PRAXISCHECK

KI-Angriffe & Datenschutz

Ist Ihr Sicherheitsprozess schnell genug?

Praxisleitfaden für Geschäftsführung, Datenschutz, Legal, IT, Informationssicherheit, Fachbereiche und Vendor Management

8	5	1
Kernfragen	**Prozessrisiken**	**30-Minuten-Test**

Vom Risiko zur beherrschbaren Reaktion

1	2	3	4	5
Risiko erkennen	**Identitäten schützen**	**Schnell erkennen**	**Eindämmen**	**Breach bewerten**
Bedrohungsdynamik	Konten & Tokens	Logs & Alarmierung	Zugänge & Systeme	Art. 33 / 34 DSGVO

Worum geht es?

Angriffe mit KI-Agenten verändern nicht die Grundpflichten der DSGVO. Sie können aber bekannte Angriffsschritte deutlich schneller, parallel und anpassungsfähig ausführen. Für Unternehmen wird dadurch besonders wichtig, ob Risikoanalyse, Berechtigungen, Erkennung und Reaktion mit dieser Geschwindigkeit mithalten.

Ausgangspunkt ist eine Veröffentlichung der spanischen Datenschutzbehörde AEPD vom 14.09.2026. Nach der Meldung einer betroffenen Organisation hätte ein KI-Agent mehrere Angriffsschritte autonom verkettet. Die AEPD betont zugleich, dass die Angaben noch zu analysieren sind und daraus noch kein festgestellter Datenschutzverstoß folgt.

Der Leitfaden überträgt deshalb nicht den Einzelfall, sondern das dahinterliegende Problem: Wie prüfen Sie, ob Ihre technischen und organisatorischen Maßnahmen auch bei stark beschleunigten Angriffen angemessen und wirksam bleiben?

Die wichtigste Erkenntnis

Art. 32 DSGVO verlangt keine statische Sicherheitsliste. Wenn sich Geschwindigkeit, Reichweite oder Anpassungsfähigkeit von Angriffen verändern, muss auch geprüft werden, ob bestehende Schutzmaßnahmen weiterhin zum Risiko passen.

Warum Geschwindigkeit zum Datenschutzthema wird

Der Ausgangsfall ist noch keine abgeschlossene Behördenentscheidung. Er zeigt aber, warum klassische Sicherheitsprozesse bei automatisierten Angriffen zu langsam werden können.

14.09.2026

AEPD veröffentlicht erste gemeldete Datenschutzverletzung mit mutmaßlich agentischem KI-Angriff

Analyse noch offen

Der Ausgangspunkt

Behörde: Agencia Española de Protección de Datos (AEPD)
Datum: 14.09.2026
Aktenzeichen: nicht ersichtlich
Problem: gemeldete Breach, bei der ein KI-Agent Angriffsschritte verkettet haben soll
Status: Angaben der meldenden Organisation, behördliche Analyse noch ausstehend
Sanktion: keine ersichtlich

Die fünf Rechtsanker

Rechtsgrundlage	Was bedeutet das praktisch?
Art. 5 Abs. 1 lit. f) DSGVO	Personenbezogene Daten müssen angemessen gegen unbefugten Zugriff, Veränderung, Verlust oder Zerstörung geschützt werden. Praktisch bedeutet das: Sicherheit ist Teil der Datenschutzgrundsätze.
Art. 24 Abs. 1 DSGVO	Der Verantwortliche muss geeignete Maßnahmen umsetzen und erforderlichenfalls überprüfen und aktualisieren. Sicherheitskonzepte dürfen deshalb nicht veralten.
Art. 32 Abs. 1 DSGVO	Das Sicherheitsniveau muss zum konkreten Risiko passen. Zu berücksichtigen sind u. a. Stand der Technik, Kosten, Verarbeitungskontext sowie Wahrscheinlichkeit und Schwere möglicher Folgen.
Art. 32 Abs. 1 lit. d) DSGVO	Die Wirksamkeit der technischen und organisatorischen Maßnahmen muss regelmäßig überprüft, bewertet und evaluiert werden.
Art. 33 / 34 DSGVO	Bei einer Datenschutzverletzung sind Risiko, Meldepflicht an die Aufsicht und gegebenenfalls die Information der Betroffenen zeitnah zu prüfen. Auftragsverarbeiter müssen nach Art. 33 Abs. 2 DSGVO unverzüglich informieren.

