CEDPO
CONFEDERATION OF EUROPEAN DATA PROTECTION ORGANISATIONS

Bonn, Bukarest, Dublin, Lissabon, Madrid, Mailand, Paris, Den Haag, Wien, Warschau

KI und persönliche Daten
Ein Leitfaden für Datenschutzbeauftragte
"Häufig gestellte Fragen"

CEDPO AI-Arbeitsgruppe
16. Juni 2023

Kontaktinformationen:
https://cedpo.eu
info@cedpo.eu

CEDPO
CONFEDERATION OF EUROPEAN
DATA PROTECTION ORGANISATIONS

Über diesen Leitfaden

Dieser Leitfaden wurde von der Arbeitsgruppe "KI und Daten" der Confederation of European Data Protection Organization (CEDPO) erstellt. Er richtet sich an Datenschutzbeauftragte und beantwortet für sie die grundlegenden Fragen, die sich stellen werden, wenn sich ihre Arbeit unweigerlich mehr und mehr mit künstlicher Intelligenz und Machine-Learning-Software überschneidet.

Die Technologien der künstlichen Intelligenz und des maschinellen Lernens entwickeln sich rasant und exponentiell, und auch wenn sie nicht immer personenbezogene Daten verarbeiten, wenn sie es tun, geschieht dies oft in einem enormen Umfang und auf einem komplexen Niveau.

Dies bringt neue Risiken für die betroffenen Personen und neue Herausforderungen für den DSB mit sich, der in der Regel nicht unbedingt über einen Informatik-Hintergrund verfügt, von dem aber dennoch erwartet wird, dass er die innere Funktionsweise und die Auswirkungen dieser Technologien analysiert und versteht. Die DSB stehen vor einer doppelten Herausforderung: Sie haben eine steile Lernkurve zu bewältigen, und das in einem dynamischen Technologiebereich, der sich täglich vor ihren Augen weiterentwickelt.

Obwohl die DSB bereits verpflichtet sind, die Datenschutzgrundsätze auf künstliche Intelligenz anzuwenden, was bereits eine komplexe Aufgabe ist (und in diesem Leitfaden erläutert wird), zeichnen sich auch neue Vorschriften ab.

Das EU-Gesetz über künstliche Intelligenz bahnt sich seinen Weg durch die EU-Gesetzgebung und wird voraussichtlich im Jahr 2024 in Kraft treten. Sobald dieses Gesetz in Kraft ist, wird es sich in wichtigen Punkten mit der DS-GVO überschneiden, was zu zusätzlichen Verpflichtungen für DSB führt. Dieser Leitfaden soll die Überschneidungen zwischen diesen beiden wichtigen und miteinander verbundenen Säulen des EU-Rechtsrahmens aufzeigen.

Unternehmen und öffentliche Einrichtungen arbeiten schnell daran, Lösungen für künstliche Intelligenz zu verstehen und zu implementieren, um alle Arten von Effizienzsteigerungen und

Möglichkeiten zur Umsatzsteigerung zu erreichen. Der DSB hat keine andere Wahl, als Schritt zu halten; die Technologie wird nicht warten. Dieser Leitfaden stellt daher einen Ausgangspunkt für DSB dar, um sich in der zunehmend kritischen und komplexen Welt der künstlichen Intelligenz zurechtzufinden.

CEDPO
CONFEDERATION OF EUROPEAN DATA PROTECTION ORGANISATIONS

Inhaltsübersicht

CEDPO
CONFEDERATION OF EUROPEAN DATA PROTECTION ORGANISATIONS

1. Regelt die Datenschutz-Grundverordnung künstliche Intelligenz und maschinelles Lernen?

Ja, die DS-GVO regelt KI und maschinelles Lernen. Die DS-GVO regelt alle Formen von Technologien, die personenbezogene Daten verarbeiten. Als horizontale, risikobasierte Omnibus-Verordnung, die eher auf allgemeiner als auf spezifischer Ebene regelt, vertritt die DS-GVO weitreichende Grundsätze, die unabhängig von dem jeweiligen Kontext gelten, in dem personenbezogene Daten verarbeitet werden. Dies steht im Gegensatz zu vertikalen, regelbasierten Vorschriften, die speziell für bestimmte Technologien oder Sektoren gelten.

Dies hat zur Folge, dass die DS-GVO in Bezug auf Technologie ausdrücklich technologieneutral ist. Die Worte "KI" oder "maschinelles Lernen" tauchen nirgendwo im Text der DS-GVO auf, aber auch keine Verweise auf Blockchain, Internet der Dinge, nicht-fungible Token (NFTs), virtuelle Realität oder andere neue Technologien. Das Fehlen solcher Verweise ist beabsichtigt und nicht zufällig. Die Logik des Gesetzgebers war, dass die Erwähnung spezifischer Technologien dazu führen könnte, dass noch unbekannte, zukünftige Technologien den Anwendungsbereich der Verordnung umgehen. So heißt es in Erwägungsgrund 15: Um ein ernsthaftes Risiko der Umgehung zu vermeiden, sollte der Schutz natürlicher Personen technologieneutral sein und nicht von den verwendeten Techniken abhängen".

Der oben genannte Grundsatz der Technologieneutralität der DS-GVO wurde auch vom Gerichtshof der Europäischen Union in der Rechtssache C-25/17 *Tietosuojavaltuutettu und Jehovan todistajat - uskonnollinen yhdyskunta* geprüft und bestätigt. Die Große Kammer des Gerichtshofs stellte fest, dass im Hinblick auf "den Schutz des Einzelnen ... der Umfang dieses Schutzes nicht von den verwendeten Techniken abhängen darf, da andernfalls die ernste Gefahr einer Umgehung bestünde".[1]

Die DS-GVO ist somit zukunftssicher, da sie hochrangige Grundsätze enthält, die für jede neu entstehende Technologie oder sogar für jeden unvorhergesehenen Datenverarbeitungszweck angepasst werden können. Die Reaktion auf die Covid-19-Pandemie im Jahr 2020 hat beispielsweise gezeigt, wie die bestehenden allgemeinen Grundsätze der DS-GVO erfolgreich auf einen unerwarteten Notfall angewandt werden können, der zur raschen Entwicklung neuer,

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62017CJ0025

potenziell in die Privatsphäre eingreifender Technologien, wie Covid-19-Track-and-Trace-Anwendungen, führte.

