

Grundrechte-Folgenabschätzung nach Artikel 27

Die sechs Pflichtinhalte, gespiegelt an der Modellakte — mit Bewertungsmatrix

Die Verordnung (EU) 2024/1689 kommt regulierten Finanzinstituten an vielen Stellen entgegen. Das Risikomanagement nach Artikel 9 darf Teil der bestehenden Verfahren sein (Absatz 10), das Qualitätsmanagementsystem gilt für Anbieter, die Finanzinstitute sind, weitgehend über die interne Governance als erfüllt (Artikel 17 Absatz 4), die Überwachungspflicht des Betreibers ebenso (Artikel 26 Absatz 5), und die Protokolle sind schlicht Teil der ohnehin geführten Dokumentation (Artikel 26 Absatz 6).

Artikel 27 enthält keine solche Klausel. Die Grundrechte-Folgenabschätzung ist damit das eine Artefakt, für das die Modellakte keine Vorlage bietet — auch dort, wo Material aus anderen Beständen des Hauses einfließt. Die einzige Anschlussmöglichkeit, die die Vorschrift selbst bietet, führt nicht zur Modellvalidierung, sondern zur Datenschutz-Folgenabschätzung; der Digital-Omnibus hat genau diese Verbindung im Juli 2026 noch etwas erweitert.

Einsatzbereich	Ein Arbeitsgerüst für den ersten Durchlauf: Schritt 0 grenzt den Anwendungsbereich ab, die Abschnitte 1 bis 6 führen durch die sechs Pflichtinhalte des Artikels 27 Absatz 1, Abschnitt 7 durch die Bewertung und die Restrisikoentscheidung, die Abschnitte 8 bis 10 durch Mitteilung, Aktualisierung und Zeichnung.
Abgrenzung	Kein Muster für den Fragebogen des Büros für Künstliche Intelligenz — dieser liegt noch nicht vor. Keine Rechtsberatung im Einzelfall. Und bewusst kein Verfahren zur Anpassung des Modells: Bei internen Modellen ist das ein aufsichtlich relevanter Vorgang eigener Art und gehört nicht in ein Prüfgerüst.
Zu den Zeilen	Die Zeile „Noch zu belegen“ benennt die fachlich geeignete Evidenz für den jeweiligen Pflichtinhalt, nicht einen gesetzlich vorgeschriebenen Kennzahlenkatalog. Artikel 27 bestimmt den Prüfgegenstand; die Methode wählt das Haus — und begründet sie.
Rechtsstand	Verordnung (EU) 2024/1689 in der Fassung der Verordnung (EU) 2026/1744 (Digital-Omnibus zur KI), in Kraft seit dem 27. Juli 2026. Artikel 27 steht in Kapitel III Abschnitt 3 und ist für Anhang-III-Systeme ab dem 2. Dezember 2027 anwendbar. Für Systeme, die davor bereits im Einsatz sind, gelten die Übergangsregelungen des Artikels 111, die im Kern an wesentliche Änderungen anknüpfen — jede substanzielle Modellüberarbeitung stellt die Frage neu.

Zur Reihenfolge: Für die Buchstaben c und d ist eine Datengrundlage erforderlich, die sich rückwirkend häufig nur unvollständig herstellen lässt. Wer die gruppendifferenzierte Ergebnismessung erst zum Anwendungsstichtag aufsetzt, hat einen Querschnitt und keine Zeitreihe — und damit keine Aussage darüber, ob sich ein gemessener Unterschied verfestigt oder abbaut. Der Aufwand für den ersten Durchlauf ist überschaubar; der Wert entsteht in der Wiederholung.

System / Modell	Institut / Bereich	Bearbeitungsstand vom
-----------------	--------------------	-----------------------

Schritt 0 Anwendungsbereich abgrenzen, statt ihn zu vermuten

Artikel 27 Absatz 1 trifft Betreiber von Hochrisiko-KI-Systemen nach Anhang III Nummer 5 Buchstaben b und c – unabhängig von Rechtsform und Trägerschaft. Die Reichweite ist enger, als sie im ersten Zugriff wirkt, und dort, wo sie greift, nicht verhandelbar.