Fünf typische Prozessrisiken

Prozessrisiko	Typisches Problem
1 Risikoanalyse bleibt zu grob	„Phishing“, „Malware“ oder „unbefugter Zugriff“ werden erfasst, aber Geschwindigkeit, Parallelität und Reichweite automatisierter Angriffe nicht bewertet.
2 Identitäten sind überprivilegiert	Admin-Konten, Service-Konten, API-Schlüssel oder Tokens besitzen mehr Rechte oder eine längere Gültigkeit als notwendig.
3 Erkennung ist zu langsam	Ungewöhnliche Zugriffe werden zwar protokolliert, aber erst Stunden oder Tage später ausgewertet.
4 Eindämmung hängt nur von Menschen ab	Konten, Tokens oder Sitzungen lassen sich nicht schnell genug sperren oder widerrufen.
5 Dienstleister melden zu spät	Vertrag und Praxis klären nicht, wie ein Auftragsverarbeiter einen Vorfall unverzüglich eskaliert und welche Informationen er liefert.

Der Selbsttest: Risikoanalyse und kritische Assets

Markieren Sie jede Frage mit Ja, Nein oder Unklar. Entscheidend ist nicht nur die Richtlinie, sondern ob die Umsetzung im Alltag nachvollziehbar funktioniert.

1

Berücksichtigt unsere Risikoanalyse ausdrücklich, dass Angriffe automatisiert, parallel und sehr schnell ablaufen können?

☐ ja ☐ nein ☐ unklar

Warum wichtig: Art. 32 DSGVO verlangt eine risikoorientierte Betrachtung. Automatisierung kann Eintrittswahrscheinlichkeit, Reichweite und Reaktionszeit verändern, auch wenn die Angriffsmethode bekannt ist.

Gute Umsetzung: Kritische Verarbeitungen enthalten konkrete Szenarien zu automatisierter Schwachstellensuche, parallelen Zugriffsversuchen und schneller Ausnutzung erlangter Rechte.

Prüfnachweis: Risikoanalyse oder TOM-Review, Bedrohungsszenarien, Review-Datum, Verantwortlicher, dokumentierte Anpassungsentscheidung.

Typisches Warnsignal: Die Risikoanalyse nennt nur Sammelbegriffe wie „Cyberangriff“, ohne Geschwindigkeit oder systemübergreifende Wirkung zu betrachten.

Praxismaßnahme: Bei der nächsten Sicherheits- oder Datenschutzprüfung mindestens ein agentisches Angriffsszenario für kritische Verarbeitungen ergänzen.

2

Können wir die Systeme, Datenbestände und Zugänge benennen, deren Kompromittierung besonders weitreichende Folgen hätte?

☐ ja ☐ nein ☐ unklar

Warum wichtig: Schnelle Angriffe werden besonders problematisch, wenn ein einzelner Zugang viele Systeme oder sensible Daten erreicht. Priorisierung setzt Transparenz über kritische Assets voraus.

Gute Umsetzung: Für zentrale Verarbeitungen sind Systemowner, Datenkategorien, privilegierte Konten, Schnittstellen und externe Zugänge bekannt und aktuell dokumentiert.

Prüfnachweis: Verzeichnis von Verarbeitungstätigkeiten, Systemlandkarte, Datenfluss, Asset-Liste, Liste privilegierter Konten und Schnittstellen.

Typisches Warnsignal: Im Ernstfall beginnt erst die Suche nach der Frage, welche Systeme ein kompromittiertes Konto überhaupt erreichen kann.

Praxismaßnahme: Für drei besonders kritische Verarbeitungen eine kompakte System-, Daten- und Zugangskarte erstellen und jährlich sowie anlassbezogen aktualisieren.