Wenn also eine KI- oder maschinelle Lerntechnologie personenbezogene Daten verarbeitet, gilt die DS-GVO unabhängig von Art, Aussehen, Technik, Kontext oder Verwendung. So wurde beispielsweise die aktuelle Entwicklung leistungsstarker großsprachiger Modelle wie ChatGPT nicht ausdrücklich vorhergesehen, als die DS-GVO 2018 in Kraft trat. Es ist jedoch klar, dass diese und andere derartige Entwicklungen in den Anwendungsbereich der DS-GVO fallen und mit ihren Grundsätzen vereinbar sein müssen.

2. Hat die automatisierte Verarbeitung immer mit KI oder maschinellem Lernen zu tun?

Nein, es gibt viele Fälle, in denen die automatisierte Verarbeitung keine KI oder maschinelles Lernen beinhaltet. Erwägungsgrund (15) der DS-GVO bestätigt, dass sich die automatisierte Verarbeitung auf die Verarbeitung mit automatisierten Mitteln bezieht, im Gegensatz zur Verarbeitung, die manuell durchgeführt wird. Datenverarbeitungsvorgänge werden häufig "automatisiert", ohne dass eine KI- oder maschinelle Lernkomponente beteiligt ist. So beinhalten beispielsweise Tools für das Kundenbeziehungsmanagement (CRM) eine automatisierte Verarbeitung personenbezogener Daten (durch Computersysteme), ohne dass notwendigerweise KI oder maschinelles Lernen beteiligt sind.

Die gleiche Argumentation gilt für die beiden Kernkonzepte, die in den Leitlinien des Europäischen Datenschutzausschusses (EDPB) zur automatisierten Einzelentscheidung und zum Profiling für die Zwecke der Verordnung (EU) 2016/679 dargelegt sind:[2] Obwohl davon auszugehen ist, dass KI und maschinelles Lernen zunehmend an Bedeutung gewinnen werden, wurden und werden sowohl die automatisierte Entscheidungsfindung als auch das Profiling auch ohne den Einsatz von KI angewendet werden können.

Profiling ist definiert in Art. 4 der EU-DS-GVO als "jede Form der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Standort oder Ortswechsel dieser Person zu analysieren oder vorherzusagen". Wie bereits erwähnt, beinhaltet das Profiling jedoch nicht immer KI oder maschinelles Lernen, was durch viele Anwendungsfälle bestätigt wird.

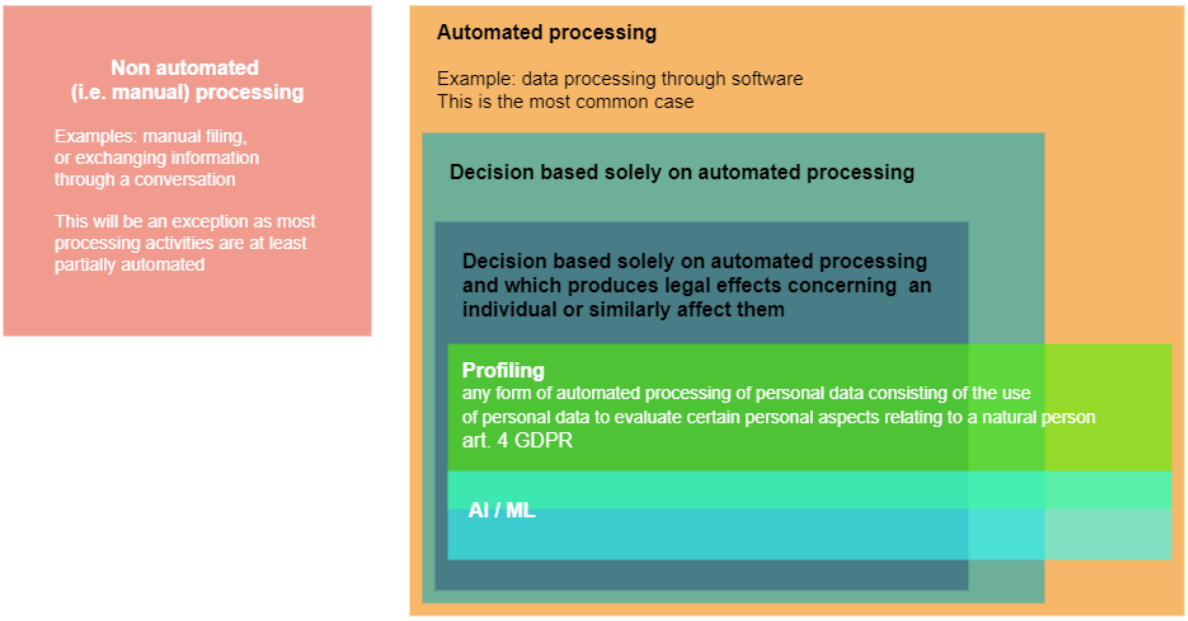
[2] https://ec.europa.eu/newsroom/article29/items/612053/en

Beispielsweise haben E-Commerce-Unternehmen schon lange vor der Verbreitung von KI oder maschinellem Lernen Profile erstellt, um die Interessen und Vorlieben von Einzelpersonen zu verstehen und dann entsprechende Produkte vorzuschlagen.

Entscheidungen, die "ausschließlich auf einer automatisierten Verarbeitung beruhen und Rechtswirkungen erzeugen oder Personen in ähnlicher Weise beeinträchtigen", werden in der EU-DS-GVO, insbesondere in Erwägungsgrund (71) und Artikel 22, behandelt. Erwägungsgrund (71) enthält zwei Beispiele: die "automatische Ablehnung eines Online-Kreditantrags" oder die Anwendung von "elektronischen Einstellungsverfahren ohne menschliches Eingreifen". Es liegt auf der Hand, dass bei solchen Entscheidungen nicht immer KI oder maschinelles Lernen zum Einsatz kommen.

Wie in den oben genannten EDPB-Leitlinien zu automatisierten Einzelentscheidungen und Profiling dargelegt, kann beispielsweise die automatische Ablehnung eines Online-Kreditantrags mit einem Algorithmus umgesetzt werden, der einen Antrag anhand einer Reihe von Kriterien bewertet, etwa anhand der im Antragsformular gemachten Angaben oder anhand von Informationen über frühere Kontobewegungen einschließlich Zahlungsrückständen. Diese können ohne KI oder maschinelles Lernen implementiert werden.