Im Anwendungsbereich

- ☐ Kreditwürdigkeitsprüfung oder Bonitätsbewertung **natürlicher Personen** (Anhang III Nr. 5 Buchst. b).
- ☐ Risikobewertung oder Preisbildung gegenüber **natürlichen Personen** in der **Lebens- oder Krankenversicherung** (Anhang III Nr. 5 Buchst. c).

Außerhalb des Anwendungsbereichs – ausdrücklich notieren

- ☐ Systeme zur **Aufdeckung von Finanzbetrug** (Ausnahme in Nr. 5 Buchst. b). Die Ausnahme trägt nur, wenn die Zweckbestimmung tatsächlich die Betrugserkennung ist.
- ☐ Kreditwürdigkeitsprüfung **juristischer Personen**.
- ☐ Versicherungssparten **außerhalb Leben und Kranken** – Kraftfahrt, Sach, Haftpflicht sind von Nr. 5 Buchst. c nicht erfasst.

Profiling prüfen	Nimmt das System ein Profiling natürlicher Personen vor, gilt es stets als hochriskant – der Filter des Artikels 6 Absatz 3 steht dann nicht offen. Bonitätsscoring und individualisierte Risiko- oder Prämienbewertung erfüllen den Profiling-Begriff regelmäßig; ob er im Einzelfall erfüllt ist, richtet sich nach der konkreten Funktionsweise und den verarbeiteten Merkmalen.
Rolle prüfen	Die Pflicht trifft den Betreiber, nicht den Anbieter. Wer ein Modell einer Auskunftsei, eines Rechenzentrumsdienstleisters, einer Verbundgesellschaft oder eines spezialisierten Scoring- oder Softwareanbieters einsetzt, kann die Verantwortung für die Abschätzung nicht auf diesen übertragen. Die Anbieterinformationen nach Artikel 13 sind eine wesentliche Grundlage; die Abschätzung selbst schuldet das einsetzende Haus.

Betroffene Systeme (Anzahl / Bezeichnung)

Ausgenommen mit Begründung

Abschnitt

e 1–6

Die sechs Pflichtinhalte nach Artikel 27 Absatz 1

Die sechs Inhalte zerfallen in zwei Gruppen. Die Buchstaben a, e und f lassen sich aus vorhandenem Material aufbauen – mit Zuschnitt, Verweistechnik und einer Ergänzung bei f. Die Buchstaben b, c und d entstehen originär.

Verweisen erlaubt	Artikel 27 Absatz 4 lässt seit dem Digital-Omnibus Querverweise auf die einschlägigen Abschnitte der Datenschutz-Folgenabschätzung und die Übernahme von Teilen ausdrücklich zu. Für ein Scoringssystem liegt eine Datenschutz-Folgenabschätzung in aller Regel vor. Die erste Arbeitssitzung sollte deshalb Risikocontrolling, Fachbereich und Datenschutz gemeinsam einbeziehen.
--------------------------	--

Buchst. a Beschreibung der Verfahren, in denen das System zweckgemäß eingesetzt wird

Verlangt wird	Die Prozesse des Betreibers, in denen das System entsprechend seiner Zweckbestimmung verwendet wird.
Liegt meist vor	Arbeitsanweisungen, Kredit- beziehungsweise Annahmerichtlinie, Prozessdokumentation der Aufbau- und Ablauforganisation.
Noch zu belegen	Der Zuschnitt auf das konkrete System: an welcher Stelle im Prozess die Ausgabe greift, welche Entscheidung darauf gestützt wird, welche Alternativpfade bestehen. Vorhandenes Material ist prozess-, nicht systembezogen geschnitten.

Fundstelle im Haus

Verantwortlich

Stand / Status

Buchst. b Zeitraum und Häufigkeit der beabsichtigten Verwendung

Verlangt wird	Eine Beschreibung des Zeitraums, innerhalb dessen, und der Häufigkeit, mit der das System eingesetzt werden soll.
Liegt meist vor	In der Regel nichts Passendes. Die Modellakte kennt Gültigkeitszeiträume der Validierung – das ist etwas anderes als die beabsichtigte Einsatzdauer.
Noch zu belegen	Eine ausdrückliche Festlegung: Einsatzbeginn, vorgesehene Einsatzdauer, Entscheidungsvolumen je Periode, geplante Überprüfungszeitpunkte. Eine Nutzungsentscheidung, keine Modelleigenschaft – und deshalb von der Modellseite nicht zu liefern.

