Firmato digitalmente da: Michael Simonini
Data: 27/10/2026 11:05:17

14.1 KI (AI)-POLICY

Stand/Aggiornata al: 04.10.2026

Versione in lingua italiana a partire da pagina 17.

INHALTSVERZEICHNIS

1. Zweck, Zielsetzung und Geltungsbereich
1.1 Hintergrund und rechtliche Ausgangslage
1.2 Zielsetzung der Shadow-AI-Governance
1.3 Geltungsbereich (Mitarbeitende, Führungskräfte, Externe)
1.4 Rechtsgrundlagen (DSGVO, AI Act, Garante Privacy, ACN)
2. Begriffsbestimmungen
2.1 Generative KI
2.2 Shadow AI
2.3 KI-Tool
2.4 Personenbezogene Daten
2.5 Hochrisiko-KI gemäß AI Act
3. Governance-Struktur und Verantwortlichkeiten
3.1 KI-Beauftragte/r
3.2 Datenschutzbeauftragte/r (DPO)
3.3 IT-Sicherheitsverantwortliche/r
3.4 Geschäftsleitung
3.5 Mitarbeitende
3.6 Externe Dienstleister
4. KI-Policy
4.1 Grundprinzipien
4.2 Zulässige KI-Nutzung
4.3 Verbotstatbestände
4.4 Anforderungen an Transparenz und Dokumentation
4.5 Umgang mit personenbezogenen und vertraulichen Daten
4.6 Nutzung privater KI-Accounts
4.7 Kennzeichnung KI-unterstützter Inhalte
5. Freigabeprozess für KI-Tools
5.1 Antragstellung
5.2 Prüfung durch KI-Beauftragte/n
5.3 Datenschutzrechtliche Prüfung (DPO)
5.4 Technische Sicherheitsprüfung (IT)
5.5 Entscheidung (Freigabe, Freigabe mit Auflagen, Ablehnung)
5.6 Dokumentation im KI-Register
5.7 Widerruf der Freigabe
6. Handlungsregeln für Mitarbeitende
6.1 Do-Regeln
6.2 Don’t-Regeln
6.3 Umgang mit Fehlern und Halluzinationen
6.4 Meldepflicht bei Shadow-AI-Vorfällen
6.5 Nutzung von KI-Ergebnissen in offiziellen Dokumenten
7. DSGVO-Konformität beim KI-Einsatz
7.1 Datenminimierung und Zweckbindung

7.2 Privacy by Design & Default
7.3 Sicherheit der Verarbeitung (Art. 32 DSGVO)
7.4 Drittlandübermittlungen
7.5 Datenschutz-Folgenabschätzung (DSFA) für KI-Systeme
7.6 Dokumentationspflichten gegenüber Garante Privacy
8. AI-Act-Konformität
8.1 Risikoklassifizierung der eingesetzten KI-Systeme
8.2 Pflichten für Hochrisiko-KI
8.3 Transparenzpflichten
8.4 Anforderungen an menschliche Aufsicht
8.5 Verbotene KI-Praktiken
8.6 Konformitätsbewertung und Nachweisführung
9. Risikoorientiertes Kontrollsystem
9.1 Kontrollplan
9.2 Shadow-AI-Detektion (Monitoring, Logfiles, Netzwerk)
9.3 Prüfung der Freigabeliste
9.4 Interne Kontrollen
9.5 Externe Kontrollen (Revision, Behörden)
9.6 Eskalationswege bei Verstößen
10. Dokumentation und Registerführung
10.1 KI-Register
10.2 Freigabeliste
10.3 Auditberichte
10.4 Schulungsnachweise
10.5 Shadow-AI-Melderegister 10.6 Aufbewahrungsfristen
11. Schulung und Sensibilisierung
11.1 Schulungskonzept
11.2 Pflichtschulungen
11.3 Awareness-Materialien
11.4 Dokumentation der Teilnahme
11.5 Wiederholungsschulungen
12. Sanktionen und Maßnahmen bei Verstößen
12.1 Interne Sanktionen
12.2 Einschränkung von Zugriffsrechten
12.3 Disziplinarmaßnahmen
12.4 Meldung an Geschäftsleitung
12.5 Externe Sanktionen (Garante Privacy, AI Act, ACN)
13. Inkrafttreten und Aktualisierung
13.1 Inkrafttreten
13.2 Jährliche Überprüfung
13.3 Anpassung an neue gesetzliche Vorgaben
13.4 Verantwortlichkeit für Aktualisierungen

1. Zweck, Zielsetzung und Geltungsbereich

1.1 Hintergrund und rechtliche Ausgangslage

(1) Der Verantwortliche erkennt die tiefgreifenden Veränderungen, die durch den Einsatz generativer Systeme der Künstlichen Intelligenz (KI/AI) in sämtlichen gesellschaftlichen, administrativen und organisatorischen Bereichen entstehen. Diese Systeme, die in der Lage sind, Inhalte autonom zu erzeugen, Entscheidungen

vorzubereiten oder komplexe Datenverarbeitungsprozesse zu unterstützen, stellen eine technologische Entwicklung dar, die sowohl Chancen als auch erhebliche Risiken birgt. (2) Die rechtliche Ausgangslage ist durch eine Vielzahl unionsrechtlicher und nationaler Normen geprägt, die den Einsatz von KI-Systemen regulieren. Hierzu zählen insbesondere die Datenschutz-Grundverordnung (DSGVO), die Verordnung über Künstliche Intelligenz (AI Act), die Leitlinien und Entscheidungen der Garante per la Protezione dei Dati Personali sowie die Vorgaben der Agenzia per la Cybersicurezza Nazionale (ACN). (3) Der Verantowrtliche erkennt an, dass die unkontrollierte Nutzung von KI-Systemen („Shadow AI“) zu erheblichen Risiken führen kann, darunter Datenschutzverletzungen, Informationssicherheitsvorfälle, Fehlentscheidungen, Haftungsrisiken, Reputationsschäden und operative Störungen. (4) Vor diesem Hintergrund ist der Verantwortliche verpflichtet, ein umfassendes internes Regelwerk zu schaffen, das die Nutzung generativer KI-Systeme regelt, kontrolliert, dokumentiert und auditierbar macht.

1.2 Zielsetzung der Shadow-AI-Governance

(1) Ziel dieses Regelwerks ist die Errichtung eines umfassenden, kohärenten und rechtskonformen Governance-Rahmens, der die sichere, transparente und verantwortungsvolle Nutzung generativer KI-Systeme innerhalb der Struktur des Veranwortlichen gewährleistet. (2) Die Shadow-AI-Governance verfolgt insbesondere folgende Ziele: a) Prävention nicht autorisierter KI-Nutzung; b) Sicherstellung der Einhaltung aller relevanten gesetzlichen Vorgaben; c) Schutz personenbezogener und vertraulicher Daten; d) Minimierung institutioneller, operativer und rechtlicher Risiken; e) Förderung einer verantwortungsvollen KI-Kultur; f) Aufbau eines dokumentierten, kontrollierten und auditierbaren KI-Ökosystems. (3) Die Governance dient der Schaffung eines normativen Rahmens, der sowohl präventive als auch reaktive Maßnahmen umfasst.

1.3 Geltungsbereich (Mitarbeitende, Führungskräfte, Externe)

(1) Dieses Regelwerk gilt für sämtliche Mitarbeitenden, Führungskräfte, Praktikanten, Ehrenamtliche, externe Dienstleister, Kooperationspartner und sonstige Personen, die im Rahmen ihrer Tätigkeit Zugang zu Informationssystemen des Verantwortlichen haben. (2) Die Bestimmungen gelten unabhängig von Beschäftigungsform, Hierarchieebene oder technischer Qualifikation. (3) Externe Dienstleister sind verpflichtet, die Bestimmungen dieses Regelwerks vertraglich anzuerkennen und einzuhalten.

1.4 Rechtsgrundlagen (DSGVO, AI Act, Garante Privacy, ACN)

(1) Dieses Regelwerk basiert auf folgenden Rechtsquellen, die in ihrer Gesamtheit den normativen Rahmen für die Nutzung generativer KI-Systeme bilden: a) Verordnung (EU) 2016/679 (DSGVO), insbesondere die Grundsätze der Datenminimierung, Zweckbindung, Transparenz, Sicherheit der Verarbeitung, Datenschutz-Folgenabschätzung und Drittlandübermittlungen; b) Verordnung (EU) 2024/… (AI Act), insbesondere die Bestimmungen zu Risikoklassifizierung, Pflichten für Hochrisiko-KI, Transparenzpflichten, menschlicher Aufsicht, Verbotstatbeständen und Konformitätsbewertung; c) Leitlinien, Entscheidungen und Stellungnahmen der Garante Privacy, insbesondere jene zur Nutzung von KI-Systemen, zu Datenschutzrisiken, zu Transparenzanforderungen und zu organisatorischen Pflichten; d) Vorgaben der Agenzia per la Cybersicurezza Nazionale (ACN), insbesondere jene zur Cybersicherheit, zur Risikoanalyse, zu technischen Schutzmaßnahmen und zur Überwachung digitaler Systeme; e) D.Lgs. 196/2003 (Codice Privacy), insbesondere die Bestimmungen zur Verarbeitung personenbezogener Daten durch öffentliche und private Einrichtungen; f) Nationale und regionale Vorgaben zur KI-Nutzung, soweit sie für den Verantwortlichen relevant sind. (2) Der Veranwortliche verpflichtet sich zur fortlaufenden Überwachung gesetzlicher Entwicklungen und zur Anpassung dieses Regelwerks an neue rechtliche Anforderungen. (3) Die Rechtsgrundlagen sind integraler Bestandteil dieses Regelwerks und bilden die normative Grundlage für alle nachfolgenden Bestimmungen.

2. Begriffsbestimmungen

2.1 Generative KI

Systeme, die mittels algorithmischer Modelle Inhalte erzeugen, darunter Texte, Bilder, Audio, Video, Code oder sonstige digitale Artefakte.

2.2 Shadow AI

Jede Nutzung eines KI-Systems ohne vorherige Genehmigung, Registrierung oder Kontrolle durch den Verantwortlichen

2.3 KI-Tool

Software, Plattform oder API, die KI-Funktionen bereitstellt.

2.4 Personenbezogene Daten

Informationen gemäß Art. 4 DSGVO.

2.5 Hochrisiko-KI gemäß AI Act

KI-Systeme, die gemäß Kapitel II des AI Act besonderen regulatorischen Anforderungen unterliegen.

3. Governance-Struktur und Verantwortlichkeiten

3.1 KI-Beauftragte/r

(1) Der Verantwortliche bestellt eine/n KI-Beauftragte/n, der/die als zentrale normative, organisatorische, strategische und operative Instanz für sämtliche Fragen der Nutzung, Kontrolle, Bewertung und Weiterentwicklung generativer KI-Systeme fungiert. (2) Der/die KI-Beauftragte ist mit umfassenden Befugnissen ausgestattet, die sowohl präventive als auch reaktive Maßnahmen umfassen. (3) Zu den Aufgaben gehören insbesondere: a) die Prüfung, Bewertung und Genehmigung von KI-Tools unter Berücksichtigung rechtlicher, technischer, organisatorischer und ethischer Kriterien; b) die Führung des KI-Registers, das sämtliche KI-Nutzungen, Freigaben, Widerrufe, Vorfälle und Prüfungen dokumentiert; c) die Durchführung von Risikoanalysen gemäß DSGVO, AI Act, Garante Privacy und ACN-Vorgaben; d) die Erstellung jährlicher Berichte an die Geschäftsleitung, die den Stand der KI-Governance, die identifizierten Risiken, die durchgeführten Maßnahmen und die geplanten Weiterentwicklungen enthalten; e) die Koordination mit dem Datenschutzbeauftragten, der EDV Verantwortlichen und externen Partnern; f) die Überwachung der Einhaltung dieses Regelwerks durch alle Mitarbeitenden und externen Dienstleister; g) die Initiierung von Maßnahmen bei Verstößen, einschließlich Schulungen, Einschränkungen von Zugriffsrechten, Widerruf von Freigaben und Eskalation an die Geschäftsleitung; h) die Sicherstellung der Konformität mit allen relevanten gesetzlichen Vorgaben und behördlichen Anforderungen; i) die Beratung der Geschäftsleitung in strategischen Fragen der KI-Nutzung; j) die kontinuierliche Weiterentwicklung der KI-Governance unter Berücksichtigung technologischer Entwicklungen und rechtlicher Änderungen. (4) Der/die KI-Beauftragte ist befugt, Freigaben zu widerrufen, Nutzungen zu untersagen, Maßnahmen zur Risikominimierung anzuordnen und Shadow-AI-Vorfälle zu untersuchen. (5) Der/die KI-Beauftragte ist verpflichtet, alle Entscheidungen nachvollziehbar zu dokumentieren.