Das folgende Diagramm zeigt, wie die Konzepte der automatisierten Verarbeitung, der KI und des maschinellen Lernens konvergieren und divergieren:



3. Sind KI und maschinelles Lernen immer mit der Verarbeitung personenbezogener Daten verbunden?

Nein, bei KI und maschinellen Lernsystemen geht es nicht immer um die Verarbeitung personenbezogener Daten. Sie können für verschiedene Zwecke eingesetzt werden, die möglicherweise keinen Bezug zu personenbezogenen Daten haben, wie z. B. die Wettervorhersage, bei der der Dateninput aus atmosphärischen Messungen von Sensoren besteht, oder die Präzisionslandwirtschaft zur Optimierung des Einsatzes von Pestiziden und Nährstoffen. Es gibt also zahlreiche Fälle, in denen KI und maschinelle Lernsysteme nicht-personenbezogene Daten verarbeiten.

Die von KI-Systemen verarbeiteten Datensätze sollten jedoch eingehender untersucht werden, auch wenn diese Systeme a priori keine personenbezogenen Daten enthalten. Es ist wichtig zu beachten, dass es zwei Arten von nicht personenbezogenen Daten geben kann: Daten, die sich ursprünglich nicht auf eine bestimmte oder bestimmbare natürliche Person bezogen haben, und Daten, die ursprünglich personenbezogen waren, dann aber anonymisiert wurden. Anonymisierte Daten können auch unter Verwendung zusätzlicher Daten nicht einer bestimmten Person zugeordnet werden. Wenn jedoch nicht-personenbezogene Daten in irgendeiner Weise mit einer Person in Verbindung gebracht werden können und diese dadurch direkt oder indirekt identifizierbar wird, müssen diese Daten als personenbezogene Daten betrachtet werden. Mehrere Beispiele für die Re-Identifizierung von vermeintlich anonymen Datensätzen haben gezeigt, dass bei der Anonymisierung von Datensätzen besondere Vorsicht geboten ist.

Der Fall der gemischten Datensätze sollte ebenfalls berücksichtigt werden, da diese Datensätze aus einer Kombination von personenbezogenen und nicht personenbezogenen Daten bestehen. Die Grenze zwischen personenbezogenen und nicht personenbezogenen Daten ist daher manchmal unscharf, und innerhalb eines gemischten Datensatzes können personenbezogene und nicht personenbezogene Daten sogar untrennbar miteinander verbunden sein. Diese Art von Datensätzen ist besonders häufig bei neuen technologischen Entwicklungen wie dem Internet der Dinge, aber auch bei KI und maschinellen Lernsystemen anzutreffen. In diesem Fall gilt die DS-GVO.

Sobald die Frage geklärt ist, ob die in den Datensätzen enthaltenen Daten personenbezogen sind oder nicht, muss eine weitere Frage geklärt werden.

Es sei darauf hingewiesen, dass die Implementierung eines KI-Systems (im Allgemeinen) in zwei Phasen erfolgt, der Trainingsphase und der Produktionsphase. In der Trainingsphase lernt das KI-System aus einer Reihe von Daten und erstellt ein Modell, das Vorhersagen oder Entscheidungen treffen kann. In der Produktionsphase wird das trainierte Modell auf neue Daten angewandt, um Ergebnisse wie Vorhersagen, Empfehlungen oder Entscheidungen zu

generieren. Diese beiden Schritte dienen nicht demselben Ziel und sollten daher voneinander getrennt werden.

Es ist also möglich, dass ein KI-System die Verarbeitung personenbezogener Daten sowohl in der Trainings- als auch in der Produktionsphase, aber auch nur in einer der beiden Phasen beinhaltet. In dieser Hinsicht ist es notwendig, alle Phasen des Prozesses der Implementierung eines KI-Systems zu untersuchen.

Wie bereits bei der Ableitung personenbezogener Daten aus nicht personenbezogenen Daten erwähnt, ist es außerdem wichtig zu betonen, dass KI-Systeme, auch wenn sie in diesen Phasen nicht ausdrücklich mit personenbezogenen Daten gefüttert werden, dennoch personenbezogene Informationen aus nicht personenbezogenen Daten ableiten können. Sowohl die Eingabedaten als auch die Ausgabedaten können personenbezogene Daten enthalten, und das eine schließt das andere nicht aus.

In Anbetracht all dieser Aspekte können wir sagen, dass KI und maschinelle Lernsysteme nicht immer personenbezogene Daten verarbeiten, aber es muss unbedingt sichergestellt werden, dass die verwendeten und erzeugten Daten wirklich nicht personenbezogen sind, wenn dies das gewünschte Ziel ist.

Eine letzte Voraussetzung sollte beachtet werden. Auch wenn die Hauptverarbeitungsaktivitäten eines KI-Tools keine personenbezogenen Daten betreffen, ist es dennoch möglich, dass es personenbezogene Daten verarbeitet, die mit dem tatsächlichen menschlichen Nutzer des Tools verbunden sind. Diese können mit dem für die Nutzung des KI-Systems erforderlichen Konto sowie mit "Nutzungsdaten" verknüpft sein, die direkt oder indirekt eine tatsächliche Person identifizieren können. Einige personenbezogene Daten könnten sogar aus einem solchen Anwendungsfall abgeleitet werden, vom Endnutzer oder einer dritten Person, insbesondere bei generativer KI.

4. Gelten bestimmte Artikel und Erwägungsgründe der Datenschutz-Grundverordnung speziell für KI und maschinelles Lernen?

Die DS-GVO gilt für jede Verarbeitung personenbezogener Daten; daher gilt die DS-GVO im Grunde immer dann, wenn ein KI- oder maschinelles Lernsystem mit der Verarbeitung personenbezogener Daten beschäftigt ist. Es ist wichtig zu beachten, dass diese Verpflichtungen jetzt gelten. Ein DSB sollte nicht auf die formale Regulierung von KI durch die Europäische Kommission im Rahmen des vorgeschlagenen KI-Gesetzes warten, um sicherzustellen, dass die Nutzung von KI durch eine Organisation mit ihren Datenschutzverpflichtungen gemäß der DS-

GVO übereinstimmt. Die DS-GVO ist natürlich technologieunabhängig und enthält keine spezifischen Verweise auf KI oder auf maschinelles Lernen basierende Verarbeitung an sich.