Fundstelle im Haus

Verantwortlich

Stand / Status

Buchst. c Kategorien betroffener natürlicher Personen und Personengruppen

Verlangt wird	Die Kategorien natürlicher Personen und Personengruppen, die von der Verwendung im spezifischen Kontext betroffen sein können.
Liegt meist vor	Portfoliosegmentierung, Anwendungsbereich, Zielpopulation.
Noch zu belegen	Risikoklassen sind keine Betroffenengruppen. Verlangt ist eine begründete Auswahl der im konkreten Verwendungskontext betroffenen Kategorien und Gruppen. Ausgangspunkt sind Artikel 21 der Charta der Grundrechte der Europäischen Union und die Merkmale des AGG – aber kein abschließender Katalog: Hinzu treten kontextbezogene und besonders verletzbare Gruppen, etwa Personen mit geringer Datenhistorie, mit atypischen Erwerbsverläufen oder in der Rolle als Mitdarlehensnehmer und Bürgen. Mittelbare, stellvertretende und intersektionale Betroffenheiten sind einzubeziehen. Festzulegen ist zugleich, welche Gruppen empirisch gemessen und welche qualitativ bewertet werden; für Merkmale ohne belastbare Datengrundlage ist die verbleibende Erkenntnisgrenze ausdrücklich zu dokumentieren.

Fundstelle im Haus

Verantwortlich

Stand / Status

Buchst. d Spezifische Schadensrisiken für die nach Buchstabe c bestimmten Gruppen

Verlangt wird	Die spezifischen Schadensrisiken für diese Gruppen, unter Berücksichtigung der vom Anbieter nach Artikel 13 bereitgestellten Informationen.
Liegt meist vor	Validierungsbericht mit Trennschärfe, Kalibrierung, Stabilität; Overridestatistik. Blickrichtung: Risiko des Instituts.
Noch zu belegen	Die Blickrichtung kehrt sich um – zu bewerten ist das Risiko der betroffenen Person. Fachlich geeignet und regelmäßig erforderlich: gruppendifferenzierte Ergebnis- und Fehlerverteilung, Ablehnungs- und Aufschlagsquoten je Gruppe, Entwicklung über die Zeit sowie eine dokumentierte Methodik einschließlich Fallzahlen, Unsicherheiten und Aussagegrenzen. Dies ist der daten- und methodenintensivste Teil der Abschätzung.

Fundstelle im Haus

Verantwortlich

Stand / Status

Zur Rechtsgrundlage	Der pauschale Einwand, besondere Kategorien personenbezogener Daten dürften für eine Verzerrungsanalyse unter keinen Umständen verarbeitet werden, greift seit Einführung des durch den Digital-Omnibus eingefügten Artikels 4a zu kurz: Dessen Absatz 2 erfasst ausdrücklich auch Betreiber. Die Vorschrift eröffnet jedoch keine allgemeine Erlaubnis zur Erhebung geschützter Merkmale, sondern eine eng auszulegende Ausnahme unter kumulativen Voraussetzungen und dem Maßstab der strikten Erforderlichkeit; sie ist ausweislich der Erwägungsgründe als Konkretisierung eines erheblichen öffentlichen Interesses im Sinne des Artikels 9 Absatz 2 Buchstabe g DSGVO zu lesen und nicht als eigenständige Erlaubnisnorm. Vor jeder Verarbeitung sind Zweck, Alternativlosigkeit, Datenumfang, Schutzmaßnahmen, Speicherdauer, Zugriffsberechtigungen und Löschung nachvollziehbar zu dokumentieren; regelmäßig ist auch die Datenschutz-Folgenabschätzung anzupassen. Die Vorschrift steht in Kapitel I und ist seit dem 27. Juli 2026 anwendbar – sie folgt der Verschiebung der Hochrisikopflichten nicht. Eine Pflicht zur Verzerrungserkennung begründet sie ausdrücklich nicht.
----------------------------	---