3.2 Datenschutzbeauftragte/r (DPO)

(1) Der/die DPO überwacht die Einhaltung der DSGVO im Kontext der KI-Nutzung und ist zentrale Instanz für alle datenschutzrechtlichen Fragen. (2) Zu den Aufgaben gehören insbesondere: a) die Durchführung von Datenschutz-Folgenabschätzungen (DSFA) bei KI-Systemen mit erhöhtem Risiko; b) die Prüfung von Drittlandübermittlungen und die Sicherstellung angemessener Garantien gemäß Art. 44 ff. DSGVO; c) die Kontrolle der Umsetzung von Privacy-by-Design-Prinzipien; d) die Beratung des Verantwortlichen in allen datenschutzrechtlichen Fragen; e) die Zusammenarbeit mit dem/der KI-Beauftragten und der EDV Verantwortlichen; f) die Teilnahme am jährlichen KI-Audit; g) die Überwachung der Einhaltung der datenschutzrechtlichen Dokumentationspflichten; h) die Meldung schwerwiegender Datenschutzvorfälle an die

Geschäftsleitung und ggf. an die Garante Privacy. (3) Der/die DPO ist unabhängig und darf in der Ausübung seiner/ihrer Aufgaben nicht benachteiligt werden.

3.3 IT-Sicherheitsverantwortliche/r

(1) Der/die IT-Sicherheitsverantwortliche ist zentrale Instanz für die technische Sicherheit der KI-Nutzung. (2) Zu den Aufgaben gehören insbesondere: a) die technische Prüfung von KI-Tools, insbesondere API-Sicherheit, Logging, Zugriffskontrollen und Datenübertragungen; b) die Überwachung des Netzwerkverkehrs, die Analyse von Logfiles und die Detektion nicht autorisierter KI-Nutzung („Shadow AI"); c) die Implementierung technischer Schutzmaßnahmen gemäß ACN-Vorgaben; d) die Meldung sicherheitsrelevanter Vorfälle an den/die KI-Beauftragte/n und den/die DPO; e) die Teilnahme am jährlichen KI-Audit; f) die Beratung des Verantwortlichen in technischen Fragen der KI-Nutzung; g) die Sicherstellung der technischen Integrität und Verfügbarkeit der KI-Systeme. (3) Der/die IT-Sicherheitsverantwortliche ist verpflichtet, alle technischen Prüfungen zu dokumentieren.

3.4 Geschäftsleitung

(1) Die Geschäftsleitung genehmigt dieses Regelwerk und stellt die organisatorischen, personellen und technischen Ressourcen zur Verfügung, die für dessen Umsetzung erforderlich sind. (2) Sie überwacht die Einhaltung und ist verantwortlich für die institutionelle Umsetzung der Governance-Struktur. (3) Sie entscheidet über schwerwiegende Verstöße und Maßnahmen.

3.5 Mitarbeitende

(1) Mitarbeitende sind verpflichtet, die KI-Policy einzuhalten, ausschließlich freigegebene KI-Tools zu nutzen und Shadow-AI-Vorfälle unverzüglich zu melden. (2) Sie müssen an Schulungen teilnehmen und die Vorgaben dieses Regelwerks beachten. (3) Verstöße können disziplinarisch geahndet werden.

3.6 Externe Dienstleister

(1) Externe Dienstleister müssen die KI-Policy vertraglich anerkennen und einhalten. (2) Sie dürfen keine nicht autorisierten KI-Tools nutzen und müssen ihre KI-Nutzung dokumentieren. (3) Verstöße können zu Vertragsauflösung führen.

4. KI-Policy

4.1 Grundprinzipien

(1) Die Nutzung generativer KI-Systeme hat den Grundsätzen der Datenminimierung, Zweckbindung, Transparenz, Sicherheit und menschlichen Aufsicht zu entsprechen. (2) Jede Nutzung muss dokumentiert, nachvollziehbar und überprüfbar sein. (3) Der Verantwortliche verpflichtet sich zur verantwortungsvollen Nutzung von KI-Systemen.

4.2 Zulässige KI-Nutzung

(1) Zulässig sind: a) Textentwürfe ohne personenbezogene Daten; b) Übersetzungen nicht vertraulicher Inhalte; c) Ideenfindung und Strukturierung; d) interne Assistenzfunktionen, sofern DSGVO-konform. (2) Jede zulässige Nutzung muss im KI-Register dokumentiert werden. (3) Der Verantwortlichen fördert die verantwortungsvolle Nutzung von KI-Systemen.

4.3 Verbotstatbestände

(1) Es ist strikt untersagt: a) personenbezogene Daten in KI-Systeme einzugeben; b) vertrauliche interne Dokumente hochzuladen; c) private KI-Accounts für dienstliche Zwecke zu verwenden; d) KI-Systeme zu nutzen, die nicht auf der Freigabeliste stehen; e) automatisierte Entscheidungen ohne menschliche Aufsicht zu treffen; f)

KI-Systeme zu verwenden, die Daten in Drittländer ohne angemessene Garantien übertragen. (2) Verstöße werden disziplinarisch geahndet.

4.4 Anforderungen an Transparenz und Dokumentation

(1) Jede KI-Nutzung muss dokumentiert werden. (2) KI-unterstützt erstellte Inhalte müssen gekennzeichnet werden. (3) Der Verantwortliche führt ein KI-Register, das alle Nutzungen erfasst. (4) Transparenz dient der Nachvollziehbarkeit gegenüber Nutzern und Behörden.

4.5 Umgang mit personenbezogenen und vertraulichen Daten

(1) Die Eingabe personenbezogener oder vertraulicher Daten in generative KI-Systeme ist strikt untersagt. (2) Verstöße werden disziplinarisch geahndet. (3) Der Verantwortliche verpflichtet sich zur Einhaltung der DSGVO.

4.6 Nutzung privater KI-Accounts

(1) Die Nutzung privater KI-Accounts für dienstliche Zwecke ist untersagt. (2) Verstöße gelten als Shadow-AI-Vorfälle.

4.7 Kennzeichnung KI-unterstützter Inhalte

(1) KI-unterstützt erstellte Inhalte müssen mit einem Hinweis versehen werden. (2) Die Kennzeichnungspflicht dient der Transparenz gegenüber Nutzern und Behörden.

5. Freigabeprozess für KI-Tools

5.1 Antragstellung

(1) Jede Person, die innerhalb der Struktur des Verantwortlichen ein KI-Tool nutzen möchte, hat vor Aufnahme der Nutzung einen schriftlichen Antrag zu stellen. Dieser Antrag ist zwingend erforderlich, um die Einhaltung der gesetzlichen, organisatorischen und technischen Anforderungen sicherzustellen. (2) Der Antrag muss mindestens folgende Angaben enthalten: a) eine detaillierte Beschreibung des beabsichtigten Nutzungszwecks, einschließlich der erwarteten Ergebnisse, der Art der zu verarbeitenden Informationen und der operativen Bedeutung des Tools; b) eine vollständige Auflistung sämtlicher Datenkategorien, die im Rahmen der Nutzung verarbeitet werden sollen, einschließlich einer Erklärung, ob personenbezogene oder vertrauliche Daten betroffen sind; c) eine Risikoabschätzung, die die potenziellen Auswirkungen auf Datenschutz, Informationssicherheit, institutionelle Integrität und operative Abläufe bewertet; d) eine technische Beschreibung des Tools, einschließlich Anbieterinformationen, Datenverarbeitungsmechanismen, Speicherorten, API-Strukturen und Sicherheitsmaßnahmen; e) eine Erklärung, ob das Tool Daten in Drittländer überträgt und welche Garantien gemäß Art. 44 ff. DSGVO bestehen; f) eine Bestätigung, dass der Antragsteller die KI-Policy vollständig gelesen und verstanden hat. (3) Der Antrag ist elektronisch über das interne KI-Governance-Portal einzureichen. (4) Unvollständige Anträge werden nicht bearbeitet und gelten als nicht gestellt.

5.2 Prüfung durch KI-Beauftragte/n

(1) Der/die KI-Beauftragte prüft den Antrag umfassend unter Berücksichtigung rechtlicher, technischer, organisatorischer und ethischer Kriterien. (2) Die Prüfung umfasst insbesondere: a) die Bewertung des Nutzungszwecks im Hinblick auf institutionelle Ziele und Risiken; b) die Analyse der Datenkategorien und die Prüfung, ob personenbezogene oder vertrauliche Daten betroffen sind; c) die Bewertung der Risikoabschätzung des Antragstellers; d) die Prüfung der technischen Beschreibung des Tools; e) die Bewertung der Sicherheitsmaßnahmen des Tools; f) die Prüfung der Konformität mit DSGVO, AI Act, Garante Privacy und ACN-Vorgaben. (3) Der/die KI-Beauftragte kann zusätzliche Informationen anfordern, wenn dies zur Bewertung erforderlich ist. (4) Die Prüfung ist zu dokumentieren und im KI-Register zu speichern.

5.3 Datenschutzrechtliche Prüfung (DPO)

© Armin Wieser

(1) Der/die DPO prüft den Antrag im Hinblick auf die Einhaltung der DSGVO. (2) Die Prüfung umfasst insbesondere: a) die Bewertung der Datenminimierung und Zweckbindung; b) die Prüfung der Rechtmäßigkeit der Verarbeitung gemäß Art. 6 DSGVO; c) die Bewertung der Sicherheit der Verarbeitung gemäß Art. 32 DSGVO; d) die Prüfung von Drittlandübermittlungen gemäß Art. 44 ff. DSGVO; e) die Bewertung, ob eine Datenschutz-Folgenabschätzung (DSFA) erforderlich ist; f) die Prüfung der Einhaltung von Privacy-by-Design-Prinzipien gemäß Art. 25 DSGVO. (3) Der/die DPO kann die Nutzung untersagen, wenn datenschutzrechtliche Risiken bestehen. (4) Die Prüfung ist zu dokumentieren.

5.4 Technische Sicherheitsprüfung (IT)

(1) Der IT Verantwortliche prüft das Tool im Hinblick auf technische Sicherheit und Integrität. (2) Die Prüfung umfasst insbesondere: a) die Bewertung der API-Sicherheit; b) die Analyse der Datenübertragungsmechanismen; c) die Prüfung der Zugriffskontrollen; d) die Bewertung der Logging-Mechanismen; e) die Prüfung der Netzwerkkommunikation; f) die Bewertung der technischen Schutzmaßnahmen gemäß ACN-Vorgaben. (3) Die IT-Sicherheit kann die Nutzung untersagen, wenn technische Risiken bestehen. (4) Die Prüfung ist zu dokumentieren.

5.5 Entscheidung (Freigabe, Freigabe mit Auflagen, Ablehnung)

(1) Die Entscheidung erfolgt durch den/die KI-Beauftragte/n nach Abschluss aller Prüfungen. (2) Die Entscheidung kann lauten: a) Freigabe; b) Freigabe mit Auflagen; c) Ablehnung. (3) Auflagen können insbesondere sein: a) Einschränkungen der Nutzung; b) zusätzliche Sicherheitsmaßnahmen; c) verpflichtende Schulungen; d) regelmäßige Kontrollen. (4) Jede Entscheidung ist zu dokumentieren und dem Antragsteller mitzuteilen.

5.6 Dokumentation im KI-Register

(1) Jede Freigabe wird im KI-Register dokumentiert. (2) Das KI-Register enthält: a) den Antrag; b) die Prüfungen; c) die Entscheidung; d) die Auflagen; e) die Nutzungshistorie; f) die Widerrufe.

5.7 Widerruf der Freigabe

(1) Freigaben können jederzeit widerrufen werden, wenn neue Risiken auftreten. (2) Der Widerruf ist zu dokumentieren und dem Nutzer mitzuteilen.

6. Handlungsregeln für Mitarbeitende

6.1 Do-Regeln

(1) Mitarbeitende des Verantwortlichen sind verpflichtet, bei jeder Nutzung generativer KI-Systeme die in diesem Regelwerk niedergelegten Grundsätze, Verfahren und Beschränkungen strikt zu beachten. (2) Insbesondere haben Mitarbeitende folgende positiven Verhaltenspflichten („Do-Regeln“):

a) Nutzung ausschließlich freigegebener KI-Tools Mitarbeitende dürfen nur solche KI-Systeme verwenden, die im Rahmen des Freigabeprozesses gemäß Kapitel 5 geprüft, genehmigt und in der Freigabeliste dokumentiert wurden.

b) Vorherige Kenntnisnahme der KI-Policy Vor der erstmaligen Nutzung eines KI-Tools haben Mitarbeitende die KI-Policy vollständig zu lesen und deren Inhalt zu verstehen. Sie bestätigen dies im Rahmen der Schulungsdokumentation.

c) Kritische Prüfung der KI-Ergebnisse Alle durch KI generierten Inhalte sind einer sorgfältigen, kritischen und fachlich fundierten Prüfung zu unterziehen. Mitarbeitende dürfen KI-Ergebnisse niemals ungeprüft übernehmen.