Ungeachtet dessen gibt es einige Nuancen, die berücksichtigt werden müssen. Zunächst einmal beinhalten nicht alle KI- oder maschinellen Lernsysteme die Verarbeitung personenbezogener Daten, so dass die DS-GVO nicht anwendbar wäre; darüber hinaus sieht Artikel 2 Absatz 2 der DS-GVO verschiedene Ausnahmen vor, und die Verwendung eines KI- oder maschinellen Lernsystems unter diesen Umständen wäre auch unter diesen Ausnahmen ausgeschlossen (unabhängig davon, ob personenbezogene Daten verarbeitet werden oder nicht).

Es gibt eine Reihe von Möglichkeiten, wie KI und maschinelle Lernsysteme mit personenbezogenen Daten in Berührung kommen können, unter anderem:

- Sie können Teil des Datensatzes sein, der zum "Trainieren" des Systems verwendet wird.
- Sie können z. B. im Internet nach einer Anfrage durchsucht werden (beachten Sie, dass es im Sinne der DS-GVO keine Rolle spielt, ob die Daten ansonsten öffentlich sind).
- Sie kann vom Endnutzer als Teil einer Abfrage oder einer anderen Eingabe bereitgestellt werden
- Sie kann durch Inferenz oder Assoziation über Mustervergleiche usw. erzeugt werden.
- Angesichts der dem generativen Modell innewohnenden Beschränkungen kann es sich einfach etwas ausdenken, d. h. plausible Inhalte erzeugen oder "halluzinieren".

Wann immer ein KI- oder maschinelles Lernsystem personenbezogene Daten verarbeitet (unabhängig davon, wie diese Daten in seinen Besitz gelangt sind), gibt es eine Reihe von Artikeln in der DS-GVO, die direkt anwendbar sind. Dazu gehören:

- Artikel 5 (Grundsätze); der Einsatz von KI oder maschinellen Lernsystemen muss, wenn personenbezogene Daten betroffen sind, alle Grundsätze einhalten. Wie bei jedem System zur Verarbeitung personenbezogener Daten sollte eine Risikobewertung durchgeführt werden; besondere Bedenken können z. B. in Bezug auf Transparenz, Minimierung und Genauigkeit bestehen (siehe Anmerkung zu "Halluzination" oben). (siehe auch Erwägungsgrund 39).

- Artikel 4, 6, 7 (Rechtmäßigkeit der Verarbeitung, Einwilligung); soweit KI und maschinelle Lernsysteme auf großen Datensätzen "trainiert" werden, muss es dafür eine angemessene Rechtsgrundlage geben. Es mag sein, dass man sich unter vielen Umständen auf das Konzept des "berechtigten Interesses" stützen würde, aber nicht, dass dies eindeutig nachgewiesen werden muss (Erwägungsgrund 47). Bestimmte Umstände (z.B. die Verarbeitung besonderer Kategorien) erfordern eine Einwilligung (Art. 7), während die Ausbildung des Systems auf der Grundlage wissenschaftlicher

Forschungszwecke durchgeführt worden sein mag, entfällt diese Grundlage, sobald die Nutzung des Systems in den kommerziellen Bereich übergeht.

- Artikel 22 (Automatisierte Entscheidungsfindung); diesem Bereich wird angesichts der potenziellen Einsatzmöglichkeiten von KI und maschinellen Lernsystemen viel Aufmerksamkeit gewidmet. Artikel 22 gibt den betroffenen Personen das Recht, gegen eine solche Verarbeitung Widerspruch einzulegen, aber von größerem Interesse ist vielleicht das entsprechende Recht nach Artikel 14 Absatz 2 Buchstabe g, "aussagekräftige Informationen über die betreffende Logik" zu erhalten, was angesichts der Art der betreffenden Systeme eine Herausforderung darstellt.

- Artikel 25 (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen); nach Artikel 25 muss der für die Verarbeitung Verantwortliche den "Stand der Technik" berücksichtigen, um die Anforderungen der Verordnung zu erfüllen. In Anbetracht der Komplexität und der Unsicherheiten, die KI und maschinelle Lernsysteme umgeben, sind möglicherweise zusätzliche Schutzmaßnahmen erforderlich, um die Rechte der betroffenen Personen zu schützen. Beachten Sie, dass in Erwägungsgrund 78 ausdrücklich die "Verarbeitung personenbezogener Daten zur Erfüllung einer Aufgabe" als ein Bereich genannt wird, für den dies gilt.

- Artikel 35, 36 (Datenschutz-Folgenabschätzung); Vieles von dem oben Gesagten verdeutlicht die Bedeutung von Datenschutzfolgenabschätzungen in diesem Bereich. Möglicherweise erfordern KI- und maschinelle Lernsysteme eher eine Datenschutzfolgenabschätzung als herkömmliche Informationsverarbeitungssysteme. Hier gibt es eine Konvergenz mit dem KI-Gesetz, wenn die Systeme "hochriskant" sind (obwohl die Bedeutung von "hochriskant" in jedem Fall unterschiedlich ist); in diesem Fall verlangt Artikel 36.1 eine vorherige Konsultation mit den Aufsichtsbehörden, wobei diese Behörden über eine angemessene technische Bandbreite in diesem Bereich verfügen müssen.

5. Wenn die DS-GVO bereits KI und maschinelles Lernen regelt, warum dann warum brauchen wir brauchen wir dann noch das KI-Gesetz?