Buchst. e Umsetzung der Maßnahmen menschlicher Aufsicht

Verlangt wird	Eine Beschreibung der Umsetzung der Maßnahmen menschlicher Aufsicht entsprechend der Betriebsanleitung.
Liegt meist vor	Kompetenzordnung, Votierungs- und Zweitvotumsregelungen, Vier-Augen-Prinzip. Der Inhalt, bei dem regulierte Häuser am besten dastehen.
Noch zu belegen	Nachzuweisen ist nicht die Regelung, sondern ihre praktische Wirksamkeit. Artikel 14 Absatz 4 benennt die Prüfpunkte selbst: Verstehbarkeit der Systemausgabe, Bewusstsein für die Neigung zum automatischen Vertrauen in die Ausgabe, Befugnis zur abweichenden Entscheidung. Zu erheben sind daher Qualifikation, Befugnisse, verfügbare Informationen und Bearbeitungszeit der aufsichtführenden Personen sowie ausgewertete Übersteuerungs- und Eskalationsfälle mit ihrer Verteilung über Fälle, Mitarbeiter und Organisationseinheiten. Eine niedrige Übersteuerungsquote ist für sich genommen kein Beleg: Sie kann ein gut funktionierendes System anzeigen oder eine faktisch wirkungslose Aufsicht.

Fundstelle im Haus

Verantwortlich

Stand / Status

Buchst. f Maßnahmen bei Risikoeintritt, interne Governance und Beschwerdemechanismen

Verlangt wird	Die im Falle des Eintretens dieser Risiken zu ergreifenden Maßnahmen, einschließlich der Regelungen zur internen Unternehmensführung und der Beschwerdemechanismen.
Liegt meist vor	Beschwerdemanagement, Eskalationswege, Ombudsverfahren.
Noch zu belegen	Der fehlende Rückkanal: ein definierter Weg von Beschwerden, Übersteuerungen und sonstigen Auffälligkeiten über die Prüfung des Einzelfalls zurück in Modellmonitoring und Governance. Festzulegen sind die Zuordnung der Beschwerde zum konkret eingesetzten System, die individuelle Abhilfe – bei ausschließlich automatisierten Entscheidungen ergänzt um Artikel 22 Absatz 3 DSGVO, für den Erklärungsanspruch um Artikel 86 KI-VO –, Auslöseschwellen für eine systemische Untersuchung, der Eskalationsweg und die Zuständigkeit für Korrekturmaßnahmen. In der Praxis endet die Beschwerde meist im Kundenservice.

Fundstelle im Haus

Verantwortlich

Stand / Status

**Abschnitt
7 Bewertung und Restrisikoentscheidung**

Die Buchstaben c und d ermitteln, wen das System trifft und in welchem Ausmaß. Eine Folgenabschätzung ist damit noch nicht abgeschlossen: Sie verlangt eine Bewertung. Sonst bleibt offen, welcher gemessene Unterschied sachlich erklärbar ist, welcher rechtlich oder ethisch problematisch bleibt, welches Restrisiko getragen wird – und wer diese Entscheidung trifft.

Die folgende Matrix hält diesen Schritt fest. Sie bleibt bewusst auf der Betreiberebene: Kontrollen und Entscheidungen betreffen den Prozess, die menschliche Aufsicht und den Beschwerdeweg – nicht die Anpassung des Modells. Eine Fairness-Anpassung an einem internen Modell ist ein aufsichtlich relevanter Modelländerungsvorgang und gehört in das dafür vorgesehene Verfahren, nicht in ein Prüfgerüst.