Zwischenstand

Wenn Sie bei einer der beiden Fragen „Nein“ oder „Unklar“ markieren, fehlt die Grundlage für eine belastbare Priorisierung. Stabilisieren Sie zuerst Risikosicht und Systemtransparenz.

Der Selbsttest: Identitäten und Berechtigungen

Bei automatisierten Angriffen entscheidet häufig nicht nur die Schwachstelle, sondern wie weit ein erlangter Zugang trägt und wie lange er nutzbar bleibt.

3

Sind Benutzer-, Admin-, Service-Konten, API-Schlüssel und Tokens nach dem Prinzip der geringsten Rechte ausgestaltet?

☐ ja ☐ nein ☐ unklar

Warum wichtig: Ein kompromittierter Zugang mit zu vielen Rechten kann in kurzer Zeit viele Systeme oder Datenbestände erschließen. Begrenzte Rechte reduzieren die Reichweite eines Vorfalls.

Gute Umsetzung: Rollen sind aufgabenbezogen, privilegierte Rechte zeitlich oder technisch begrenzt und Service-Konten haben nur die für ihre Funktion benötigten Berechtigungen.

Prüfnachweis: Berechtigungskonzept, Rollenmatrix, Access-Reviews, Liste privilegierter und technischer Konten, Freigabeprotokolle.

Typisches Warnsignal: Ein dauerhaft genutztes Administratorkonto oder API-Token funktioniert in mehreren Systemen mit weitreichenden Rechten.

Praxismaßnahme: Privilegierte und technische Konten priorisiert überprüfen und nicht benötigte Rechte, Alt-Konten und unnötige Schnittstellenberechtigungen entfernen.

4

Können kompromittierte Zugangsmittel schnell erkannt, widerrufen und ersetzt werden?

☐ ja ☐ nein ☐ unklar

Warum wichtig: Bei hoher Angriffsgeschwindigkeit ist die Restlaufzeit eines kompromittierten Tokens oder einer Sitzung entscheidend. Sperrung und Rotation müssen praktisch funktionieren.

Gute Umsetzung: Mehrfaktor-Authentifizierung ist risikoorientiert eingesetzt, Tokens sind angemessen befristet, Sitzungen zentral widerrufbar und kritische Schlüssel können kurzfristig rotiert werden.

Prüfnachweis: MFA-Konfiguration, Token-Policy, Key-Inventory, Sperr- und Rotationsverfahren, Notfallkontakte, Testprotokolle.

Typisches Warnsignal: Niemand weiß, wie ein kompromittierter API-Schlüssel am Wochenende gesperrt wird, oder die Änderung würde mehrere Systeme ungeplant stoppen.

Praxismaßnahme: Für kritische Konten und Tokens einen dokumentierten „Sperren und Rotieren“-Ablauf mit Stellvertretung testen.

Praxisregel

Ein kompromittierter Zugang darf nicht automatisch zu einem kompromittierten Unternehmen werden. Begrenzen Sie Reichweite, Laufzeit und Wiederverwendung von Identitäten und Zugangsmitteln.

Der Selbsttest: Erkennung und Eindämmung

Je stärker Angriffe automatisiert werden, desto weniger darf die Abwehr ausschließlich von manueller Sichtung und langen Freigabeketten abhängen.

5

Erkennen wir ungewöhnliche Aktivitäten schnell genug, um auf maschinelle Angriffsgeschwindigkeit zu reagieren?

☐ ja ☐ nein ☐ unklar

Warum wichtig: Art. 32 DSGVO verlangt ein angemessenes Sicherheitsniveau. Logs helfen nur, wenn relevante Auffälligkeiten rechtzeitig erkannt und bewertet werden.

Gute Umsetzung: Kritische Konten und Systeme haben priorisierte Alarmierungen, sinnvolle Schwellenwerte und klare Eskalationen. Ungewöhnliche Login-, Rechte- oder Datenzugriffsmuster werden zeitnah sichtbar.

Prüfnachweis: Logging-Konzept, Alarmregeln, SIEM/SOC-Konfiguration, Eskalationsmatrix, Alarmtests, dokumentierte Reaktionszeiten.