Während die EU-DS-GVO und das EU-Gesetz über künstliche Intelligenz (KI-Gesetz) vordergründig wie ähnliche Rechtsvorschriften erscheinen mögen, da beide Regelungen zur Rechenschaftspflicht, Steuerung und Überwachung vorsehen, ist es wichtig, zunächst anzuerkennen, dass sie allein im Kontext von KI und maschinellem Lernen unterschiedlichen Regulierungszwecken dienen. Einerseits ist die DS-GVO, die sich in erster Linie mit dem Schutz

personenbezogener Daten befasst, technologieunabhängig und bezieht sich nicht ausdrücklich auf spezifische technologische Anwendungen (einschließlich KI oder maschinelles Lernen). Andererseits stellt das KI-Gesetz einen direkteren, praxisorientierten Ansatz für die KI-Regulierung dar und zielt darauf ab, einen umfassenden Rechtsrahmen zu schaffen, um die verantwortungsvolle Entwicklung und Nutzung von KI und auf maschinellem Lernen basierenden Systemen in der EU zu fördern.

In der DS-GVO wird anerkannt, dass sich bestimmte Verarbeitungsvorgänge auf die Ausübung der Grundrechte und -freiheiten auswirken, insbesondere auf das Recht auf Privatsphäre und Datenschutz, sofern diese Arten von Verarbeitungstätigkeiten die Verwendung personenbezogener Daten von EU-Bürgern beinhalten. Da die DS-GVO im Wesentlichen für alle Verarbeitungen personenbezogener Daten gilt, findet die DS-GVO im Grunde immer dann Anwendung, wenn ein KI- oder maschinelles Lernsystem mit der Verarbeitung personenbezogener Daten beschäftigt ist. Auf den ersten Blick ist dieser Ansatz relativ einfach, doch gibt es einige Nuancen, die zu beachten sind. Erstens erfordern nicht alle KI- oder maschinellen Lernsysteme die Verarbeitung personenbezogener Daten, so dass die DS-GVO unter diesen Umständen nicht gilt. Darüber hinaus sieht Artikel 2 Absatz 2 der DS-GVO vor, dass die Verwendung einer KI oder eines maschinellen Lernsystems unter bestimmten Umständen ebenfalls ausgeschlossen ist (unabhängig davon, ob personenbezogene Daten verarbeitet werden oder nicht).

Da nicht alle Anwendungen von KI und maschinellem Lernen zu Aktivitäten führen, die einer Verarbeitung personenbezogener Daten gleichkommen, erkennt das KI-Gesetz an, dass die Nutzung und der Einsatz von KI und maschinellen Lernsystemen einen Bereich von breiterem ethischem und gesellschaftlichem Interesse darstellt, der oft nicht in den Anwendungsbereich der DS-GVO fallen wird. Bestimmte Praktiken, die KI oder auf maschinellem Lernen basierende Techniken nutzen, könnten beispielsweise zur Aufrechterhaltung kultureller Vorurteile oder diskriminierender Praktiken führen oder Sicherheitsrisiken in Echtzeit darstellen. Die DS-GVO könnte unter diesen Umständen einfach nur wenig relevant oder anwendbar sein. In Anbetracht der Tatsache, dass die KI-Gesetzgebung nur begrenzt in der Lage ist, Bereiche von allgemeinem Interesse zu behandeln, die nicht in den Bereich des Schutzes der Privatsphäre und des Datenschutzes fallen, verpflichtet sie sich, einen umfassenden und technologisch maßgeschneiderten Rahmen zu entwickeln, der die DS-GVO in ihren Bemühungen um die Förderung verantwortungsvoller KI-Innovationen in Europa unter Wahrung der Grundrechte und -werte der Union ergänzen wird.

6. Wie lassen sich einige der Grundprinzipien des Datenschutzes auf KI und maschinelles Lernen anwenden?

Wie bereits erwähnt, gilt die DS-GVO generell für die Verarbeitung personenbezogener Daten durch KI-/Maschinenlernsysteme, so dass zwangsläufig alle Kerngrundsätze des Datenschutzes Anwendung finden. Bestimmte Grundprinzipien der DS-GVO sind jedoch für KI/Maschinelles Lernen besonders geeignet und anwendbar. In diesen Fällen gibt es eine starke Überschneidung zwischen Datenschutz und KI-Governance.

Erstens ist der grundlegende Grundsatz der Transparenz, wie er in Artikel 12 der DS-GVO verankert ist, für die Verwaltung von KI/Maschinenlernsystemen von Bedeutung. Bei vielen derartigen Systemen wird es für die betroffenen Personen nicht immer offensichtlich sein, dass ihre Daten mit Hilfe dieser Technologien sozusagen im Hintergrund verarbeitet werden, und es wird auch nicht klar sein, wie diese Systeme funktionieren. In dieser Hinsicht sollten sich die DSB der Transparenzanforderungen der DS-GVO und des KI-Gesetzes bewusst sein, die beide in unterschiedlicher Hinsicht Transparenz verlangen.

Die DS-GVO schreibt eine allgemeine Transparenzpflicht bei der automatisierten Verarbeitung vor. In Artikel 12 heißt es: Der für die Verarbeitung Verantwortliche ergreift geeignete Maßnahmen, um der betroffenen Person alle Informationen ..., die sich auf die Verarbeitung beziehen, in knapper, transparenter, verständlicher und leicht zugänglicher Form unter Verwendung einer klaren und einfachen Sprache zur Verfügung zu stellen; dies gilt insbesondere für Informationen, die sich speziell an ein Kind richten". Wenn beispielsweise die von Ihrer Organisation geplante Nutzung eines KI-Systems die Verwendung personenbezogener Daten erfordert, die direkt von Einzelpersonen erhoben wurden, um ein Modell zu trainieren, müssen Sie zunächst prüfen, ob Sie die Transparenzverpflichtung gemäß der DS-GVO erfüllt haben, und die betroffenen Personen darüber informieren, wie ihre Daten während des Lebenszyklus Ihres KI-Systems verwendet werden.

Das KI-Gesetz ergänzt diese allgemeine Anforderung jedoch durch eine Reihe spezifischer Transparenzanforderungen. Insbesondere Artikel 52 erlegt Verpflichtungen in Bezug auf die Schaffung sogenannter Deep Fakes auf, die auf KI/Maschinenlerntechnologie basieren. In Artikel 52 Absatz 1 heißt es: "Die Anbieter stellen sicher, dass KI-Systeme, die für die Interaktion mit natürlichen Personen bestimmt sind, so konzipiert und entwickelt werden, dass natürliche Personen darüber informiert werden, dass sie mit einem KI-System interagieren, es sei denn, dies ist aus den Umständen und dem Kontext der Nutzung offensichtlich.