Betroffene Gruppe	Beobachteter Unterschied	Sachliche Erklärung geprüft	Schwere und Reichweite	Vorhandene Kontrolle (Prozessebene)	Restrisiko	Entscheidung, Entscheider, Datum
-------------------	--------------------------	-----------------------------	------------------------	-------------------------------------	------------	----------------------------------

Zur Anwendung	Die Matrix beantwortet vier Fragen, die in der Praxis regelmäßig offen bleiben. Ist der beobachtete Unterschied durch einen sachlichen, nachvollziehbaren Grund erklärt – und ist diese Prüfung dokumentiert? Wie schwer und wie weitreichend wirkt er für die betroffene Gruppe? Welche bereits vorhandene Kontrolle auf Prozessebene mindert ihn tatsächlich? Und wer entscheidet über die Tragung des verbleibenden Restrisikos, mit Namen und Datum. Die vierte Frage ist die, an der Abschätzungen in der Prüfung scheitern.
----------------------	---

Abschnitt
8

Mitteilung: für wen die Ergebnisse aufbereitet werden

Artikel 27 Absatz 3 verlangt, der Marktüberwachungsbehörde die Ergebnisse der Abschätzung mitzuteilen, unter Verwendung des Fragebogens nach Absatz 5. Das ist nicht gleichbedeutend mit der Übersendung des vollständigen internen Berichts – wohl aber mit der Anforderung, dass der interne Bericht die mitgeteilten Ergebnisse trägt.

Wer die Mitteilung entgegennimmt, bestimmt Artikel 74 Absatz 6: Für Hochrisiko-KI-Systeme, die von durch Unionsrecht regulierten Finanzinstituten verwendet werden, ist Marktüberwachungsbehörde die für deren Finanzaufsicht zuständige nationale Behörde – soweit die Verwendung in unmittelbarem Zusammenhang mit der Erbringung der Finanzdienstleistungen steht. Für die meisten deutschen Banken und Versicherer ist das die BaFin. Für kleinere Versicherungsvereine auf Gegenseitigkeit und öffentlich-rechtliche Versicherer unter Länderaufsicht ist die zuständige Behörde eine andere; die konkrete Zuständigkeit ist vor der Mitteilung zu klären.

Daraus folgt der Qualitätsmaßstab. Die Ergebnisse werden im finanzaufsichtlichen Umfeld beurteilt und müssen an das dort übliche Evidenzniveau anschlussfähig sein. Als fachlicher Maßstab bietet sich das Dokumentationsniveau eines Validierungsberichts an: benannte Methode, benannte Datengrundlage, benannte Grenzen der Aussage. Dass es sich dabei um dieselbe Stelle handelt, die auch die Modelle beurteilt, gilt allerdings nicht durchgehend – die Genehmigung interner Modelle SSM-signifikanter Institute liegt bei der Europäischen Zentralbank, nicht bei der nationalen Aufsicht.

Zum Fragebogen

Der Fragebogen nach Artikel 27 Absatz 5 liegt noch nicht vor. Das ist kein Grund zu warten: Die sechs Pflichtinhalte stehen in Absatz 1 und sind vom Format unabhängig. Der Fragebogen ist die Übermittlungsform, nicht die Substanz.

Abschnitt
9

Aktualisierungsauslöser festlegen

Artikel 27 Absatz 2 knüpft die Pflicht an die erste Verwendung, erlaubt in ähnlich gelagerten Fällen den Rückgriff auf frühere Abschätzungen und verlangt Aktualisierung, sobald ein Element nicht mehr aktuell ist. Ohne definierte Auslöser ist diese Pflicht nicht steuerbar. Der ökonomischste Ort für die Verankerung ist der bestehende Validierungszyklus – mit der Einschränkung, dass die Grundrechte-Folgenabschätzung darin nicht aufgehen darf, weil sie eine andere Frage beantwortet.