Typisches Warnsignal: Auffälligkeiten sind im Log vorhanden, werden aber nur im Monatsreport oder nach einem Hinweis von außen entdeckt.

Praxismaßnahme: Für privilegierte Konten und sensible Systeme drei bis fünf wirklich relevante Alarme definieren und deren Zustellung praktisch testen.

6

Können wir einen verdächtigen Zugriff innerhalb kurzer Zeit begrenzen, ohne erst lange Zuständigkeiten zu klären?

☐ ja ☐ nein ☐ unklar

Warum wichtig: Erkennung ohne schnelle Eindämmung schützt nicht ausreichend. Bei parallelen Zugriffen kann organisatorische Verzögerung den möglichen Schaden vergrößern.

Gute Umsetzung: Es ist geklärt, wer Konten sperrt, Tokens widerruft, Systeme isoliert oder Zugriffe drosselt. Kritische Schritte sind vorbereitet und benötigen keine unnötig langen Freigabeketten.

Prüfnachweis: Notfallplan, Runbooks, Berechtigungen für Sofortmaßnahmen, Stellvertretung, dokumentierte Übungen und Lessons Learned.

Typisches Warnsignal: Die IT erkennt einen Vorfall, darf aber ohne mehrere Freigaben kein Konto sperren oder eine externe Verbindung trennen.

Praxismaßnahme: Für die wichtigsten Eindämmungsmaßnahmen eine abgestufte Notfallbefugnis mit klaren Grenzen und Nachkontrolle festlegen.

Praxisregel

Menschliche Kontrolle bleibt wichtig. Sie sollte aber durch Erkennungs- und Eindämmungsmechanismen unterstützt werden, die nicht erst nach menschlicher Sichtung jedes einzelnen Schritts reagieren können.

Der Selbsttest: Breach-Prozess und Dienstleister

Sobald personenbezogene Daten betroffen sein könnten, müssen technische Reaktion und datenschutzrechtliche Bewertung zusammenlaufen.

7

Ist unser Prozess für Datenschutzverletzungen direkt mit dem technischen Sicherheitsvorfall verknüpft?

☐ ja ☐ nein ☐ unklar

Warum wichtig: Art. 33 DSGVO verlangt eine unverzügliche Bewertung und bei meldepflichtigen Verletzungen eine Meldung binnen 72 Stunden nach Bekanntwerden. Art. 34 DSGVO kann bei hohem Risiko zusätzlich die Information der Betroffenen verlangen.

Gute Umsetzung: IT und Informationssicherheit eskalieren mögliche Datenschutzverletzungen sofort an die zuständige Stelle. Risikoentscheidung, Friststart, betroffene Daten und weitere Schritte werden nachvollziehbar dokumentiert.

Prüfnachweis: Breach-Register, Eskalationsweg, 72-Stunden-Check, Risikobewertung, Kommunikationsvorlagen, Entscheidungs- und Versandnachweise.

Typisches Warnsignal: Der technische Vorfall wird vollständig bearbeitet, bevor Datenschutz oder Legal überhaupt von möglichen personenbezogenen Daten erfahren.

Praxismaßnahme: Für Sicherheitsvorfälle mit möglichem Personenbezug einen festen Datenschutz-Trigger und eine sofortige Übergabe an den Breach-Prozess definieren.

8

Sind Auftragsverarbeiter und kritische Dienstleister in Meldung, Aufklärung und Eindämmung praktisch eingebunden?

☐ ja ☐ nein ☐ unklar

Warum wichtig: Nach Art. 33 Abs. 2 DSGVO muss ein Auftragsverarbeiter den Verantwortlichen nach Bekanntwerden einer Datenschutzverletzung unverzüglich informieren. Der Verantwortliche benötigt zudem schnell belastbare Fakten für seine eigene Bewertung.

Gute Umsetzung: Verträge und Betriebsabläufe nennen erreichbare Kontakte, Eskalationsweg, erwartete Mindestinformationen und Unterstützung bei Logs, Eindämmung und Ursachenklärung.