Ein weiterer Grundsatz, bei dem sich Datenschutz und KI-Governance überschneiden, ist der Grundsatz der Fairness. Artikel 5 Absatz 1 Buchstabe a der DS-GVO sieht eine weitreichende Verpflichtung vor, dass personenbezogene Daten "nach Treu und Glauben" verarbeitet werden müssen. Im Zusammenhang mit der Verarbeitung personenbezogener Daten ist Fairness ein absichtlich dehnbarer Grundsatz, der die unzähligen Möglichkeiten erfassen soll, wie eine Partei personenbezogene Daten auf unlautere Weise verarbeiten kann. Im Zusammenhang mit künstlicher Intelligenz und maschinellem Lernen hat der Fairness-Grundsatz jedoch eine eindeutigere Anwendung. Wenn Sie als DSB beispielsweise die Fairness einer KI-/Maschinenlernanwendung prüfen, werden Sie sich Gedanken über das Potenzial für Voreingenommenheit und/oder Diskriminierung in den verwendeten Algorithmen machen. Dabei kann es sich um rassistische Voreingenommenheit handeln, wenn die Trainingsdaten selbst gegenüber einer bestimmten Rasse voreingenommen sind, oder um geschlechtsspezifische Voreingenommenheit, wenn ein Geschlecht unverhältnismäßig stark betroffen ist. In diesen Fällen handelt es sich um eine unlautere Verarbeitung personenbezogener Daten.

Schließlich hat der Grundsatz der Erklärbarkeit, ein Begriff aus der KI-Governance, der das Ausmaß bezeichnet, in dem eine von einer KI/einem maschinellen Lernalgorithmus getroffene Entscheidung in menschlich lesbaren Begriffen erklärt werden kann, auch seine Entsprechung in der DS-GVO. In Bezug auf die KI-Governance bedeutet die Anforderung der Erklärbarkeit, dass die Verantwortlichen die kausalen Zusammenhänge zwischen den Eingabedaten und den endgültigen Entscheidungen darlegen müssen, soweit dies möglich ist. Die DSB sollten sich bewusst sein, dass Artikel 14 Absatz 2 Buchstabe g diese Anforderung im Zusammenhang mit personenbezogenen Daten klar formuliert und feststellt, dass den betroffenen Personen "aussagekräftige Informationen über die Logik" der automatisierten Verarbeitung zur Verfügung gestellt werden müssen.

7. KI und maschinelles Lernen! Das ist doch dasselbe, oder?

KI und maschinelles Lernen sind zwei eng miteinander verbundene, aber unterschiedliche Bereiche der Informatik.

KI bezieht sich auf das umfassendere Konzept der Entwicklung von Maschinen, die Aufgaben ausführen können, für die normalerweise menschliche Intelligenz erforderlich wäre. Dies kann eine Reihe von Technologien umfassen, z. B. die Verarbeitung natürlicher Sprache, Robotik, Computer Vision und mehr. Ziel der KI ist es, Systeme zu schaffen, die Aufgaben ausführen können, für die normalerweise menschliche Intelligenz erforderlich wäre, wie z. B. das Erkennen von Bildern oder das Verstehen natürlicher Sprache, und die in der Lage sind, Entscheidungen zu treffen. Der Grad der Leistungsfähigkeit eines KI-Systems hängt von der

Ebene und der Komplexität des Systems ab. Die Entwicklung eines KI-Systems umfasst die Entwicklung von Algorithmen und Systemen, die auf der Grundlage von Eingabedaten denken, lernen und Entscheidungen treffen können.

Maschinelles Lernen hingegen ist ein Teilbereich der KI, der sich auf die Entwicklung von Algorithmen konzentriert, die mit der Zeit lernen und sich verbessern können. Im Wesentlichen geht es beim maschinellen Lernen darum, Maschinen beizubringen, aus Daten zu lernen, ohne ausdrücklich programmiert zu werden. Im Wesentlichen geht es beim maschinellen Lernen darum, einen Computer darauf zu trainieren, Muster zu erkennen und auf der Grundlage großer Datenmengen Vorhersagen zu treffen. Dies kann überwachtes Lernen, unüberwachtes Lernen und halbüberwachtes Lernen umfassen. Beim überwachten Lernen wird ein Algorithmus mit markierten Daten trainiert, was bedeutet, dass für eine bestimmte Eingabe die richtige Ausgabe bereitgestellt wird. Der Algorithmus lernt, die Eingaben auf der Grundlage der gelabelten Beispiele, die er erhalten hat, den Ausgaben zuzuordnen. Beim unüberwachten Lernen hingegen wird ein Algorithmus auf nicht gekennzeichnete Daten trainiert, und der Algorithmus muss selbständig Muster und Strukturen in den Daten finden. Semi-überwachtes Lernen ist eine Kombination aus überwachtem und unüberwachtem Lernen, bei der einige gekennzeichnete Daten zur Verfügung gestellt werden, der Algorithmus aber auch aus nicht gekennzeichneten Daten lernen muss.

Zusammenfassend lässt sich sagen, dass KI ein breiteres Konzept ist, das eine Reihe von Technologien umfasst, während maschinelles Lernen eine spezifische Untergruppe der KI ist, die sich auf die Entwicklung von Algorithmen konzentriert, die lernen und sich mit der Zeit verbessern können.

8. Ich bin ein DSB. Sollte ich mir Sorgen über das Wachstum von KI und maschinellem Lernen machen?

Als DSB sollten Sie in der Tat über das Wachstum von KI und maschinellem Lernen besorgt sein, da diese Technologien zu einer automatisierten Entscheidungsfindung führen können, die potenziell schwerwiegende Auswirkungen auf die Rechte und Freiheiten der betroffenen Personen haben kann. KI kann zum Beispiel dazu verwendet werden, automatisierte Entscheidungen über die Vorauswahl von Bewerbern zu treffen. Wenn Sie verstehen, wie die Algorithmen funktionieren, können Sie potenzielle Datenschutzrisiken erkennen und bei Bedarf geeignete Schutzmaßnahmen ergreifen.