© Armin Wieser

d) Keine Eingabe sensibler oder personenbezogener Daten Mitarbeitende haben sicherzustellen, dass in generative KI-Systeme keine personenbezogenen Daten, keine vertraulichen internen Informationen und keine besonders schützenswerten Daten eingegeben werden.

e) Dokumentation der Nutzung Jede relevante Nutzung eines KI-Systems ist im KI-Register oder in den dafür vorgesehenen Dokumentationssystemen zu erfassen, insbesondere bei Projekten, Berichten, Stellungnahmen oder externen Kommunikationen.

f) Meldung von Auffälligkeiten und Vorfällen Mitarbeitende sind verpflichtet, jede Auffälligkeit, jeden Verdacht auf Shadow-AI-Nutzung und jeden sicherheitsrelevanten Vorfall unverzüglich an den/die KI-Beauftragte/n oder die EDV Verantwortlichen zu melden.

g) Teilnahme an Schulungen Mitarbeitende haben an den verpflichtenden Schulungen gemäß Kapitel 11 teilzunehmen und sich aktiv mit den vermittelten Inhalten auseinanderzusetzen.

(3) Die Verletzung dieser Do-Regeln kann als Verstoß gegen dieses Regelwerk gewertet und disziplinarisch geahndet werden.

6.2 Don't-Regeln

(1) Neben den positiven Pflichten bestehen für Mitarbeitende klare Verbote („Don't-Regeln"), deren Missachtung als schwerwiegender Verstoß gilt.

(2) Insbesondere ist es Mitarbeitenden untersagt:

a) Eingabe personenbezogener Daten

Es ist strikt verboten, Namen, Adressen, Kontaktdaten, Gesundheitsdaten, Sozialdaten, Mitarbeiterdaten oder sonstige personenbezogene Informationen in generative KI-Systeme einzugeben.

b) Upload vertraulicher Dokumente

Interne Dokumente, Verträge, Protokolle, E-Mails, interne Berichte, Finanzdaten oder sonstige vertrauliche Unterlagen dürfen nicht in KI-Systeme hochgeladen oder als Prompt verwendet werden.

c) Nutzung privater KI-Accounts für dienstliche Zwecke

Die Verwendung privater Accounts (z. B. persönliche ChatGPT-Logins, private Copilot-Zugänge) für dienstliche Aufgaben ist untersagt und gilt als Shadow-AI-Nutzung.

d) Nutzung nicht freigegebener KI-Tools

Der Einsatz von KI-Systemen, die nicht in der Freigabeliste gemäß Kapitel 10.2 aufgeführt sind, ist verboten.

e) Automatisierte Entscheidungen ohne menschliche Aufsicht

Mitarbeitende dürfen KI-Systeme nicht zur automatisierten Entscheidungsfindung einsetzen, ohne dass eine qualifizierte menschliche Prüfung und Verantwortung gewährleistet ist.

f) Umgehung technischer Schutzmaßnahmen

Es ist untersagt, technische Schutzmaßnahmen, Zugriffsbeschränkungen oder Monitoring-Systeme zu umgehen oder zu manipulieren.

(3) Verstöße gegen diese Don't-Regeln sind als schwerwiegende Verletzung der KI-Policy zu werten und können arbeitsrechtliche Konsequenzen nach sich ziehen.

6.3 Umgang mit Fehlern und Halluzinationen

(1) Generative KI-Systeme können fehlerhafte, unvollständige oder frei erfundene („halluzinierte“) Inhalte erzeugen. Mitarbeitende sind verpflichtet, sich dieser Risiken bewusst zu sein und entsprechend vorsichtig zu handeln.

(2) Beim Umgang mit KI-Ergebnissen gilt:

a) Prüfung auf Plausibilität Alle KI-Ergebnisse sind auf Plausibilität, fachliche Richtigkeit und Konsistenz mit bekannten Fakten zu prüfen.

b) Abgleich mit Primärquellen Bei rechtlichen, fachlichen oder sensiblen Inhalten ist ein Abgleich mit Primärquellen (Gesetze, interne Richtlinien, offizielle Dokumente) zwingend erforderlich.

c) Keine Übernahme ohne menschliche Bewertung KI-Ergebnisse dürfen nicht als „Wahrheit“ betrachtet werden, sondern nur als Vorschläge, die einer menschlichen Bewertung bedürfen.

d) Dokumentation von Fehlern Erkannte gravierende Fehler oder Halluzinationen sind zu dokumentieren und dem/der KI-Beauftragten zu melden, sofern sie auf systematische Probleme hindeuten.

(3) Der Verantwortliche erkennt an, dass die Fähigkeit zur kritischen Bewertung von KI-Ergebnissen ein zentrales Element der Shadow-AI-Governance ist.

6.4 Meldepflicht bei Shadow-AI-Vorfällen

(1) Shadow-AI-Vorfälle sind alle Situationen, in denen KI-Systeme außerhalb der genehmigten, dokumentierten und kontrollierten Verfahren genutzt wurden oder genutzt werden sollten.

(2) Mitarbeitende sind verpflichtet, folgende Vorfälle unverzüglich zu melden:

a) Nutzung privater KI-Accounts für dienstliche Zwecke; b) Nutzung nicht freigegebener KI-Tools; c) Eingabe personenbezogener oder vertraulicher Daten in KI-Systeme; d) Umgehung technischer Schutzmaßnahmen; e) Verdacht auf unautorisierte KI-Nutzung durch Dritte.

(3) Meldungen sind an den/die KI-Beauftragte/n oder die EDV Verantwortlichen zu richten und möglichst detailliert zu beschreiben.

(4) Der Verantwortliche stellt klar, dass die Meldung von Vorfällen als verantwortungsvolles Verhalten gewertet wird und nicht zu Nachteilen für die meldende Person führen darf, sofern kein vorsätzliches Fehlverhalten vorliegt.

6.5 Nutzung von KI-Ergebnissen in offiziellen Dokumenten

(1) Offizielle Dokumente des Verantwortlichen (Berichte, Stellungnahmen, Schreiben, interne Richtlinien, externe Kommunikation) dürfen nur dann KI-unterstützte Inhalte enthalten, wenn:

a) die Inhalte einer sorgfältigen fachlichen Prüfung unterzogen wurden; b) die Verantwortung für den Inhalt eindeutig bei einer menschlichen Person liegt; c) die Nutzung der KI im KI-Register dokumentiert ist.

(2) Bei sensiblen Dokumenten (z. B. rechtlichen Stellungnahmen, Datenschutzdokumenten, Compliance-Berichten) ist der Einsatz generativer KI besonders restriktiv zu handhaben.

(3) Der Verantwortliche kann für bestimmte Dokumenttypen den Einsatz generativer KI vollständig untersagen.

7. DSGVO-Konformität beim KI-Einsatz

7.1 Datenminimierung und Zweckbindung

(1) Die Verarbeitung von Daten im Zusammenhang mit der Nutzung generativer KI-Systeme hat den Grundsätzen der Datenminimierung und Zweckbindung gemäß Art. 5 Abs. 1 lit. b und c DSGVO zu entsprechen.

(2) Datenminimierung bedeutet, dass ausschließlich solche Daten verarbeitet werden dürfen, die für den konkret definierten Zweck der KI-Nutzung zwingend erforderlich sind. (3) Zweckbindung bedeutet, dass die Verarbeitung nur zu dem Zweck erfolgen darf, der im Freigabeantrag gemäß Kapitel 5.1 angegeben und genehmigt wurde. (4) Eine Zweckänderung ist nur zulässig, wenn: a) ein neuer Zweck klar definiert wird; b) eine neue Rechtsgrundlage gemäß Art. 6 DSGVO besteht; c) eine erneute Prüfung durch den/die KI-Beauftragte/n und den/die DPO erfolgt; d) die Änderung im KI-Register dokumentiert wird. (5) Der Verantwortliche untersagt ausdrücklich die Nutzung generativer KI-Systeme zur Verarbeitung personenbezogener Daten, sofern keine ausdrückliche Rechtsgrundlage besteht und die Verarbeitung nicht durch interne Systeme erfolgt, die vollständig unter Kontrolle des Verantwortlichen stehen. (6) Mitarbeitende sind verpflichtet, vor jeder Nutzung zu prüfen, ob die eingegebenen Daten dem Grundsatz der Datenminimierung entsprechen.

7.2 Privacy by Design & Default

(1) Der Verantwortliche verpflichtet sich, sämtliche KI-Nutzungen nach dem Prinzip „Privacy by Design & Default" gemäß Art. 25 DSGVO zu gestalten. (2) Privacy by Design bedeutet, dass Datenschutzaspekte bereits bei der Konzeption, Entwicklung, Auswahl und Implementierung von KI-Systemen berücksichtigt werden müssen. (3) Privacy by Default bedeutet, dass die datenschutzfreundlichsten Einstellungen standardmäßig aktiviert sein müssen. (4) Die Umsetzung umfasst insbesondere: a) technische Maßnahmen zur Vermeidung unnötiger Datenverarbeitung; b) Beschränkung von Zugriffsrechten auf das notwendige Minimum; c) Pseudonymisierung oder Anonymisierung von Daten, sofern möglich; d) Einsatz von Verschlüsselungstechnologien; e) regelmäßige Überprüfung der Systeme auf Datenschutzkonformität; f) Dokumentation aller Maßnahmen im KI-Register. (5) Der/die DPO überwacht die Umsetzung dieser Prinzipien und kann Maßnahmen anordnen, wenn Verstöße festgestellt werden.

7.3 Sicherheit der Verarbeitung (Art. 32 DSGVO)

(1) Der Verantwortliche verpflichtet sich, die Sicherheit der Verarbeitung gemäß Art. 32 DSGVO durch geeignete technische und organisatorische Maßnahmen sicherzustellen. (2) Diese Maßnahmen umfassen insbesondere: a) Verschlüsselung von Daten während der Übertragung und Speicherung; b) Implementierung von Zugriffskontrollen, die sicherstellen, dass nur autorisierte Personen KI-Systeme nutzen können; c) Protokollierung aller Zugriffe und Nutzungen; d) regelmäßige Sicherheitsupdates und Patches; e) Netzwerk-Monitoring zur Erkennung von Anomalien; f) Schutz vor unbefugtem Zugriff, Datenverlust und Manipulation. (3) Die EDV Verantwortlichen ist für die Umsetzung dieser Maßnahmen verantwortlich und dokumentiert alle sicherheitsrelevanten Vorgänge. (4) Bei sicherheitsrelevanten Vorfällen ist unverzüglich der/die KI-Beauftragte und der/die DPO zu informieren.

7.4 Drittlandübermittlungen

(1) Werden im Rahmen der KI-Nutzung Daten in Drittländer übertragen, sind die Vorgaben der Art. 44 ff. DSGVO strikt einzuhalten. (2) Der/die DPO prüft: a) ob ein Angemessenheitsbeschluss gemäß Art. 45 DSGVO vorliegt; b) ob geeignete Garantien gemäß Art. 46 DSGVO bestehen (Standardvertragsklauseln, Binding Corporate Rules); c) ob zusätzliche Schutzmaßnahmen erforderlich sind (z. B. Verschlüsselung, Pseudonymisierung); d) ob die Übermittlung mit den Grundsätzen der Datenminimierung und Zweckbindung vereinbar ist. (3) Ohne ausreichende Garantien ist die Nutzung des betreffenden KI-Tools untersagt. (4) Die Prüfung ist im KI-Register zu dokumentieren.

7.5 Datenschutz-Folgenabschätzung (DSFA) für KI-Systeme

(1) Für KI-Systeme, die ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen darstellen, ist eine DSFA gemäß Art. 35 DSGVO durchzuführen. (2) Eine DSFA ist insbesondere erforderlich, wenn: a) das KI-System Entscheidungen vorbereitet, die erhebliche Auswirkungen auf Personen haben; b) das KI-System sensible Daten verarbeitet; c) das KI-System umfangreiche Datenanalysen durchführt; d) das KI-System neue Technologien einsetzt, deren Risiken noch nicht vollständig bekannt sind. (3) Die DSFA umfasst: a) eine

detaillierte Beschreibung der geplanten Verarbeitung; b) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit; c) eine Risikoanalyse; d) Maßnahmen zur Risikominderung; e) eine Stellungnahme des/der DPO. (4) Die DSFA ist im KI-Register zu dokumentieren.