Auslöser	Schwelle / Definition im Haus	Zuständig	Zuletzt geprüft
Modelländerung (Neuschätzung, Merkmalsänderung, Schwellenanpassung)			
Wesentliche Änderung der Datenbasis (neue Quelle, neue Proxyvariable, veränderte Abdeckung)			
Änderung der Kredit- oder Annahmerichtlinie			
Portfolio- oder Populationsverschiebung über definierte Schwelle			
Überschreitung einer Schwelle im laufenden Monitoring			
Technischer oder organisatorischer Vorfall (Fehlfunktion, Datenqualitätsproblem, fehlerhafte Schnittstelle)			
Neue Anbieterinformation nach Artikel 13 (neue Version, geänderte Betriebsanleitung)			
Erkenntnis aus dem Beschwerderückkanal (Buchstabe f)			

Auslöser	Schwelle / Definition im Haus	Zuständig	Zuletzt geprüft
Neue rechtliche oder tatsächliche Erkenntnisse (Rechtsprechung, Aufsichtshinweis, Studienlage)			
Turnusmäßige Überprüfung, gekoppelt an den Validierungszyklus			

Abschnitt 10

Zeichnung: Erstellung, Prüfung, Verantwortung trennen

Artikel 27 schreibt keine bestimmte organisatorische Zeichnungsfolge vor. Für regulierte Finanzinstitute bietet sich jedoch eine Trennung von fachlicher Erstellung, unabhängiger Prüfung, beratender Beteiligung und abschließender Verantwortung an – schon deshalb, weil in der Praxis drei Zuständigkeiten konkurrieren: Risikocontrolling, Compliance und Datenschutz. Jede Zuordnung an nur eine der drei erzeugt ein Dokument mit einer bekannten Schwäche: beim Datenschutz fehlt die Modellempirie, bei Compliance die Messgrundlage, beim Risikocontrolling die Grundrechtsperspektive.

Rolle	Typische Funktion	Name	Datum
Fachliche Erstellung	Modellverantwortung und verantwortlicher Fachbereich		
Methodische Prüfung und Mitzeichnung	Unabhängige Validierung oder vergleichbare Kontrollfunktion		
Rechtliche und grundrechtliche Prüfung	Compliance beziehungsweise Rechtsfunktion		
Datenschutzrechtliche Beteiligung	Datenschutzbeauftragte oder Datenschutzfunktion (Absatz 4)		
Verantwortung und Freigabe	Zuständiges Leitungsorgan als Betreiber		

Empfehlung von waveImpact: Eine Grundrechte-Folgenabschätzung, die die Validierungsfunktion nicht mitzeichnet, ist ein Dokument über ein Modell, für dessen Aussagen niemand einsteht. Ob die Freigabe durch das gesamte Leitungsorgan oder eine delegierte Funktion erfolgt, legt das Institut anhand seiner Kompetenzordnung fest.

Wenn Sie den Zuschnitt besprechen möchten

Der Punkt, an dem dieses Gerüst in der Praxis stehen bleibt, ist regelmäßig Buchstabe d – die gruppendifferenzierte Messung, die aus der Validierung nicht herausfällt. waveImpact erzeugt diese Messung in einer abgeschotteten, client-seitigen Umgebung: Die Analyse der Ausgangsdaten läuft im Container beim Kunden; für die Berichterstellung werden ausschließlich zuvor festgelegte und geprüfte Analyseergebnisse auf EU-residenter Infrastruktur verarbeitet. Roh- und Einzeldaten verlassen die Kundenumgebung nicht. Für die Vendor-Prüfung eines regulierten Hauses ist das der entscheidende Unterschied.

Für eine fachliche Frage genügt eine formlose E-Mail an valentin.mayr@waveimpact.de. Kein Formular, kein Newsletter, keine Registrierung – und keine Verpflichtung.

Dr. Valentin José Mayr ist Gründer und Geschäftsführer der waveImpact GmbH in Bremen. waveImpact prüft KI-Systeme auf Fairness, Transparenz und regulatorische Anschlussfähigkeit.

Rechtsstand: 29. Juli 2026. Verordnung (EU) 2024/1689 in der Fassung der Verordnung (EU) 2026/1744 (Digital-Omnibus zur KI), ABl. L vom 24. Juli 2026, in Kraft seit dem 27. Juli 2026. Die Wiedergabe der Vorschriften ist sinngemäß und ersetzt nicht den Blick in den amtlichen Text. Dieses Dokument gibt eine fachliche Einschätzung wieder und stellt keine Rechtsberatung im Einzelfall dar. Weitergabe innerhalb Ihres Hauses ausdrücklich erwünscht.