Prüfnachweis: AV-Vertrag, Incident-Klausel, Notfallkontakte, SLA/OLA, Übungsprotokoll, Lieferantenbewertung, Lösch- und Log-Nachweise.

Typisches Warnsignal: Im Vertrag steht nur „unverzüglich“, aber niemand kennt die zuständige Rufnummer oder weiß, welche technischen Informationen der Dienstleister liefern kann.

Praxismaßnahme: Für kritische Auftragsverarbeiter einmal jährlich den Incident-Kontakt und die Informationskette testen.

Schnelle Selbstauswertung

Orientierung	Einordnung
7–8 × Ja	Gute Ausgangslage. Prüfen Sie trotzdem regelmäßig Risikoanalyse, Berechtigungen, Erkennungszeiten und Breach-Prozess mit realistischen Tests.
4–6 × Ja	Mehrere Lücken sind möglich. Priorisieren Sie privilegierte Zugänge, schnelle Eindämmung und die Verzahnung von IT- und Datenschutzprozessen.
0–3 × Ja	Der Prozess sollte zeitnah grundlegend geprüft und verbindlich geordnet werden. Beginnen Sie mit kritischen Verarbeitungen und Zugängen.

Wichtig

Die Selbstauswertung ist nur eine praktische Orientierung und keine rechtliche Bewertung. Ein einzelner kritischer Fehler kann bereits erheblich sein.

Wer sollte sich darum kümmern?

KI-gestützte Angriffsszenarien sind ein bereichsübergreifendes Thema. Klare Rollen verhindern, dass technische Reaktion, Datenschutzbewertung und Dienstleistersteuerung auseinanderfallen.

Bereich	Kernaufgabe	Typischer Nachweis
Geschäftsführung / Prozessowner	Prioritäten, Ressourcen, Risikobereitschaft, Eskalation und Gesamtverantwortung festlegen.	Beschlüsse, Risikofreigaben, Eskalationsmatrix
IT / Informationssicherheit	Identitäten schützen, Schwachstellen bearbeiten, Erkennung betreiben und technische Eindämmung durchführen.	Systemliste, IAM-Konzept, Logs, Runbooks, Testprotokolle
Datenschutz / Legal	Datenschutzrisiken, Art. 32, Breach-Bewertung nach Art. 33/34 und Dokumentation rechtlich einordnen.	Prüfschema, Breach-Register, Rechtsvermerk, Vorlagen
Fachbereich / Systemowner	Kritische Daten und Funktionen kennen, fachlichen Kontext liefern und Maßnahmen praktisch umsetzen.	Asset-Owner, Verfahrensbeschreibung, Berechtigungsfreigaben
Vendor Management / Einkauf	Kritische Dienstleister, Incident-Pflichten und Eskalationswege vertraglich und praktisch absichern.	AV-Vertrag, SLA, Notfallkontakt, Kontrollnachweis
Datenschutzbeauftragter	Beraten, überwachen, sensibilisieren und bei Kontrollen oder Beschwerden unterstützen.	Beratungsvermerk, Auditbericht, Schulung

Vier Signale, die intern sofort eskaliert werden sollten

Typische Beobachtung	Was daraus folgen sollte
„Ein privilegiertes Konto meldet sich ungewöhnlich schnell an mehreren Systemen an.“	Identität prüfen, Zugriff begrenzen, Logs sichern und mögliche Datenbetroffenheit bewerten.
„Ein API-Schlüssel wird außerhalb des vorgesehenen Dienstes verwendet.“	Token widerrufen oder rotieren, Reichweite feststellen und abhängige Systeme prüfen.
„Ein Dienstleister meldet ungewöhnlichen Zugriff auf Kundendaten.“	Technische Fakten anfordern, Fristbeginn dokumentieren und Art. 33/34 DSGVO prüfen.
„Personenbezogene Daten wurden unerwartet verändert oder massenhaft abgerufen.“	Vorfall eindämmen, Datenumfang klären, Risiken für Betroffene bewerten und Nachweise sichern.