7.6 Dokumentationspflichten gegenüber Garante Privacy

(1) Der Verantwortliche ist verpflichtet, gegenüber der Garante Privacy jederzeit nachweisen zu können, dass KI-Nutzungen DSGVO-konform erfolgen. (2) Dazu gehören: a) DSFA-Dokumente; b) KI-Register; c) Freigabelisten; d) Schulungsnachweise; e) Auditberichte; f) technische Prüfberichte; g) Risikoanalysen. (3) Der/die DPO koordiniert die Bereitstellung dieser Nachweise. (4) Der Verantwortliche verpflichtet sich zur konstruktiven Zusammenarbeit mit der Garante Privacy.

8. AI-Act-Konformität

8.1 Risikoklassifizierung der eingesetzten KI-Systeme

(1) Alle eingesetzten KI-Systeme sind gemäß AI Act einer Risikoklasse zuzuordnen. (2) Der Verantwortliche unterscheidet: a) verbotene KI-Praktiken gemäß Kapitel II AI Act; b) Hochrisiko-KI gemäß Kapitel III AI Act; c) KI mit begrenztem Risiko; d) KI mit minimalem Risiko. (3) Der/die KI-Beauftragte dokumentiert die Einstufung im KI-Register. (4) Die Einstufung ist regelmäßig zu überprüfen und bei technologischen oder rechtlichen Änderungen anzupassen.

8.2 Pflichten für Hochrisiko-KI

(1) Für Hochrisiko-KI gelten besondere Pflichten, darunter: a) umfassende technische Dokumentation; b) Transparenz gegenüber Nutzern; c) menschliche Aufsicht; d) kontinuierliche Risikoüberwachung; e) Konformitätsbewertung; f) Implementierung von Qualitätsmanagementsystemen; g) Protokollierung aller relevanten Vorgänge. (2) Der Verantwortliche setzt Hochrisiko-KI nur ein, wenn diese Pflichten erfüllt werden können. (3) Der/die KI-Beauftragte ist für die Überwachung verantwortlich.

8.3 Transparenzpflichten

(1) Nutzer müssen darüber informiert werden, wenn sie mit KI-Systemen interagieren oder wenn Inhalte durch KI erzeugt wurden. (2) Transparenz umfasst: a) Hinweise in Dokumenten; b) Information in Schulungen; c) klare Kommunikation gegenüber Betroffenen; d) Kennzeichnung KI-unterstützter Inhalte gemäß Kapitel 4.7. (3) Der Verantwortlichen verpflichtet sich zur vollständigen Transparenz gegenüber Nutzern und Behörden.

8.4 Anforderungen an menschliche Aufsicht

(1) KI-Systeme dürfen nicht autonom Entscheidungen treffen, die erhebliche Auswirkungen auf Personen haben, ohne menschliche Aufsicht. (2) Menschliche Aufsicht bedeutet: a) Möglichkeit zur Intervention; b) Verantwortung für die endgültige Entscheidung; c) Verständnis der Funktionsweise des Systems; d) regelmäßige Überprüfung der Ergebnisse; e) Dokumentation der Aufsicht. (3) Der Verantwortliche stellt sicher, dass menschliche Aufsicht jederzeit gewährleistet ist.

8.5 Verbotene KI-Praktiken

(1) Der Verantwortliche setzt keine KI-Praktiken ein, die gemäß AI Act verboten sind, insbesondere: a) manipulative Systeme, die menschliches Verhalten beeinflussen; b) biometrische Echtzeitüberwachung; c) Systeme zur Ausnutzung von Schwächen bestimmter Personengruppen; d) Systeme, die unzulässige Profiling-Methoden einsetzen. (2) Verstöße werden als schwerwiegende Verletzung der KI-Policy gewertet.

8.6 Konformitätsbewertung und Nachweisführung

(1) Für bestimmte KI-Systeme ist eine Konformitätsbewertung erforderlich. (2) Der Verantwortliche dokumentiert: a) technische Unterlagen; b) Risikoanalysen; c) Prüfberichte; d) Zertifizierungen; e) Auditberichte. (3) Der/die KI-Beauftragte ist für die Nachweisführung verantwortlich.

9. Risikoorientiertes Kontrollsystem

9.1 Kontrollplan

(1) Der Verantwortliche implementiert einen risikoorientierten Kontrollplan für KI-Nutzungen. (2) Dieser umfasst: a) quartalsweise Kontrollen; b) jährliche Audits; c) anlassbezogene Prüfungen; d) Stichprobenkontrollen; e) systematische Überprüfungen der Freigabeliste. (3) Der Kontrollplan wird jährlich aktualisiert.

9.2 Shadow-AI-Detektion (Monitoring, Logfiles, Netzwerk)

(1) Die EDV Verantwortlichen überwacht: a) Netzwerkverkehr; b) Logfiles; c) Nutzungsmuster; d) API-Zugriffe; e) ungewöhnliche Datenübertragungen. (2) Ziel ist die Erkennung nicht autorisierter KI-Nutzung. (3) Verdachtsfälle werden dokumentiert und untersucht.

9.3 Prüfung der Freigabeliste

(1) Die Freigabeliste wird regelmäßig überprüft und aktualisiert. (2) Nicht mehr konforme Tools werden entfernt. (3) Änderungen werden dokumentiert.

9.4 Interne Kontrollen

(1) Der/die KI-Beauftragte führt interne Kontrollen durch, um die Einhaltung der KI-Policy zu überwachen. (2) Ergebnisse werden dokumentiert und der Geschäftsleitung vorgelegt.

9.5 Externe Kontrollen (Revision, Behörden)

(1) Der Verantwortliche ermöglicht externen Prüfern und Behörden Einsicht in relevante Dokumente. (2) Sie arbeitet konstruktiv mit Aufsichtsbehörden zusammen. (3) Externe Prüfungen werden dokumentiert.

9.6 Eskalationswege bei Verstößen

(1) Bei Verstößen gegen dieses Regelwerk gelten klare Eskalationswege: a) Meldung an KI-Beauftragte/n; b) Information des/der DPO; c) ggf. Meldung an Geschäftsleitung; d) Einleitung von Maßnahmen; e) Dokumentation im Shadow-AI-Melderegister. (2) Schwerwiegende Verstöße können arbeitsrechtliche Konsequenzen haben.

10. Dokumentation und Registerführung

(NEU, ausführlich)

10.1 KI-Register

(1) Das KI-Register ist das zentrale Dokumentationsinstrument für alle KI-Nutzungen. (2) Es enthält: a) freigegebene Tools; b) Nutzungen; c) Vorfälle; d) Prüfungen; e) Entscheidungen; f) Widerrufe; g) Risikoanalysen; h) technische Prüfberichte. (3) Das KI-Register wird elektronisch geführt.

10.2 Freigabeliste

(1) Die Freigabeliste enthält alle KI-Tools, die offiziell genehmigt wurden. (2) Sie wird regelmäßig aktualisiert und ist für alle Mitarbeitenden einsehbar.

10.3 Auditberichte

© Armin Wieser

(1) Jährliche Auditberichte dokumentieren: a) den Stand der KI-Governance; b) identifizierte Risiken; c) durchgeführte Maßnahmen; d) Empfehlungen für Verbesserungen. (2) Auditberichte werden der Geschäftsleitung vorgelegt.

10.4 Schulungsnachweise

(1) Die Teilnahme an Schulungen wird dokumentiert und im Schulungsregister erfasst. (2) Diese Nachweise dienen als Beleg gegenüber Behörden.

10.5 Shadow-AI-Melderegister

(1) Alle Shadow-AI-Vorfälle werden in einem eigenen Register erfasst. (2) Dieses dient der Analyse und Risikominimierung. (3) Das Register wird jährlich ausgewertet.

10.6 Aufbewahrungsfristen

(1) Dokumente im Rahmen der KI-Governance werden mindestens 5 Jahre aufbewahrt. (2) Bei gesetzlichen Vorgaben gelten längere Fristen.

11. Schulung und Sensibilisierung

11.1 Schulungskonzept

(1) Der Verantwortliche implementiert ein umfassendes, mehrstufiges und systematisch aufgebautes Schulungskonzept zur Governance, sicheren Nutzung und institutionellen Kontrolle generativer KI-Systeme. Dieses Schulungskonzept bildet einen integralen Bestandteil der Shadow-AI-Governance und dient der Sicherstellung, dass sämtliche Mitarbeitende über die erforderlichen Kenntnisse, Fähigkeiten und Verhaltensweisen verfügen, um KI-Systeme verantwortungsvoll, rechtskonform und im Einklang mit den organisatorischen Vorgaben des Verantwortlichen zu nutzen.

(2) Das Schulungskonzept umfasst sowohl theoretische als auch praktische Inhalte. Die theoretischen Inhalte vermitteln Grundlagenwissen über KI-Technologien, rechtliche Rahmenbedingungen, Datenschutzanforderungen, Risiken und organisatorische Vorgaben. Die praktischen Inhalte umfassen Übungen, Fallbeispiele, Simulationen, Risikoanalysen und die Anwendung der KI-Policy in realitätsnahen Szenarien.

(3) Das Schulungskonzept ist modular aufgebaut und umfasst mindestens folgende Elemente: a) Grundlagenschulung für neue Mitarbeitende; b) Vertiefungsschulung für Mitarbeitende mit erhöhtem KI-Nutzungsbedarf; c) Spezialschulung für Führungskräfte, DPO, KI-Beauftragte und IT-Sicherheitsverantwortliche; d) Auffrischungsschulung zur Wiederholung und Aktualisierung wesentlicher Inhalte; e) Anlassbezogene Schulungen, z. B. bei neuen gesetzlichen Vorgaben, neuen KI-Tools oder sicherheitsrelevanten Vorfällen.

(4) Das Schulungskonzept wird jährlich überprüft und an neue technologische, rechtliche und organisatorische Entwicklungen angepasst. Die Überprüfung erfolgt durch den/die KI-Beauftragte/n in Zusammenarbeit mit dem/der DPO und der EDV Verantwortlichen.

(5) Der Verantwortliche stellt sicher, dass Schulungen in einer Form durchgeführt werden, die den unterschiedlichen Lernbedürfnissen der Mitarbeitenden gerecht wird. Dies umfasst Präsenzschulungen, digitale Schulungen, interaktive Workshops, E-Learning-Module und schriftliche Materialien.

(6) Die Teilnahme an Schulungen ist verpflichtend und stellt eine arbeitsvertragliche Nebenpflicht dar. Der Verantwortliche kann die Teilnahme an Schulungen als Voraussetzung für die Nutzung bestimmter KI-Tools festlegen.

11.2 Pflichtschulungen

(1) Alle Mitarbeitenden des Verantwortlichen sind verpflichtet, an den Pflichtschulungen zur Shadow-AI-Governance teilzunehmen. Diese Pflicht erstreckt sich auf sämtliche Beschäftigungsformen, einschließlich Vollzeit-, Teilzeit-, Praktikanten-, Ehrenamts- und externen Mitarbeitenden, sofern diese Zugang zu Informationssystemen des Verantwortlichen haben.

(2) Die Pflichtschulungen umfassen mindestens folgende Inhalte:

a) KI-Grundlagen Einführung in Funktionsweise, Modelle, Risiken und Grenzen generativer KI-Systeme.

b) Risiken der KI-Nutzung Darstellung technischer, rechtlicher, ethischer und organisatorischer Risiken, einschließlich Halluzinationen, Bias, Fehlentscheidungen, Datenschutzverletzungen und Shadow-AI-Gefahren.

c) KI-Policy des Verantwortlichen und detaillierte Vermittlung der internen Regeln, Verbote, Pflichten, Freigabeprozesse und Kontrollmechanismen gemäß diesem Regelwerk.

d) Praktische Beispiele und Fallstudien Analyse realer und hypothetischer Szenarien, in denen KI-Systeme fehlerhafte oder riskante Ergebnisse erzeugen, sowie Übungen zur korrekten Bewertung und Reaktion.

e) Rechtliche Vorgaben Vermittlung der relevanten Bestimmungen der DSGVO, des AI Act, der Garante Privacy und der ACN-Vorgaben.

f) Technische Schutzmaßnahmen Einführung in technische Sicherheitsmechanismen, Zugriffskontrollen, Monitoring-Systeme und sichere Nutzung digitaler Werkzeuge.

(3) Die Pflichtschulungen werden mindestens einmal jährlich durchgeführt. Bei wesentlichen Änderungen der Rechtslage oder der eingesetzten KI-Systeme sind zusätzliche Schulungen verpflichtend.

