender daher nicht möglich ist, diese Entscheidungen nachzuvollziehen. Es entsteht ein Konflikt zwischen KI und Datenschutz, der Wettbewerbsfähigkeit der Unternehmen und der Sicherheit der Bürger und ihrer Daten.

Was zählt bei KI-Systemen und personenbezogenen Daten?

1 OHNE RECHTSGRUNDLAGE KEINE VERARBEITUNG

Jede Verarbeitung personenbezogener Daten (zB für KI-Training) benötigt eine Rechtsgrundlage gemäß Art.6 DSGVO - besonders relevant sind in der Praxis die Einwilligung der betroffenen Personen (gem. Art.6 Abs. 1 lit. a DSGVO), die Verarbeitung zur Erfüllung eines Vertrages oder zur Durchführung vorvertraglicher Maßnahmen (gem. Art. 6 Abs. 1 lit. b DSGVO) sowie das berechtigte Interesse des Verantwortlichen (gem. Art.6 Abs. 1 lit. f DSGVO).
Für besondere Kategorien personenbezogener Daten (wie zB Gesundheitsdaten) gelten zusätzlich die verschärften Voraussetzungen aus Art.9 Abs. 2 DSGVO

2 BESTANDSDATEN NIE UNGEPRÜFT FÜR KI-TRAININGS VERWENDEN

Der Zweckbindungsgrundsatz gemäß Art. 5 Abs. 1 lit. b DSGVO verlangt, dass personenbezogene Daten **nur für den Zweck verarbeitet werden, zudem sie ursprünglich erhoben wurden.**
Werden Daten etwa zur Vertragserfüllung gespeichert, ist ihre Weiterverwendung für das Training von KI-Systemen nicht ohne Weiteres zulässig.
Eine Zweckänderung ist nur möglich, wenn zuvor eine Kompatibilitätsprüfung nach Art. 6 Abs. 4 DSGVO erfolgt. Zusätzlich sind die betroffenen Personen gemäß Art. 13 Abs. 3 bzw. Art. 14 Abs. 4 DSGVO über den neuen Zweck zu informieren.

info@datenschutz-kroes.at https://datenschutz-kroes.at

3 SO WENIG WIE MÖGLICH, SO VIEL WIE NÖTIG

Beim Training von KI-Modellen ist das Prinzip der Datenminimierung gemäß Art. 5 Abs. 1 lit. c DSGVO zu beachten. **Personenbezogene Daten dürfen nur verarbeitet werden, wenn sie für den konkreten Trainingszweck erforderlich sind.** Setzen Sie daher nach Möglichkeit datenschutzfreundliche Alternativen ein, etwa anonymisierte oder synthetische Datensätze. Gleichzeitig bedeutet Datenminimierung nicht, grundsätzlich auf personenbezogene Daten zu verzichten, wenn sie für ein verlässliches Modell zwingend erforderlich sind. Entscheidend ist eine sorgfältige Abwägung zwischen der technischen Notwendigkeit und dem Risiko für die Rechte und Freiheiten der betroffenen Personen.

4 SCHATTEN-KI ERKENNEN UND STOPPEN

In Unternehmen arbeiten Mitarbeitende zunehmend mit KI-gestützten Anwendungen, oft ohne formale Freigabe oder Kontrolle. Deshalb ist es für Arbeitgeber wichtig, jetzt zu handeln und den unregulierten Einsatz sog. Schatten-KI zu unterbinden.
Schatten-KI bezeichnet den nicht genehmigten oder unbekannten Einsatz von KI-Tools durch Mitarbeitende. **Das birgt erhebliche Risiken für den Datenschutz, da nicht nachvollziehbar ist, welche personenbezogenen oder vertraulichen Daten verarbeitet oder an Dritte übermittelt werden.** Um dem entgegenzuwirken, sollte jedes Unternehmen eine verbindliche KI-Nutzungsrichtlinie etablieren, in der alle zugelassenen Tools benannt sind und klare Vorgaben zur datenschutzkonformen Nutzung gemacht werden. So erhalten Mitarbeitende Orientierung und Unternehmen reduzieren das Risiko unbeabsichtigter Datenschutzverstöße erheblich.