Praxisregel

Benennen Sie einen Gesamtverantwortlichen für den Prozess. Er muss nicht jede technische oder rechtliche Aufgabe selbst erledigen, aber sicherstellen, dass Risiken, Zugänge, Reaktion, Meldung und Dienstleister zusammengeführt werden.

Der 30-Minuten-Praxistest

Prüfen Sie nicht durch einen echten Angriff, sondern mit einem kontrollierten Tabletop-Test, ob Erkennung, Eindämmung und Datenschutzbewertung praktisch zusammenspielen.

1	☐ **Szenario wählen**	Nehmen Sie ein kritisches System mit personenbezogenen Daten, z. B. CRM, HR- oder Kundenportal. Verwenden Sie ausschließlich Testkonten und Testdaten.
2	☐ **Testalarm auslösen**	Erzeugen Sie eine harmlose, vorab abgestimmte Auffälligkeit, z. B. einen Testlogin oder einen definierten SIEM-Testevent.
3	☐ **Zeit stoppen**	Dokumentieren Sie, wann der Alarm sichtbar wird, wer ihn erhält und wann die erste qualifizierte Bewertung erfolgt.
4	☐ **Eindämmung simulieren**	Prüfen Sie, ob Testkonto, Sitzung oder Testtoken schnell gesperrt bzw. widerrufen werden kann und wer dazu befugt ist.
5	☐ **Datenbezug prüfen**	Simulieren Sie die Frage: Welche personenbezogenen Daten und Personen könnten bei einem vergleichbaren echten Vorfall betroffen sein?
6	☐ **Breach-Prozess starten**	Prüfen Sie, ob Fristst art, Risikobewertung und Zuständigkeit nach Art. 33/34 DSGVO ohne Umwege ausgelöst werden.
7	☐ **Dienstleister einbeziehen**	Falls relevant: Testen Sie, ob der Incident-Kontakt des Dienstleisters erreichbar und die erwartete Informationskette klar ist.
8	☐ **Abweichungen festhalten**	Dokumentieren Sie Zeitverluste, unklare Rechte, fehlende Logs, nicht erreichbare Ansprechpartner und konkrete Maßnahmen.

Welche Nachweise sollten auffindbar sein?

Bereich	Beispiele
Erkennung	Alarmzeitpunkt, betroffene Quelle, Empfänger, Bewertung und Reaktionszeit.
Identität / Zugriff	Konten, Tokens, Rollen, Sperr- oder Widerrufsmöglichkeit, Verantwortlicher.
Datenschutzbewertung	Betroffene Daten, Personen, mögliche Folgen, Art. 33/34-Entscheidung, Fristst art.
Dienstleister	Notfallkontakt, Meldungszeit, technische Fakten, gemeinsame Maßnahmen.
Kontrolle	Abweichungen, Verbesserungsmaßnahmen, Verantwortliche, Frist und Abschlussnachweis.

Ihr Maßnahmenplan

Nutzen Sie diese Seite als interne Arbeitsvorlage. Nicht jede Maßnahme ist in jedem Unternehmen zwingend erforderlich. Priorisieren Sie nach Risiko und tatsächlicher Systemlandschaft.

Maßnahme	Verantwortlich	Priorität	Frist	Status	Nachweis
				☐ erledigt	
				☐ erledigt	
				☐ erledigt	
				☐ erledigt	
				☐ erledigt	
				☐ erledigt	
				☐ erledigt	

Drei Prioritäten, wenn Sie heute anfangen

Zwingend prüfen	Ob kritische Verarbeitungen ein angemessenes Sicherheitsniveau nach Art. 32 DSGVO haben, privilegierte Zugänge beherrscht werden und ein funktionsfähiger Prozess für Datenschutzverletzungen besteht.
Empfohlen	Risikoanalyse ausdrücklich um Geschwindigkeit, Parallelität und Reichweite automatisierter Angriffe ergänzen und Reaktionszeiten mit kontrollierten Tests messen.
Zusätzliche Absicherung	Für besonders kritische Systeme kurze Token-Laufzeiten, stärkere Anomalieerkennung, automatisierte Eindämmungsoptionen und regelmäßige Tabletop-Übungen etablieren.