(4) Der Verantwortliche stellt sicher, dass die Pflichtschulungen von fachlich qualifizierten Personen durchgeführt werden, die über Expertise in KI-Technologie, Datenschutzrecht und Informationssicherheit verfügen.

11.3 Awareness-Materialien

(1) Der Verantwortliche stellt umfassende Awareness-Materialien bereit, die der kontinuierlichen Sensibilisierung der Mitarbeitenden dienen und die Bedeutung einer verantwortungsvollen KI-Nutzung im Arbeitsalltag verdeutlichen.

(2) Awareness-Materialien werden regelmäßig aktualisiert und an neue technologische und rechtliche Entwicklungen angepasst.

(3) Awareness-Materialien sind verpflichtend zu beachten und stellen eine Ergänzung zu den Pflichtschulungen dar.

11.4 Dokumentation der Teilnahme

(1) Die Teilnahme an Schulungen wird vollständig dokumentiert und im Schulungsregister erfasst. Das Schulungsregister ist ein offizielles Dokument des Verantwortlichen und dient als Nachweis gegenüber internen und externen Prüfinstanzen.

(2) Das Schulungsregister enthält mindestens: a) Name des Teilnehmenden; b) Datum der Schulung; c) Art der Schulung; d) Inhalte der Schulung; e) Name der Schulungsleitung; f) Bestätigung der Teilnahme.

(3) Fehlende Teilnahme an Pflichtschulungen kann zu organisatorischen Maßnahmen führen, einschließlich: a) Einschränkung der Nutzung bestimmter KI-Tools; b) Verpflichtung zur Nachschulung; c) disziplinarischen Maßnahmen gemäß Kapitel 12.

(4) Der Verantwortliche stellt sicher, dass das Schulungsregister jederzeit aktuell und vollständig ist.

© Armin Wieser

11.5 Wiederholungsschulungen

(1) Wiederholungsschulungen dienen der Auffrischung, Vertiefung und Aktualisierung der Kenntnisse der Mitarbeitenden im Bereich der KI-Governance.

(2) Wiederholungsschulungen finden statt: a) regelmäßig, mindestens einmal jährlich; b) anlassbezogen, z. B. bei neuen gesetzlichen Vorgaben, neuen KI-Tools, sicherheitsrelevanten Vorfällen oder identifizierten Wissenslücken.

(3) Wiederholungsschulungen umfassen sowohl theoretische als auch praktische Inhalte und können spezifische Schwerpunkte setzen, z. B. Datenschutz, technische Sicherheit, Risikoanalyse oder neue KI-Modelle.

(4) Die Teilnahme an Wiederholungsschulungen ist verpflichtend und wird im Schulungsregister dokumentiert.

12. Sanktionen und Maßnahmen bei Verstößen

12.1 Interne Sanktionen

(1) Verstöße gegen dieses Regelwerk stellen eine Verletzung arbeitsvertraglicher Pflichten dar und können zu internen Sanktionen führen.

(2) Interne Sanktionen umfassen mindestens: a) **Verwarnungen**, die als formelle Hinweise auf Fehlverhalten dienen; b) **Abmahnungen**, die als schwerwiegende Rüge dokumentiert werden; c) **Disziplinarmaßnahmen**, einschließlich verpflichtender Nachschulungen, Einschränkungen von Zugriffsrechten oder organisatorischer Maßnahmen; d) **Einschränkung von Zugriffsrechten**, insbesondere auf KI-Tools, interne Systeme oder sensible Daten.

(3) Die Art der Sanktion richtet sich nach Schwere, Häufigkeit und Auswirkungen des Verstoßes.

(4) Alle Sanktionen werden dokumentiert und im Shadow-AI-Melderegister erfasst.

12.2 Einschränkung von Zugriffsrechten

(1) Bei Verstößen gegen dieses Regelwerk können Zugriffsrechte auf Systeme eingeschränkt oder entzogen werden, insbesondere wenn: a) ein Risiko für Datenschutz oder Informationssicherheit besteht; b) ein Shadow-AI-Vorfall festgestellt wurde; c) ein Mitarbeitender wiederholt gegen die KI-Policy verstoßen hat.

(2) Einschränkungen dienen der Risikominimierung und können temporär oder dauerhaft sein.

(3) Entscheidungen über Einschränkungen werden dokumentiert.

12.3 Disziplinarmaßnahmen

(1) Schwere Verstöße gegen dieses Regelwerk können arbeitsrechtliche Konsequenzen nach sich ziehen.

(2) Disziplinarmaßnahmen umfassen mindestens: a) Versetzung in eine Position mit geringeren Zugriffsrechten; b) Abmahnung; c) Kündigung, insbesondere bei vorsätzlichen oder wiederholten Verstößen.

(3) Die Geschäftsleitung entscheidet über Disziplinarmaßnahmen.

12.4 Meldung an Geschäftsleitung

(1) Schwerwiegende Vorfälle werden der Geschäftsleitung gemeldet.

(2) Die Geschäftsleitung entscheidet über weitere Maßnahmen, einschließlich: a) organisatorischer Änderungen; b) Anpassung der KI-Policy; c) Einleitung externer Prüfungen; d) Meldung an Behörden.

12.5 Externe Sanktionen (Garante Privacy, AI Act, ACN)

(1) Verstöße gegen dieses Regelwerk können zu externen Sanktionen führen, insbesondere wenn gesetzliche Vorgaben verletzt wurden.

(2) Externe Sanktionen umfassen: a) Bußgelder gemäß DSGVO oder AI Act; b) Auflagen durch die Garante Privacy oder ACN; c) Einschränkungen von Tätigkeiten, z. B. Verbot bestimmter KI-Nutzungen; d) behördliche Prüfungen oder Audits.

(3) Der Verantwortliche arbeitet konstruktiv mit Behörden zusammen und stellt alle erforderlichen Dokumente bereit.

13. Inkrafttreten und Aktualisierung

13.1 Inkrafttreten

(1) Dieses Regelwerk tritt am 01. September 2026 in Kraft.

(2) Es ersetzt alle früheren Regelungen zur KI-Nutzung, KI-Governance, digitalen Assistenzsystemen und verwandten Themen.

(3) Mit Inkrafttreten sind alle Mitarbeitenden verpflichtet, die Inhalte dieses Regelwerks zu beachten.

13.2 Jährliche Überprüfung

(1) Das Regelwerk wird mindestens einmal jährlich überprüft, um sicherzustellen, dass es den aktuellen rechtlichen, technologischen und organisatorischen Anforderungen entspricht.

(2) Die jährliche Überprüfung umfasst: a) Analyse rechtlicher Änderungen (DSGVO, AI Act, Garante Privacy, ACN); b) Bewertung technologischer Entwicklungen (neue KI-Modelle, neue Risiken); c) Prüfung organisatorischer Anforderungen; d) Auswertung der Ergebnisse der jährlichen Audits; e) Analyse von Shadow-AI-Vorfällen; f) Bewertung der Wirksamkeit der Schulungen.

(3) Die Ergebnisse der Überprüfung werden dokumentiert und der Geschäftsleitung vorgelegt.

13.3 Anpassung an neue gesetzliche Vorgaben

(1) Bei Änderungen der Rechtslage wird das Regelwerk unverzüglich angepasst.

(2) Anpassungen umfassen: a) Ergänzung neuer Pflichten; b) Anpassung bestehender Regelungen; c) Einführung neuer Prozesse; d) Aktualisierung der Schulungsinhalte.

(3) Anpassungen werden dokumentiert und allen Mitarbeitenden kommuniziert.

13.4 Verantwortlichkeit für Aktualisierungen

(1) Der/die KI-Beauftragte ist für Aktualisierungen verantwortlich.

(2) Die Geschäftsleitung genehmigt Änderungen und stellt die erforderlichen Ressourcen bereit.

(3) Der/die DPO und die EDV Verantwortlichen unterstützen die Aktualisierung.

© Armin Wieser

ITALIANO

INDICE COMPLETO

1. **Scopo, obiettivi e ambito di applicazione** 1.1 Contesto e quadro normativo 1.2 Obiettivi della Shadow AI Governance 1.3 Ambito di applicazione (personale, dirigenti, esterni) 1.4 Basi giuridiche (GDPR, AI Act, Garante Privacy, ACN)
2. **Definizioni** 2.1 Intelligenza Artificiale Generativa 2.2 Shadow AI 2.3 Strumenti di IA 2.4 Dati personali 2.5 Sistemi di IA ad alto rischio secondo l'AI Act
3. **Struttura di governance e responsabilità** 3.1 Responsabile IA 3.2 Responsabile della Protezione dei Dati (DPO) 3.3 Responsabile della Sicurezza Informatica 3.4 Direzione 3.5 Personale 3.6 Fornitori esterni
4. **Policy per l'uso dell'IA** 4.1 Principi generali 4.2 Utilizzi consentiti 4.3 Divieti 4.4 Trasparenza e documentazione 4.5 Gestione dei dati personali e riservati 4.6 Uso di account IA privati 4.7 Indicazione dei contenuti generati con IA
5. **Procedura di approvazione degli strumenti IA** 5.1 Presentazione della richiesta 5.2 Valutazione del Responsabile IA 5.3 Valutazione del DPO 5.4 Verifica tecnica (IT) 5.5 Decisione (approvazione, approvazione con condizioni, rifiuto) 5.6 Registrazione nel Registro IA 5.7 Revoca dell'approvazione
6. **Regole operative per il personale** 6.1 Comportamenti consentiti (Do) 6.2 Comportamenti vietati (Don't) 6.3 Gestione di errori e allucinazioni dell'IA 6.4 Obbligo di segnalazione di casi di Shadow AI 6.5 Uso di contenuti IA in documenti ufficiali
7. **Conformità al GDPR nell'uso dell'IA** 7.1 Minimizzazione dei dati e limitazione della finalità 7.2 Privacy by Design & Default 7.3 Sicurezza del trattamento (Art. 32 GDPR) 7.4 Trasferimenti verso Paesi terzi 7.5 Valutazione d'impatto sulla protezione dei dati (DPIA) per sistemi IA 7.6 Obblighi documentali verso il Garante Privacy
8. **Conformità all'AI Act** 8.1 Classificazione del rischio dei sistemi IA 8.2 Obblighi per sistemi IA ad alto rischio 8.3 Obblighi di trasparenza 8.4 Supervisione umana 8.5 Pratiche IA vietate 8.6 Valutazione di conformità e dimostrazione
9. **Sistema di controllo basato sul rischio** 9.1 Piano dei controlli 9.2 Rilevazione della Shadow AI (monitoraggio, log, rete) 9.3 Verifica della lista degli strumenti approvati 9.4 Controlli interni 9.5 Controlli esterni (revisione, autorità) 9.6 Procedure di escalation in caso di violazioni
10. **Documentazione e gestione dei registri** 10.1 Registro IA 10.2 Lista degli strumenti approvati 10.3 Rapporti di audit 10.4 Attestati di formazione 10.5 Registro delle segnalazioni di Shadow AI 10.6 Tempi di conservazione
11. **Formazione e sensibilizzazione** 11.1 Piano formativo 11.2 Formazioni obbligatorie 11.3 Materiali di sensibilizzazione 11.4 Documentazione della partecipazione 11.5 Formazioni periodiche
12. **Sanzioni e misure in caso di violazioni** 12.1 Sanzioni interne 12.2 Limitazione dei diritti di accesso 12.3 Misure disciplinari 12.4 Segnalazione alla Direzione 12.5 Sanzioni esterne (Garante Privacy, AI Act, ACN)
13. **Entrata in vigore e aggiornamenti** 13.1 Entrata in vigore 13.2 Revisione annuale 13.3 Adeguamento alle nuove normative 13.4 Responsabilità degli aggiornamenti

Wenn du willst, übersetze ich dir **den gesamten Haupttext ebenfalls geglättet**, Abschnitt für Abschnitt.

CAPITOLO 1 – Scopo, obiettivi e ambito di applicazione

1.1 Contesto e quadro normativo

(1) Il Titolare riconosce le profonde trasformazioni derivanti dall'impiego di sistemi di Intelligenza Artificiale generativa in ambiti sociali, amministrativi e organizzativi. Tali sistemi, capaci di generare contenuti autonomamente, supportare decisioni o facilitare processi complessi di trattamento dei dati, rappresentano un'evoluzione tecnologica che comporta opportunità ma anche rischi significativi.

(2) Il quadro normativo è definito da una serie articolata di norme europee e nazionali che regolano l'uso dei sistemi di IA, tra cui il Regolamento (UE) 2016/679 (GDPR), il Regolamento sull'Intelligenza Artificiale (AI Act), le linee guida e i provvedimenti del Garante per la Protezione dei Dati Personali, nonché le disposizioni dell'Agenzia per la Cybersicurezza Nazionale (ACN).