Unabhängig von der Größe Ihres Unternehmens werden Sie als DSB von der Integration von KI und maschinellem Lernen in die IT-Systeme Ihres Unternehmens betroffen sein. Die folgenden Anwendungen nutzen sie beispielsweise bereits oder planen, sie in Zukunft zu nutzen:

- Microsoft Office soll bereits in diesem Jahr, 2023, über KI und maschinelles Lernen verfügen;
- Viele HR-, Gehaltsabrechnungs-, Vertriebs- und/oder Codierungssysteme nutzen bereits KI und maschinelles Lernen, und diejenigen, die dies nicht tun, haben Pläne, diese Technologien in naher Zukunft zu integrieren;
- Chatbots, die persönlichen Daten von Unternehmen und Kunden nutzen, um personalisierte Antworten zu geben, sind bereits in vielen Unternehmen im Einsatz und werden in Zukunft noch stärker genutzt werden.

Als DSB müssen Sie und Ihr Team für alle neuen Datenverarbeitungstätigkeiten Datenschutz-Folgenabschätzungen durchführen. Dabei ist es wichtig, die Auswirkungen und Grenzen des KI-Systems zu verstehen, insbesondere im Hinblick auf mögliche Verzerrungen. Auch die Möglichkeit, dass die KI ungenaue Ergebnisse liefert, muss berücksichtigt werden.

Wie bereits in früheren Fragen dargelegt, werden Organisationen, die ihre eigenen KI-Hochrisikosysteme entwickeln, in naher Zukunft nicht nur durch die DS-GVO, sondern auch durch das KI-Gesetz geregelt. Beispiele für solche Hochrisikosysteme sind in den folgenden Szenarien zu finden:

- allgemeine oder berufliche Bildung,
- für die Einstellung, Bewertung oder Aufgabenzuweisung von Mitarbeitern,
- Kreditwürdigkeitsprüfung von Einzelpersonen,
- die Feststellung der Anspruchsberechtigung von Einzelpersonen auf Sozialdienstleistungen und -leistungen.

Als DSB, der für eine Organisation arbeitet, die KI-Systeme implementiert, sollten Sie eine Rolle im KI-Risikomanagementverfahren spielen. Da die DS-GVO die Umsetzung des Datenschutzes durch Technik und durch Voreinstellungen vorschreibt, hat der DSB die Aufgabe, die bekannten und vorhersehbaren Risiken durch eine angemessene Gestaltung und Entwicklung von KI-Systemen, die personenbezogene Daten verarbeiten, zu ermitteln, zu verringern oder zu mindern.

9. Ich habe von ChatGPT und generativer KI gehört. Sollte ich mir als DSB Sorgen machen?

ChatGPT ist derzeit das am weitesten verbreitetes Modell für generative KI (oder Gen-AI) in der Welt und hat bereits zwei Monate nach seiner Einführung mehr als 100 Millionen Nutzer. Gen-AI ist eine Kategorie der künstlichen Intelligenz, die eine Vielzahl von Inhalten oder Daten erstellen kann, wie z. B. Bilder, Videos, Audio, Text und 3D-Modelle. Wie andere Formen der

künstlichen Intelligenz wird auch die künstliche Intelligenz auf der Grundlage großer Datenmengen (z. B. von Internetseiten) trainiert. Ein typischer Anwendungsfall ist die Bereitstellung einiger Eingabedaten und einer Anfrage oder Aufforderung, die dann die Gen-AI-Technologie zur Erstellung einer Antwort anleitet. Bei der Antwort kann es sich auch um eine beliebige Form von Daten handeln.

Die europäischen Datenschutzaufsichtsbehörden haben eine Reihe von Bedenken hinsichtlich der Verarbeitung personenbezogener Daten durch ChatGPT geäußert. Die spanische Datenschutzbehörde (AEPD) teilte Anfang April 2023 in einer Erklärung mit, dass sie eine Untersuchung gegen OpenAI, die Entwickler von ChatGPT, eingeleitet habe, um "einen möglichen Verstoß gegen die Vorschriften" zum Datenschutz in Spanien zu untersuchen.

Die Entscheidung der AEPD, gegen ChatGPT zu ermitteln, folgt auf eine ähnliche Entscheidung der italienischen Datenschutzaufsichtsbehörde (Garante per la protezione dei dati personali) von Ende März 2023, den Chatbot in Italien vorübergehend zu sperren, weil Bedenken hinsichtlich der Verwendung personenbezogener Daten italienischer Bürger bestehen.

Die italienische Datenschutzaufsichtsbehörde erklärte, es gebe keine Rechtsgrundlage, die "die massenhafte Erhebung und Speicherung personenbezogener Daten zum Zwecke des 'Trainings' der dem Betrieb der Plattform zugrunde liegenden Algorithmen" rechtfertige. Da es keine Möglichkeit gebe, das Alter der Nutzer zu überprüfen, setze die App "Minderjährige im Vergleich zu ihrem Entwicklungs- und Bewusstseinsstand absolut ungeeigneten Antworten aus", so die Behörde.

Die italienische Datenschutzbehörde zog daraufhin ihre Sperrung der ChatGPT-Anwendung unter der Bedingung zurück, dass OpenAI eine Reihe von Maßnahmen zum Schutz der Rechte und Freiheiten der italienischen Betroffenen ergreift, darunter:

- Die Bereitstellung angemessener Informationen über die Rechte, die den betroffenen Personen, sowohl Nutzern als auch Nicht-Nutzern von ChatGPT, gewährt werden, sowie von Einzelheiten über die Verarbeitung der Daten durch die Anwendung.
- Nachweis der ausdrücklichen Einwilligung der betroffenen Personen oder Angabe des berechtigten Interesses des für die Datenverarbeitung Verantwortlichen als Rechtsgrundlage für die Datenverarbeitung.
- Einführung eines Systems zur Überprüfung des Alters der Nutzer.
- Einrichtung von technischen und organisatorischen Maßnahmen zur Ausübung der Rechte der betroffenen Personen, einschließlich des Rechts auf Berichtigung, Löschung oder Widerspruch gegen die Verarbeitung ihrer personenbezogenen Daten.

Außerdem ist ChatGPT bereits in mehreren Ländern außerhalb Europas unzugänglich, darunter China, Iran, Nordkorea und Russland.