Merksatz

Ein Sicherheitsprozess ist nicht dann gut, wenn er viele Kontrollen auflistet. Er ist gut, wenn das Unternehmen Risiken nachvollziehbar priorisieren, verdächtige Zugriffe schnell erkennen, wirksam eindämmen und eine mögliche Datenschutzverletzung rechtzeitig bewerten kann.

Rechtsgrundlagen, Quellen und Hinweise

Die drei wichtigsten Punkte

1	Angemessenheit ist dynamisch. Verändert sich die Bedrohungsdynamik, muss geprüft werden, ob Schutzmaßnahmen nach Art. 32 DSGVO noch zum Risiko passen.
2	Identitäten und Reaktionszeit sind Schlüsselfaktoren. Begrenzte Rechte, schnelle Erkennung und praktikable Eindämmung reduzieren die Reichweite eines Vorfalls.
3	Technische Reaktion und Datenschutzbewertung gehören zusammen. Sobald personenbezogene Daten betroffen sein könnten, müssen Art. 33 und gegebenenfalls Art. 34 DSGVO früh in den Ablauf integriert werden.

Rechtsgrundlagen

Art. 5 Abs. 1 lit. f) DSGVO: Integrität und Vertraulichkeit: angemessener Schutz vor unbefugter oder unrechtmäßiger Verarbeitung sowie vor Verlust, Zerstörung oder Schädigung.
Art. 24 Abs. 1 DSGVO: Verantwortung des Unternehmens: geeignete Maßnahmen umsetzen und erforderlichenfalls überprüfen und aktualisieren.
Art. 32 DSGVO: Sicherheit der Verarbeitung: risikoorientiertes Schutzniveau und regelmäßige Überprüfung der Wirksamkeit technischer und organisatorischer Maßnahmen.
Art. 33 DSGVO: Meldung von Datenschutzverletzungen an die Aufsichtsbehörde; Art. 33 Abs. 2 DSGVO verpflichtet Auftragsverarbeiter zur unverzüglichen Information des Verantwortlichen.
Art. 34 DSGVO: Benachrichtigung betroffener Personen, wenn die Datenschutzverletzung voraussichtlich ein hohes Risiko für ihre Rechte und Freiheiten zur Folge hat.

Kurzes Glossar

Begriff	Einfach erklärt
KI-Agent	Ein System, das auf ein Ziel hinarbeiten, Zwischenschritte planen, Werkzeuge nutzen und sein Vorgehen anhand von Ergebnissen anpassen kann.
Datenschutzverletzung	Eine Sicherheitsverletzung, die zur Vernichtung, zum Verlust, zur Veränderung, zur unbefugten Offenlegung oder zum unbefugten Zugang zu personenbezogenen Daten führt.
TOM	Technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten, etwa Zugriffsschutz, Protokollierung, Datensicherung und Sicherheitsprozesse.
Token / API-Schlüssel	Technische Zugangsmittel für Anwendungen oder Dienste. Werden sie kompromittiert, können Funktionen ohne normalen Benutzerlogin nutzbar sein.
Least Privilege	Prinzip der geringsten Rechte: Benutzer und technische Konten erhalten nur die Berechtigungen, die für ihre Aufgabe tatsächlich erforderlich sind.

Quellen

Primärquelle: AEPD, Francisco Pérez Bes, „Primera notificación de una brecha de datos personales causada por un ataque ejecutado mediante un agente de IA“, 14.09.2026. Quelle öffnen
Rechtsgrundlage: Verordnung (EU) 2016/679 (DSGVO), insbesondere Art. 5, 24, 32, 33, 34 und 35. EUR-Lex öffnen

Hinweis

Dieses Dokument dient der allgemeinen Information und als praktische Arbeitshilfe. Es ersetzt keine Prüfung des konkreten Einzelfalls. Welche technischen und organisatorischen Maßnahmen erforderlich und angemessen sind, hängt von der jeweiligen Datenverarbeitung, der aktuellen Risikolage, den eingesetzten Systemen und Technologien sowie den konkreten Umständen des Unternehmens ab.