(3) Il Titolare riconosce che l'uso non controllato di sistemi di IA ("Shadow AI") può generare rischi rilevanti, tra cui violazioni della protezione dei dati, incidenti di sicurezza informatica, decisioni errate, responsabilità legali, danni reputazionali e disfunzioni operative.

(4) Alla luce di ciò, il Titolare si impegna a definire un quadro interno completo che regoli, controlli, documenti e renda verificabile l'utilizzo dei sistemi di IA generativa.

1.2 Obiettivi della Shadow AI Governance

(1) Il presente documento ha l'obiettivo di istituire un sistema di governance coerente, completo e conforme alla normativa, che garantisca un uso sicuro, trasparente e responsabile dei sistemi di IA generativa all'interno dell'organizzazione.

(2) La Shadow AI Governance persegue in particolare i seguenti obiettivi: a) prevenire l'uso non autorizzato di strumenti IA; b) garantire il rispetto delle normative vigenti; c) proteggere dati personali e informazioni riservate; d) ridurre rischi istituzionali, operativi e legali; e) promuovere una cultura di utilizzo responsabile dell'IA; f) costruire un ecosistema IA documentato, controllato e verificabile.

(3) La governance comprende misure sia preventive sia reattive.

1.3 Ambito di applicazione

(1) Il presente regolamento si applica a tutto il personale, ai dirigenti, ai tirocinanti, ai volontari, ai fornitori esterni, ai partner e a qualsiasi soggetto che abbia accesso ai sistemi informativi del Titolare.

(2) Le disposizioni si applicano indipendentemente dal ruolo, dalla forma contrattuale o dal livello gerarchico.

(3) I fornitori esterni devono accettare e rispettare contrattualmente le presenti regole.

1.4 Basi giuridiche

(1) Il regolamento si fonda sulle seguenti fonti normative: a) **GDPR**, in particolare minimizzazione dei dati, limitazione della finalità, trasparenza, sicurezza del trattamento, DPIA e trasferimenti verso Paesi terzi; b) **AI Act**, in particolare classificazione del rischio, obblighi per sistemi ad alto rischio, trasparenza, supervisione umana, pratiche vietate e valutazione di conformità; c) linee guida e decisioni del **Garante Privacy**; d) disposizioni dell'**ACN** in materia di cybersicurezza; e) **Codice Privacy (D.Lgs. 196/2003)**; f) normative nazionali e regionali rilevanti.

(2) Il Titolare si impegna a monitorare costantemente gli sviluppi normativi e ad aggiornare il regolamento.

(3) Le basi giuridiche costituiscono parte integrante del presente documento.

CAPITOLO 2 – Definizioni

2.1 Intelligenza Artificiale Generativa

Sistemi che, tramite modelli algoritmici, sono in grado di generare contenuti quali testi, immagini, audio, video, codice o altri artefatti digitali.

2.2 Shadow AI

Qualsiasi utilizzo di un sistema di IA senza previa autorizzazione, registrazione o controllo da parte del Titolare.

2.3 Strumento di IA

Software, piattaforma o API che mette a disposizione funzionalità basate sull'Intelligenza Artificiale.

2.4 Dati personali

Informazioni relative a una persona fisica identificata o identificabile, ai sensi dell'art. 4 GDPR.

2.5 Sistemi di IA ad alto rischio (AI Act)

Sistemi di IA che, ai sensi del Capitolo II dell'AI Act, sono soggetti a requisiti regolatori specifici e più stringenti.

CAPITOLO 3 – Struttura di governance e responsabilità

3.1 Responsabile IA

(1) Il Titolare nomina un Responsabile IA che funge da riferimento normativo, organizzativo e operativo per tutte le attività legate all'uso, al controllo e allo sviluppo dei sistemi di IA generativa.

(2) Il Responsabile IA dispone di poteri ampi, sia preventivi sia reattivi.

(3) Le sue principali responsabilità includono: a) valutazione e approvazione degli strumenti IA; b) gestione del Registro IA; c) conduzione di analisi dei rischi secondo GDPR, AI Act, Garante Privacy e ACN; d) redazione di report annuali alla Direzione; e) coordinamento con DPO, IT e partner esterni; f) monitoraggio della conformità alle regole interne; g) attivazione di misure correttive in caso di violazioni; h) garanzia della conformità normativa; i) consulenza strategica alla Direzione; j) aggiornamento continuo della governance IA.

(4) Il Responsabile IA può revocare approvazioni, vietare utilizzi e avviare indagini su casi di Shadow AI.

(5) Ogni decisione deve essere documentata.

3.2 Responsabile della Protezione dei Dati (DPO)

(1) Il DPO vigila sulla conformità al GDPR nell'uso dei sistemi IA.

(2) Le sue responsabilità includono: a) valutazioni d'impatto (DPIA) per sistemi IA ad alto rischio; b) verifica dei trasferimenti verso Paesi terzi; c) controllo del principio di Privacy by Design; d) consulenza al Titolare; e) collaborazione con Responsabile IA e IT; f) partecipazione agli audit annuali; g) verifica degli obblighi documentali; h) segnalazione di incidenti gravi alla Direzione e, se necessario, al Garante.

(3) Il DPO opera in piena indipendenza.

3.3 Responsabile della Sicurezza Informatica

(1) È la figura incaricata della sicurezza tecnica dei sistemi IA.

(2) Le sue responsabilità includono: a) verifica della sicurezza delle API; b) analisi dei meccanismi di trasmissione dei dati; c) controllo degli accessi; d) valutazione dei sistemi di logging; e) monitoraggio del traffico di rete; f) implementazione delle misure ACN; g) segnalazione di incidenti al Responsabile IA e al DPO; h) partecipazione agli audit.

© Armin Wieser

(3) Ogni verifica tecnica deve essere documentata.

3.4 Direzione

(1) La Direzione approva il regolamento e garantisce le risorse necessarie. (2) Vigila sulla corretta attuazione della governance. (3) Decide sulle violazioni gravi.

3.5 Personale

(1) Il personale deve rispettare la Policy IA, utilizzare solo strumenti approvati e segnalare eventuali casi di Shadow AI. (2) È obbligatoria la partecipazione alle formazioni. (3) Le violazioni possono comportare misure disciplinari.

3.6 Fornitori esterni

(1) I fornitori devono accettare contrattualmente la Policy IA. (2) Devono documentare l'uso degli strumenti IA. (3) Le violazioni possono comportare la risoluzione del contratto.

CAPITOLO 4 – Policy per l'uso dell'Intelligenza Artificiale

4.1 Principi generali

(1) L'utilizzo dei sistemi di IA generativa deve rispettare i principi di minimizzazione dei dati, limitazione della finalità, trasparenza, sicurezza e supervisione umana. (2) Ogni utilizzo deve essere documentato, tracciabile e verificabile. (3) Il Titolare si impegna a garantire un impiego responsabile e conforme dei sistemi di IA.

4.2 Utilizzi consentiti

(1) Sono consentiti: a) bozze di testi privi di dati personali; b) traduzioni di contenuti non riservati; c) attività di brainstorming e strutturazione di idee; d) funzioni di assistenza interna, purché conformi al GDPR.

(2) Ogni utilizzo consentito deve essere registrato nel Registro IA. (3) Il Titolare promuove una cultura di utilizzo responsabile dell'IA.

4.3 Divieti

(1) È severamente vietato: a) inserire dati personali nei sistemi IA; b) caricare documenti interni riservati; c) utilizzare account IA privati per attività lavorative; d) impiegare strumenti IA non presenti nella lista degli strumenti approvati; e) adottare decisioni automatizzate senza supervisione umana; f) utilizzare sistemi IA che trasferiscono dati verso Paesi terzi senza adeguate garanzie.

(2) Le violazioni comportano misure disciplinari.

4.4 Trasparenza e documentazione

(1) Ogni utilizzo dell'IA deve essere documentato. (2) I contenuti generati con supporto IA devono essere chiaramente indicati. (3) Il Titolare mantiene un Registro IA che raccoglie tutte le attività. (4) La trasparenza garantisce tracciabilità verso utenti e autorità.

4.5 Gestione dei dati personali e riservati

(1) L'inserimento di dati personali o informazioni riservate nei sistemi IA generativa è vietato. (2) Le violazioni comportano misure disciplinari. (3) Il Titolare garantisce il pieno rispetto del GDPR.

4.6 Uso di account IA privati

(1) L'uso di account IA privati per scopi lavorativi è vietato. (2) Tale comportamento è considerato Shadow AI.

4.7 Indicazione dei contenuti generati con IA

(1) I contenuti generati con supporto IA devono essere accompagnati da un'indicazione esplicita. (2) L'obbligo di indicazione garantisce trasparenza verso utenti e autorità.

CAPITOLO 5 – Procedura di approvazione degli strumenti di Intelligenza Artificiale

5.1 Presentazione della richiesta

(1) Chiunque desideri utilizzare uno strumento di IA all'interno dell'organizzazione deve presentare una richiesta formale prima dell'avvio dell'utilizzo. Tale richiesta è obbligatoria per garantire la conformità ai requisiti legali, organizzativi e tecnici.

(2) La richiesta deve contenere almeno: a) una descrizione dettagliata della finalità prevista, degli obiettivi, dei risultati attesi e del tipo di informazioni trattate; b) un elenco completo delle categorie di dati coinvolti, specificando se sono presenti dati personali o informazioni riservate; c) una valutazione dei rischi, con particolare riferimento a privacy, sicurezza informatica, integrità istituzionale e impatti operativi; d) una descrizione tecnica dello strumento, incluse informazioni sul fornitore, modalità di trattamento dei dati, luoghi di conservazione, struttura delle API e misure di sicurezza; e) una dichiarazione relativa a eventuali trasferimenti verso Paesi terzi e alle garanzie previste dal GDPR; f) una conferma che il richiedente ha letto e compreso la Policy IA.

(3) La richiesta deve essere presentata tramite il portale interno di governance IA. (4) Le richieste incomplete non vengono elaborate e sono considerate non valide.

5.2 Valutazione del Responsabile IA

(1) Il Responsabile IA valuta la richiesta considerando aspetti legali, tecnici, organizzativi ed etici.

(2) La valutazione comprende: a) analisi della finalità e dei rischi istituzionali; b) verifica delle categorie di dati coinvolti; c) valutazione della risk analysis del richiedente; d) esame della descrizione tecnica dello strumento; e) verifica delle misure di sicurezza; f) controllo della conformità a GDPR, AI Act, Garante Privacy e ACN.

(3) Il Responsabile IA può richiedere informazioni aggiuntive. (4) La valutazione deve essere documentata nel Registro IA.

5.3 Valutazione del DPO

(1) Il DPO verifica la conformità della richiesta al GDPR.

(2) La valutazione comprende: a) minimizzazione dei dati e limitazione della finalità; b) verifica della base giuridica ai sensi dell'art. 6 GDPR; c) controllo delle misure di sicurezza (art. 32 GDPR); d) verifica dei trasferimenti verso Paesi terzi; e) valutazione della necessità di una DPIA; f) controllo del rispetto del principio di Privacy by Design.

(3) Il DPO può vietare l'utilizzo se emergono rischi per la protezione dei dati. (4) La valutazione deve essere documentata.

5.4 Verifica tecnica (IT)

(1) Il Responsabile IT verifica la sicurezza tecnica dello strumento.

(2) La verifica comprende: a) sicurezza delle API; b) modalità di trasmissione dei dati; c) controllo degli accessi; d) sistemi di logging; e) analisi della comunicazione di rete; f) misure tecniche previste dall'ACN.

(3) Il Responsabile IT può vietare l'utilizzo se emergono rischi tecnici. (4) La verifica deve essere documentata.

5.5 Decisione (approvazione, approvazione con condizioni, rifiuto)

(1) La decisione finale è presa dal Responsabile IA dopo tutte le verifiche. (2) Le possibili decisioni sono: a) approvazione; b) approvazione con condizioni; c) rifiuto.

(3) Le condizioni possono includere: a) limitazioni d'uso; b) misure di sicurezza aggiuntive; c) formazione obbligatoria; d) controlli periodici.

(4) La decisione deve essere documentata e comunicata al richiedente.

5.6 Registrazione nel Registro IA

(1) Ogni approvazione deve essere registrata nel Registro IA. (2) Il Registro IA contiene: a) la richiesta; b) le valutazioni; c) la decisione; d) eventuali condizioni; e) la cronologia d'uso; f) eventuali revoche.