5 DATENQUALITÄT UND DATENZUGRIFF SICHERSTELLEN

KI-Systeme liefern nur dann zuverlässige Ergebnisse und erfüllen datenschutzrechtliche Anforderungen, wenn die verwendeten Datensätze relevant, hinreichend repräsentativ und so weit wie möglich fehlerfrei und vollständig sind. **Verantwortliche sollten daher Verfahren etablieren, mit denen die Qualität der Datensätze regelmäßig geprüft und bei Bedarf angepasst wird.** Neben der Datenqualität ist auch die Zugriffskontrolle entscheidend. Nicht alle Mitarbeitende dürfen auf alle personenbezogenen Daten zugreifen, der Zugriff ist strikt nach dem “Need-to-know” Prinzip zu beschränken.

6 DATENFOLGEABSCHÄTZUNG (DSFA) & RISIKOBEWERTUNG FEST VERANKERN

Bei risikobehafteten KI-Anwendungen ist eine Datenschutz-Folgenabschätzung (DSFA) gemäß Art. 35 DSGVO frühzeitig durchzuführen – und zwar vor Beginn der Verarbeitung personenbezogener Daten. **Ziel ist es, potenzielle Risiken für die Rechte und Freiheiten betroffener Personen zu identifizieren und durch geeignete Maßnahmen zu minimieren.** Die DSFA muss rechtzeitig abgeschlossen sein, damit ihre Ergebnisse in die Gestaltung der Verarbeitung einfließen können. Wann im Einzelnen eine DSFA erforderlich ist, erläutern die folgenden Tipps.

Wann und warum eine DSFA bei KI-Projekten unbedingt notwendig ist

7 WANN EINE DSFA VERPFLICHTEND IST GEMÄSS DSGVO

Laut Art. 35 Abs. 1 DSGVO ist eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen, wenn eine Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt – etwa bei dem Einsatz neuer Technologien wie KI-Syteme.

Art. 35 Abs. 3 DSGVO nennt drei Fälle, in denen eine DSFA verpflichtend ist:

1. Bei systematischer und umfassender Bewertung persönlicher Aspekte mittels automatisierter Verarbeitung im Sinne des Art. 22 DSGVO (z. B. beim Scoring im Kreditwesen, der automatisierten Bewerberauswahl oder KI-gestützter Bonitätsprüfung).

2. Bei umfangreicher Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DSGVO oder Art. 10 DSGVO (z. B. bei der KI-gestützter Analyse von Gesundheitsakten, biometrischen Zutrittssystemen oder der automatisierten Verarbeitung von Mitarbeiterdaten zu politischen Überzeugungen oder Religionszugehörigkeit).

3. Bei systematischer Überwachung öffentlich zugänglicher Bereiche.

KROES
ZERTIFIZIERTER DATENSCHUTZ

8 POSITIVLISTE DER DATENSCHUTZKONFERENZ BEACHTEN

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) stellt eine **Liste mit Verarbeitungstätigkeiten** zur Verfügung, bei denen eine Datenschutz-Folgenabschätzung verpflichtend durchzuführen ist.

Nach Punkt 11 dieser Liste ist dies insbesondere dann der Fall, wenn künstliche Intelligenz (KI) zur Verarbeitung personenbezogener Daten eingesetzt wird, um die Interaktion mit betroffenen Personen zu steuern oder deren persönliche Aspekte zu bewerten.

Die wichtigsten Schritte zur AI - Goverance im Unternehmen

9 AI MANAGEMENT SYSTEMATISCH ETABLIEREN

Ein funktionierendes AI Management regelt, wie KI-Systeme im Unternehmen verantwortungsvoll entwickelt, eingesetzt und überwacht wird. Dazu gehören **klare Zuständigkeiten, strukturierte Prozesse und verbindliche Leitlinien**. Integrieren Sie Ihr KI-Managementsystem (AIMS) möglichst in bestehende Systeme wie DSMS oder ISMS, denn das spart Aufwand und sorgt für eine einheitliche Steuerung. Die neue Norm ISO/IEC 42001 folgt dabei bewährten Standards wie ISO/IEC 27001.

10 AI MANAGEMENT EINSTUFEN & UMSETZEN

Bevor eine KI-Anwendung im Unternehmen eingeführt wird, sollte sie einer Risikoklassifizierung nach dem AI Act unterzogen werden. **Dabei wird bewertet, ob es sich um ein KI-System mit unannehmbarem, hohem, systemischem oder geringem Risiko handelt.** Gleichzeitig ist zu bestimmen, ob das Unternehmen Anbieter oder Betreiber ist, denn davon hängen laut AI Act konkrete Pflichten ab. Die richtige Einstufung ist daher entscheidend für rechtssichere Umsetzung und Compliance.