Infolge dieser schnellen Reaktionen auf diese neue Technologie müssen die DSB wachsam sein und eine Rolle bei der Überwachung und Sensibilisierung für die Risiken spielen, die diese

Technologie birgt, insbesondere die unregulierte und potenziell rücksichtslose Nutzung solcher Technologien im Hinblick auf den Schutz der personenbezogenen Daten von Personen. Zu den von den Nutzern in ChatGPT eingegebenen Daten können personenbezogene, sensible oder biometrische Daten gehören, die unter die DS-GVO fallen, während andere Arten von Daten vertrauliches oder geistiges Eigentum umfassen können, das durch Organisationsrichtlinien und/oder andere Rechtsvorschriften geregelt ist.

Eine wichtige Aufgabe des DSB in Bezug auf diese Technologie ist daher die Förderung eines sachkundigen Ansatzes bei der Konzeption, Entwicklung und Nutzung dieser Gen-AI-Systeme. Es gibt auch eine Reihe von Governance- und technischen Kontrollen, die es den DSB ermöglichen, die angemessene Nutzung von Gen-AI-Diensten innerhalb ihrer Organisation zu steuern, darunter:

- Die Richtlinien zum Datenschutz und zur Informationssicherheit müssen möglicherweise ergänzt und aktualisiert werden.
- DLP (Data Loss Prevention) und zugehörige Tools können so konfiguriert werden, dass die gemeinsame Nutzung von Daten mit Gen-AI-Diensten oder Internet-Domänen blockiert oder eingeschränkt wird.
- Sensibilisierungs- und Schulungsprogramme sind ebenfalls angebracht, da die Verbreitung von Gen-AI-Diensten und die Kanäle zu ihrer Nutzung die technischen Mittel zur Steuerung überholen werden.
- DSB mit internationaler Reichweite sollten sich auch des dynamischen rechtlichen Status von Gen-AI-Diensten in mehreren Ländern, sowohl innerhalb der EU als auch weltweit, bewusst sein.

Neben der ungewollten Weitergabe von Daten erhöht Gen-AI auch das Risiko eines ausgeklügelten Phishings zur Erlangung vertraulicher Daten, da sie die Automatisierung von E-Mails und anderen Kommunikations- und Dokumenten ermöglicht, die denen der Organisation oder von Einzelpersonen ähneln.

10. Was sind also die wichtigsten Gespräche, die ich intern führen sollte, um mich auf das Aufkommen von KI und maschinellem Lernen vorzubereiten?

In Zukunft sollten die Datenschutzbeauftragten eng mit anderen Interessengruppen in ihrem Unternehmen zusammenarbeiten, z. B. mit Datenwissenschaftlern, IT-Fachleuten, Rechtsexperten und Führungskräften, um ein KI-Champion-Netzwerk zu bilden (ähnlich wie ein Datenschutz-Champion-Netzwerk). Dieses Champion-Netzwerk wird sicherstellen, dass die Nutzung von KI-Technologien und -Systemen in der Organisation transparent,

rechenschaftspflichtig und fair ist und vor allem, dass die Nutzung von KI mit der DS-GVO konform ist.

Im Folgenden sind einige Schritte aufgeführt, die die DSB und ihr Champion-Netzwerk unternehmen können, um sich auf die Zunahme von KI-Systemen in ihrer Organisation vorzubereiten:

1. Verstehen der KI-Technologie: Die DSB sollten ein gutes Verständnis der in ihrem Unternehmen eingesetzten KI-Technologie haben. Dieses Verständnis wird durch die Zusammenarbeit mit dem Champion-Netzwerk unterstützt, um die abteilungsspezifischen KI-Technologien zu verstehen, einschließlich ihrer Funktionsweise, der Daten, die sie in jeder Abteilung sammeln und verarbeiten, und der Arten von Entscheidungen, die die KI-Systeme treffen können.
2. Spezifizieren und dokumentieren Sie eindeutig die Zwecke der Datenverarbeitung im Zusammenhang mit dem KI-System: Dies ist sowohl in der Konzeptions- und Entwicklungsphase des neuen KI-Systems besonders wichtig, um die Validierung der wichtigsten Grundsätze der DS-GVO wie Datenminimierung und Datenschutz durch Technik und Voreinstellungen zu gewährleisten, als auch bei der Einführung des KI-Systems bei den Endnutzern, insbesondere bei KI-Systemen, die Daten besonderer Kategorien wie Gesundheitsdaten verarbeiten.
3. Durchführung von Datenschutz-Folgenabschätzungen: Die Durchführung einer Datenschutz-Folgenabschätzung ist ein Prozess, der Einzelpersonen hilft, die Datenschutzrisiken eines Projekts zu ermitteln und zu minimieren. Datenschutz-Folgenabschätzungen müssen immer dann durchgeführt werden, wenn die Datenverarbeitung eines Projekts voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen gemäß Artikel 35 der DS-GVO mit sich bringt. Die DSB sollten in Zusammenarbeit mit dem Champion-Netzwerk und den verschiedenen Abteilungen der Organisation DPIAs durchführen, um die mit KI-Systemen verbundenen Risiken in jedem Bereich des Arbeitsplatzes zu bewerten und mögliche Auswirkungen auf die Privatsphäre und die Datenschutzrechte von Personen zu ermitteln. Ein wichtiger Bestandteil einer Datenschutzfolgenabschätzung für KI-Systeme ist die Überprüfung auf Verzerrungen im Algorithmus, die zu Diskriminierung führen könnten.
4. Überprüfung von Auftragsdatenverarbeitungsverträgen: Die DSB sollten alle Auftragsdatenverarbeitungsverträge mit Drittanbietern von KI überprüfen, um sicherzustellen, dass sie angemessene Garantien für die Verarbeitung personenbezogener Daten durch KI-Systeme enthalten.
5. Umsetzung geeigneter Sicherheitsmaßnahmen: Die DSB sollten sicherstellen, dass geeignete Sicherheitsmaßnahmen getroffen werden, um personenbezogene Daten bei der Nutzung von KI-Systemen vor unbefugtem Zugriff, Verlust oder Zerstörung zu schützen.

6. Überwachung und Prüfung von KI-Systemen: Die DSB sollten die KI-Systeme regelmäßig überwachen und prüfen, um sicherzustellen, dass sie wie beabsichtigt funktionieren und dass die Datenschutzrisiken wirksam gehandhabt werden.