5.7 Revoca dell'approvazione

(1) L'approvazione può essere revocata in qualsiasi momento se emergono nuovi rischi. (2) La revoca deve essere documentata e comunicata all'utente.

CAPITOLO 6 – Regole operative per il personale

6.1 Comportamenti consentiti (Do)

(1) Il personale è tenuto a rispettare rigorosamente i principi, le procedure e le limitazioni stabilite nel presente regolamento per l'uso dei sistemi di IA generativa.

(2) In particolare, il personale deve:

a) **Utilizzare esclusivamente strumenti IA approvati** È consentito utilizzare solo strumenti che sono stati valutati, approvati e inseriti nella lista ufficiale degli strumenti autorizzati.

b) **Conoscere la Policy IA prima dell'utilizzo** Prima di utilizzare qualsiasi strumento IA, il personale deve leggere integralmente la Policy IA e confermare di averla compresa.

c) **Valutare criticamente i risultati dell'IA** I contenuti generati dall'IA devono essere sempre verificati con attenzione, valutati criticamente e confrontati con competenze professionali.

d) **Non inserire dati personali o riservati** Il personale deve assicurarsi che nei sistemi IA non vengano inseriti dati personali, informazioni interne riservate o dati particolarmente sensibili.

e) **Documentare l'utilizzo dell'IA** Ogni utilizzo rilevante deve essere registrato nel Registro IA o negli strumenti di documentazione previsti.

f) **Segnalare anomalie o sospetti di Shadow AI** Qualsiasi anomalia, sospetto di uso non autorizzato o incidente deve essere segnalato immediatamente al Responsabile IA o all'IT.

g) **Partecipare alle formazioni obbligatorie** Il personale deve partecipare alle attività formative previste e applicare le conoscenze acquisite.

(3) La violazione delle regole "Do" può comportare misure disciplinari.

6.2 Comportamenti vietati (Don't)

(1) Oltre ai comportamenti richiesti, esistono divieti chiari e vincolanti.

(2) È severamente vietato:

a) **Inserire dati personali** Nomi, indirizzi, contatti, dati sanitari, dati sociali, informazioni sul personale o qualsiasi dato personale non possono essere inseriti nei sistemi IA.

b) **Caricare documenti riservati** Documenti interni, contratti, verbali, email, report finanziari o altri contenuti riservati non possono essere caricati o utilizzati come prompt.

c) **Utilizzare account IA privati per scopi lavorativi** L'uso di account personali (es. ChatGPT privato, Copilot privato) per attività lavorative è vietato e considerato Shadow AI.

d) **Usare strumenti IA non approvati** È vietato utilizzare strumenti IA che non figurano nella lista degli strumenti autorizzati.

e) **Delegare decisioni automatizzate all'IA senza supervisione umana** L'IA non può prendere decisioni operative o istituzionali senza una verifica umana qualificata.

f) **Eludere misure tecniche di sicurezza** È vietato aggirare, manipolare o disattivare controlli tecnici, limitazioni di accesso o sistemi di monitoraggio.

(3) Le violazioni delle regole "Don't" sono considerate gravi e possono comportare conseguenze disciplinari.

6.3 Gestione di errori e allucinazioni dell'IA

(1) I sistemi IA possono generare contenuti errati, incompleti o inventati ("allucinazioni"). Il personale deve esserne consapevole e adottare misure adeguate.

(2) In particolare:

a) **Verificare la plausibilità dei risultati** Ogni output IA deve essere controllato per coerenza, correttezza e plausibilità.

b) **Confrontare con fonti primarie** Per contenuti giuridici, tecnici o sensibili è obbligatorio confrontare i risultati con fonti ufficiali.

c) **Non accettare risultati IA senza valutazione umana** I contenuti IA sono suggerimenti, non verità: richiedono sempre una valutazione professionale.

d) **Documentare errori rilevanti** Errori gravi o ricorrenti devono essere documentati e segnalati al Responsabile IA.

(3) La capacità di valutare criticamente l'IA è considerata parte essenziale della governance.

6.4 Obbligo di segnalazione di casi di Shadow AI

(1) I casi di Shadow AI comprendono qualsiasi utilizzo non autorizzato di sistemi IA.

(2) Il personale deve segnalare immediatamente:

a) uso di account IA privati per scopi lavorativi; b) uso di strumenti IA non approvati; c) inserimento di dati personali o riservati nei sistemi IA; d) elusione di misure tecniche di sicurezza; e) sospetti di utilizzo non autorizzato da parte di terzi.

(3) Le segnalazioni devono essere dettagliate e inviate al Responsabile IA o all'IT.

(4) Le segnalazioni non comportano conseguenze negative per chi le effettua, salvo dolo o violazioni intenzionali.

6.5 Uso di contenuti IA in documenti ufficiali

(1) I documenti ufficiali (rapporti, pareri, comunicazioni interne o esterne, linee guida) possono contenere contenuti generati con IA solo se:

a) tali contenuti sono stati verificati professionalmente; b) la responsabilità del contenuto è chiaramente attribuita a una persona; c) l'utilizzo dell'IA è documentato nel Registro IA.

(2) Per documenti sensibili (pareri legali, documenti di compliance, rapporti di protezione dati) l'uso dell'IA deve essere particolarmente limitato.

(3) Il Titolare può vietare completamente l'uso dell'IA per specifiche tipologie di documenti.

CAPITOLO 7 – Conformità al GDPR nell'uso dell'Intelligenza Artificiale

7.1 Minimizzazione dei dati e limitazione della finalità

(1) Il trattamento dei dati connesso all'uso di sistemi di IA generativa deve rispettare i principi di minimizzazione dei dati e limitazione della finalità previsti dall'art. 5, par. 1, lett. b e c del GDPR.

(2) **Minimizzazione dei dati** significa che possono essere trattati solo i dati strettamente necessari per la finalità specifica dell'utilizzo dell'IA.

(3) **Limitazione della finalità** significa che il trattamento deve avvenire esclusivamente per lo scopo indicato nella richiesta di approvazione (Capitolo 5.1) e autorizzato dal Titolare.

(4) Una modifica della finalità è consentita solo se: a) viene definito un nuovo scopo in modo chiaro; b) esiste una nuova base giuridica ai sensi dell'art. 6 GDPR; c) il Responsabile IA e il DPO effettuano una nuova valutazione; d) la modifica viene documentata nel Registro IA.

(5) Il Titolare vieta espressamente l'uso di sistemi di IA generativa per trattare dati personali, salvo che esista una base giuridica esplicita e che il trattamento avvenga tramite sistemi interni completamente sotto il controllo del Titolare.

(6) Il personale deve verificare, prima di ogni utilizzo, che i dati inseriti rispettino il principio di minimizzazione.

7.2 Privacy by Design & Default

(1) Il Titolare si impegna a garantire che ogni utilizzo dell'IA sia progettato secondo il principio di **Privacy by Design & Default** (art. 25 GDPR).

(2) **Privacy by Design** implica che gli aspetti di protezione dei dati siano considerati fin dalla fase di progettazione, selezione e implementazione dei sistemi IA.

(3) **Privacy by Default** implica che le impostazioni più rispettose della privacy siano attivate come predefinite.

(4) L'attuazione comprende: a) misure tecniche per evitare trattamenti non necessari; b) limitazione degli accessi al minimo indispensabile; c) anonimizzazione o pseudonimizzazione dei dati, ove possibile; d) uso di tecnologie di cifratura; e) verifiche periodiche della conformità; f) documentazione delle misure nel Registro IA.

(5) Il DPO supervisiona l'applicazione di tali principi e può imporre misure correttive.

7.3 Sicurezza del trattamento (Art. 32 GDPR)

(1) Il Titolare garantisce la sicurezza del trattamento mediante misure tecniche e organizzative adeguate, ai sensi dell'art. 32 GDPR.

(2) Le misure comprendono: a) cifratura dei dati in transito e a riposo; b) controlli di accesso che limitano l'uso dell'IA a personale autorizzato; c) registrazione e tracciamento degli accessi; d) aggiornamenti e patch di sicurezza regolari; e) monitoraggio della rete per rilevare anomalie; f) protezione contro accessi non autorizzati, perdita o manipolazione dei dati.

(3) Il Responsabile IT è incaricato dell'attuazione e documentazione delle misure.

(4) In caso di incidenti di sicurezza, il Responsabile IA e il DPO devono essere informati immediatamente.

7.4 Trasferimenti verso Paesi terzi

(1) Se, nell'ambito dell'uso dell'IA, vengono trasferiti dati verso Paesi terzi, tali trasferimenti devono rispettare gli artt. 44–49 GDPR.

(2) Il Titolare verifica che: a) il Paese terzo disponga di una decisione di adeguatezza; b) siano adottate garanzie adeguate (es. SCC, BCR); c) siano implementate misure supplementari tecniche e organizzative; d) il trasferimento sia documentato nel Registro IA.

(3) In assenza di garanzie adeguate, il trasferimento è vietato.

7.5 Valutazione d'impatto sulla protezione dei dati (DPIA)

(1) Per sistemi IA che comportano rischi elevati per i diritti e le libertà degli interessati, è obbligatoria una DPIA ai sensi dell'art. 35 GDPR.

(2) La DPIA deve valutare: a) natura, ambito e finalità del trattamento; b) rischi per gli interessati; c) misure tecniche e organizzative previste; d) necessità di consultazione preventiva con il Garante Privacy.

(3) Il DPO coordina la DPIA e può imporre misure correttive o vietare l'uso dello strumento IA.

7.6 Obblighi documentali verso il Garante Privacy

(1) Il Titolare garantisce la disponibilità di tutta la documentazione relativa all'uso dell'IA, incluse: a) Registro IA; b) DPIA; c) valutazioni tecniche; d) misure di sicurezza; e) segnalazioni di incidenti.

(2) La documentazione deve essere fornita al Garante Privacy su richiesta.

CAPITOLO 8 – Conformità all'AI Act

8.1 Classificazione del rischio dei sistemi IA

(1) Il Titolare valuta ogni sistema di IA in base alla classificazione del rischio prevista dall'AI Act. (2) La classificazione considera: a) finalità del sistema; b) impatti potenziali sui diritti fondamentali; c) livello di autonomia decisionale; d) contesto operativo; e) possibilità di danni fisici, psicologici, economici o reputazionali. (3) I sistemi IA sono classificati come:

- **vietati**,
- **ad alto rischio**,
- **a rischio limitato**,
- **a rischio minimo**. (4) La classificazione determina gli obblighi applicabili.

8.2 Obblighi per sistemi IA ad alto rischio

(1) I sistemi IA classificati come **ad alto rischio** devono rispettare requisiti stringenti previsti dall'AI Act. (2) Tali requisiti includono: a) gestione del rischio; b) qualità dei dati e governance dei dataset; c) documentazione tecnica completa; d) registrazione e tracciabilità; e) trasparenza e informazioni agli utenti; f) supervisione umana; g) robustezza, sicurezza e accuratezza; h) monitoraggio continuo delle prestazioni. (3) Il Titolare garantisce che tali requisiti siano implementati prima dell'uso. (4) L'uso di sistemi ad alto rischio senza conformità è vietato.

8.3 Obblighi di trasparenza

(1) Il Titolare garantisce che gli utenti siano informati quando interagiscono con sistemi IA generativa. (2) È obbligatorio indicare chiaramente: a) che il contenuto è stato generato o assistito da IA; b) eventuali limitazioni

del sistema; c) rischi di errore o allucinazione; d) modalità di supervisione umana. (3) Per sistemi che generano contenuti destinati a terzi, la trasparenza deve essere esplicita e verificabile.

8.4 Supervisione umana

(1) L'AI Act richiede che i sistemi IA siano soggetti a supervisione umana adeguata. (2) La supervisione deve garantire che: a) l'IA non prenda decisioni autonome senza controllo; b) gli operatori possano intervenire, correggere o interrompere il sistema; c) i risultati siano valutati criticamente; d) eventuali rischi siano identificati tempestivamente. (3) Il Titolare assicura che la supervisione sia svolta da personale qualificato.

8.5 Pratiche IA vietate

(1) Il Titolare vieta qualsiasi utilizzo di IA che rientri nelle pratiche proibite dall'AI Act, tra cui: a) manipolazione cognitiva o comportamentale che possa causare danni; b) sistemi di identificazione biometrica in tempo reale in spazi pubblici (salvo eccezioni legali); c) classificazione delle persone basata su caratteristiche sensibili; d) sistemi che sfruttano vulnerabilità di gruppi specifici (minori, disabili, ecc.). (2) L'uso di tali pratiche comporta sanzioni immediate e segnalazione alle autorità competenti.