KROES
ZERTIFIZIERTER DATENSCHUTZ

BONUS DOKUMENTATION VON ASSETS UND USE-CASES

Dokumentieren Sie systematisch alle eingesetzten KI-Anwendungen im Unternehmen. Nutzen Sie dafür z. B. Asset-Verzeichnisse, die KI-Systeme anwendungsbezogen erfassen, sowie Use-Case-Dokumentationen nach dem Vorbild der Verzeichnisse von Verarbeitungstätigkeiten im Datenschutz. So **schaffen Sie Transparenz, erfüllen die Dokumentationspflichten und erleichtern Risikobewertungen** wie z. B. DSFA deutlich**.**

DSFA-FRAGEBOGEN

Prüfen, dokumentieren & umsetzen

KROES
ZERTIFIZIERTER DATENSCHUTZ

1) BESCHREIBUNG DER VERARBEITUNG

- Welche personenbezogenen Daten werden verarbeitet?
- Welche Personengruppen sind betroffen?
- Zu welchem Zweck erfolgt die Verarbeitung?
- Auf welcher Rechtsgrundlage basiert die Verarbeitung?
- Wer verarbeitet die Daten (intern/extern)?
- Gibt es Übermittlungen in Drittländer? Wenn ja, welche Garantien bestehen?

2) PRÜFUNG VON NOTWENDIGKEIT & VERHÄLTNISSMÄSSIGKEIT

- Welcher Zweck wird verfolgt?
- Ist die Datenverarbeitung zur Zweckerreichung geeignet?
- Gibt es gleich geeignete, jedoch weniger eingriffsintensive Alternativen?
- Ist der Eingriff in die Rechte der Betroffenen angemessen?

3) BEWERTUNG DER RISIKEN FÜR BETROFFENE

- Welche Risiken ergeben sich für die Rechte und Freiheiten der Betroffenen?
- Welche Schutzziele könnte verletzt werden? (zB Vertraulichkeit, Transparenz, etc)
- Wie wahrscheinlich ist ein Schaden? Und wie schwerwiegend wäre dieser?
- Ist der Eingriff in die Rechte der Betroffenen angemessen?

4) GEPLANTE ABHILFEMASSNAHMEN

- Welche technischen Maßnahmen sind vorgesehen?
- Welche organisatorischen Maßnahmen sind geplant?
- Wie stellen sie sicher, dass Betroffenenrechte wahrgenommen werden können?
- Reichen die Maßnahmen aus, um das Risiko auf ein akzeptables Maß zu senken?

PRAXIS-TIPP

Dokumentieren Sie unbedingt Ihre Antworten so konkret wie möglich und passen Sie den Fragebogen an Ihre konkrete Unternehmenspraxis an.
Bei Fragen, kommen Sie gerne auf mich zu – ich helfe Ihnen gern weiter.

info@datenschutz-kroes.at https://datenschutz-kroes.at

KROES
ZERTIFIZIERTER DATENSCHUTZ

DSGVO Datenschutzlösungen für Ihr Unternehmen

Datenschutz, Informationssicherheit, KI und Datenstrategien sind komplex. Und werden zwangsläufig noch komplexer werden.

Profitieren Sie von klaren Strukturen, reduziertem Aufwand und messbaren Einsparungen. Durch unsere individuelle Beratung und nachhaltige Betreuung. Ein externer Datenschutzbeauftragter ist nicht nur gesetzliche Pflicht, sondern auch eine strategisch kluge Entscheidung – mit echtem wirtschaftlichen Nutzen.

Mehr Mehr Zeit für Ihr Kerngeschäft mit unseren klaren, verlässlichen und rechtssicheren DSGVO Datenschutz-Lösungen. Ihr Unternehmen in besten Händen – gemeinsam sorgen wir für klare, rechtssichere Lösungen.
Wir begleiten Sie persönlich – **verständlich, praxisnah und rechtssicher.**

Sie benötigen Hilfe bei der Umsetzung?

Vereinbaren Sie Ihr kostenfreies Erstgespräch direkt mit mir.

Ob Sie gerade erst starten oder bestehende Prozesse optimieren wollen: Der erste Schritt kostet Sie nichts – aber er kann viel bewirken. Ganz sicher.

GRATIS 15MIN CALL BUCHEN

Alexander Kroes
externer zertifizierter Datenschutzbeauftragter

info@datenschutz-kroes.at https://datenschutz-kroes.at