8.6 Valutazione di conformità e dimostrazione

(1) Il Titolare garantisce che ogni sistema IA soggetto a obblighi di conformità sia sottoposto alle verifiche previste dall'AI Act. (2) La valutazione comprende: a) analisi tecnica; b) verifica dei requisiti di sicurezza; c) controllo della documentazione; d) audit interni; e) eventuali audit esterni. (3) Il Titolare mantiene evidenze documentali che dimostrano la conformità. (4) La documentazione deve essere disponibile per le autorità competenti.

CAPITOLO 9 – Sistema di controllo basato sul rischio

9.1 Piano dei controlli

(1) Il Titolare adotta un piano di controlli strutturato e basato sul rischio, volto a garantire un uso conforme, sicuro e documentato dei sistemi di IA. (2) Il piano definisce frequenza, responsabilità, strumenti di verifica e criteri di valutazione. (3) I controlli comprendono verifiche tecniche, organizzative, documentali e di conformità normativa.

9.2 Rilevazione della Shadow AI (monitoraggio, log, rete)

(1) Il Titolare implementa misure tecniche per individuare utilizzi non autorizzati di IA ("Shadow AI"). (2) Le misure comprendono: a) analisi dei log di sistema; b) monitoraggio del traffico di rete; c) rilevazione di accessi a piattaforme IA non autorizzate; d) strumenti di alerting per comportamenti anomali. (3) Eventuali anomalie devono essere analizzate dal Responsabile IT e segnalate al Responsabile IA.

9.3 Verifica della lista degli strumenti approvati

(1) Il Titolare mantiene una lista aggiornata degli strumenti IA approvati. (2) La lista è soggetta a controlli periodici per verificare: a) conformità tecnica; b) conformità normativa; c) rispetto delle condizioni di approvazione; d) eventuali nuovi rischi. (3) Gli strumenti non conformi possono essere sospesi o rimossi.

9.4 Controlli interni

(1) Il Titolare effettua controlli interni regolari per verificare il rispetto della Policy IA. (2) I controlli comprendono: a) audit documentali; b) verifiche sull'uso effettivo degli strumenti IA; c) controlli sulle registrazioni nel Registro IA; d) verifiche sulla formazione del personale. (3) Le irregolarità devono essere documentate e gestite secondo le procedure di escalation.

9.5 Controlli esterni (revisione, autorità)

(1) Il Titolare può essere soggetto a controlli esterni da parte di revisori indipendenti o autorità competenti (Garante Privacy, ACN, altre autorità). (2) Il Titolare garantisce piena collaborazione e mette a disposizione la

documentazione richiesta. (3) Le raccomandazioni derivanti dai controlli esterni devono essere implementate tempestivamente.

9.6 Procedure di escalation in caso di violazioni

(1) In caso di violazioni della Policy IA o di rischi significativi, si applicano procedure di escalation definite. (2) Le fasi comprendono: a) segnalazione immediata al Responsabile IA; b) valutazione preliminare del rischio; c) coinvolgimento del DPO e dell'IT, se necessario; d) informazione alla Direzione in caso di violazioni gravi; e) attuazione di misure correttive e preventive. (3) Le violazioni devono essere documentate nel Registro IA e, se richiesto, comunicate alle autorità competenti.

CAPITOLO 10 – Documentazione e gestione dei registri

10.1 Registro IA

(1) Il Titolare mantiene un **Registro IA** che documenta tutte le attività legate all'uso dei sistemi di Intelligenza Artificiale. (2) Il Registro IA contiene informazioni su: a) strumenti approvati; b) richieste di utilizzo; c) valutazioni tecniche, legali e organizzative; d) decisioni di approvazione o rifiuto; e) condizioni imposte; f) cronologia d'uso; g) incidenti e segnalazioni; h) revoche. (3) Il Registro IA deve essere aggiornato regolarmente e mantenuto in modo conforme ai requisiti del GDPR e dell'AI Act.

10.2 Lista degli strumenti approvati

(1) Il Titolare mantiene una **lista ufficiale degli strumenti IA approvati**, aggiornata e verificata periodicamente. (2) La lista include: a) nome dello strumento; b) fornitore; c) versione; d) finalità autorizzate; e) condizioni o limitazioni d'uso; f) data di approvazione; g) eventuali revoche. (3) Solo gli strumenti presenti in questa lista possono essere utilizzati dal personale.

10.3 Rapporti di audit

(1) Il Titolare redige rapporti di audit periodici relativi all'uso dell'IA. (2) I rapporti includono: a) risultati dei controlli interni; b) verifiche tecniche e organizzative; c) valutazioni di conformità; d) raccomandazioni e misure correttive; e) esiti di audit esterni. (3) I rapporti devono essere conservati e messi a disposizione delle autorità competenti su richiesta.

10.4 Attestati di formazione

(1) Il Titolare documenta la partecipazione del personale alle attività formative previste dal Capitolo 11. (2) Gli attestati di formazione includono: a) nome del partecipante; b) data della formazione; c) contenuti trattati; d) eventuali verifiche o test; e) obblighi formativi futuri. (3) La documentazione deve essere conservata per dimostrare la conformità ai requisiti normativi.

10.5 Registro delle segnalazioni di Shadow AI

(1) Il Titolare mantiene un **Registro delle segnalazioni di Shadow AI**, che raccoglie tutti i casi di utilizzo non autorizzato o sospetto di IA. (2) Il registro contiene: a) descrizione del caso; b) data e ora della segnalazione; c) persona che ha segnalato; d) valutazione del Responsabile IA; e) misure adottate; f) eventuali comunicazioni alle autorità. (3) Il registro è parte integrante del sistema di controllo interno.

10.6 Tempi di conservazione

(1) Il Titolare definisce tempi di conservazione specifici per ogni categoria documentale relativa all'IA. (2) I tempi di conservazione devono rispettare: a) GDPR; b) Codice Privacy; c) AI Act; d) normative nazionali e settoriali; e) esigenze operative e di audit. (3) Al termine del periodo di conservazione, la documentazione deve essere eliminata in modo sicuro.

© Armin Wieser

CAPITOLO 11 – Formazione e sensibilizzazione

11.1 Piano formativo

(1) Il Titolare adotta un piano formativo strutturato per garantire che tutto il personale comprenda i rischi, le opportunità e le regole relative all'uso dei sistemi di IA generativa. (2) Il piano formativo definisce: a) contenuti obbligatori; b) modalità di erogazione (in presenza, online, moduli interattivi); c) frequenza delle sessioni; d) responsabilità dei formatori; e) criteri di valutazione dell'apprendimento. (3) La formazione è parte integrante della governance IA.

11.2 Formazioni obbligatorie

(1) Tutto il personale deve partecipare alle formazioni obbligatorie sull'uso dell'IA. (2) Le formazioni coprono almeno: a) principi fondamentali dell'IA generativa; b) rischi di privacy e sicurezza; c) regole "Do & Don't"; d) gestione delle allucinazioni dell'IA; e) obblighi di documentazione; f) procedure di segnalazione dei casi di Shadow AI. (3) La partecipazione è registrata e verificata periodicamente.

11.3 Materiali di sensibilizzazione

(1) Il Titolare mette a disposizione materiali di sensibilizzazione per promuovere un uso consapevole dell'IA. (2) I materiali possono includere: a) linee guida sintetiche; b) poster informativi; c) video formativi; d) FAQ; e) esempi di buone pratiche; f) avvisi sui rischi più comuni. (3) I materiali devono essere aggiornati regolarmente.

11.4 Documentazione della partecipazione

(1) La partecipazione alle attività formative deve essere documentata. (2) La documentazione include: a) nome del partecipante; b) data della formazione; c) contenuti trattati; d) eventuali verifiche o test; e) obblighi formativi futuri. (3) La documentazione è conservata per dimostrare la conformità ai requisiti normativi.

11.5 Formazioni periodiche

(1) Il Titolare organizza formazioni periodiche per garantire che il personale sia aggiornato sulle evoluzioni normative e tecnologiche. (2) Le formazioni periodiche sono obbligatorie per: a) personale che utilizza strumenti IA; b) dirigenti; c) Responsabile IA; d) DPO; e) Responsabile IT. (3) Le sessioni periodiche possono includere aggiornamenti sull'AI Act, nuove minacce informatiche, nuove policy interne o nuovi strumenti approvati.

CAPITOLO 12 – Sanzioni e misure in caso di violazioni

12.1 Sanzioni interne

(1) Le violazioni del presente regolamento sull'uso dell'IA possono comportare sanzioni interne proporzionate alla gravità del comportamento. (2) Le sanzioni possono includere: a) avvertimenti formali; b) richiami disciplinari; c) sospensione temporanea di attività o incarichi; d) misure correttive obbligatorie; e) segnalazione alla Direzione. (3) Le sanzioni sono applicate nel rispetto delle normative sul lavoro e delle procedure interne.

12.2 Limitazione dei diritti di accesso

(1) In caso di violazioni, il Titolare può limitare o revocare i diritti di accesso ai sistemi informatici e agli strumenti IA. (2) Le limitazioni possono includere: a) sospensione dell'accesso agli strumenti IA; b) restrizioni su specifiche funzionalità; c) obbligo di supervisione per ogni utilizzo; d) blocco temporaneo dell'account. (3) Le misure sono documentate nel Registro IA.

12.3 Misure disciplinari

(1) Le violazioni gravi, in particolare l'uso intenzionale di Shadow AI, l'inserimento di dati personali o riservati nei sistemi IA o l'elusione di misure tecniche di sicurezza, possono comportare misure disciplinari severe. (2) Le misure possono includere: a) sospensione; b) trasferimento di mansioni; c) riduzione delle responsabilità; d)

risoluzione del rapporto di lavoro nei casi più gravi. (3) Ogni misura disciplinare deve essere proporzionata e motivata.

12.4 Segnalazione alla Direzione

(1) Le violazioni che comportano rischi significativi per la sicurezza, la protezione dei dati o la conformità normativa devono essere segnalate alla Direzione. (2) La Direzione valuta: a) la gravità dell'incidente; b) le misure correttive necessarie; c) eventuali obblighi di notifica verso autorità o terzi; d) responsabilità interne. (3) La Direzione può imporre misure aggiuntive o avviare indagini interne.

12.5 Sanzioni esterne (Garante Privacy, AI Act, ACN)

(1) Le violazioni che comportano rischi per la protezione dei dati o per la sicurezza informatica possono essere soggette a sanzioni da parte delle autorità competenti, tra cui: a) **Garante per la Protezione dei Dati Personali**; b) **autorità competenti per l'AI Act**; c) **Agenzia per la Cybersicurezza Nazionale (ACN)**.

(2) Le sanzioni esterne possono includere: a) multe amministrative; b) ordini di sospensione o limitazione dell'uso dell'IA; c) obblighi di adeguamento; d) audit obbligatori; e) responsabilità civili o penali nei casi più gravi.

(3) Il Titolare collabora pienamente con le autorità e attua tempestivamente le misure richieste.

CAPITOLO 13 – Entrata in vigore e aggiornamento

13.1 Entrata in vigore

(1) Il presente regolamento entra in vigore alla data stabilita dalla Direzione. (2) A partire da tale data, tutte le persone che operano all'interno dell'organizzazione sono tenute a rispettarne integralmente le disposizioni. (3) L'entrata in vigore deve essere comunicata formalmente a tutto il personale e ai fornitori esterni.

13.2 Revisione annuale

(1) Il regolamento è soggetto a revisione almeno una volta all'anno. (2) La revisione comprende: a) valutazione dell'efficacia delle misure adottate; b) analisi dei rischi emergenti; c) aggiornamento delle procedure operative; d) verifica della conformità alle normative vigenti. (3) Le revisioni devono essere documentate e approvate dalla Direzione.

13.3 Adeguamento alle nuove normative

(1) Il Titolare si impegna ad adeguare tempestivamente il regolamento in caso di modifiche legislative o regolamentari rilevanti, incluse: a) aggiornamenti del GDPR; b) modifiche o nuove disposizioni dell'AI Act; c) provvedimenti del Garante Privacy; d) linee guida dell'ACN; e) normative nazionali o settoriali. (2) Gli aggiornamenti devono essere comunicati al personale e ai fornitori esterni. (3) Se necessario, il Titolare può introdurre misure transitorie per garantire la continuità operativa.

13.4 Responsabilità degli aggiornamenti

(1) Il Responsabile IA è incaricato di monitorare l'evoluzione normativa e tecnologica e di proporre aggiornamenti del regolamento. (2) Il DPO e il Responsabile IT collaborano alla valutazione degli impatti legali e tecnici. (3) La Direzione approva gli aggiornamenti e garantisce le risorse necessarie per la loro attuazione. (4) Ogni aggiornamento deve essere documentato nel Registro IA.

© Armin Wieser