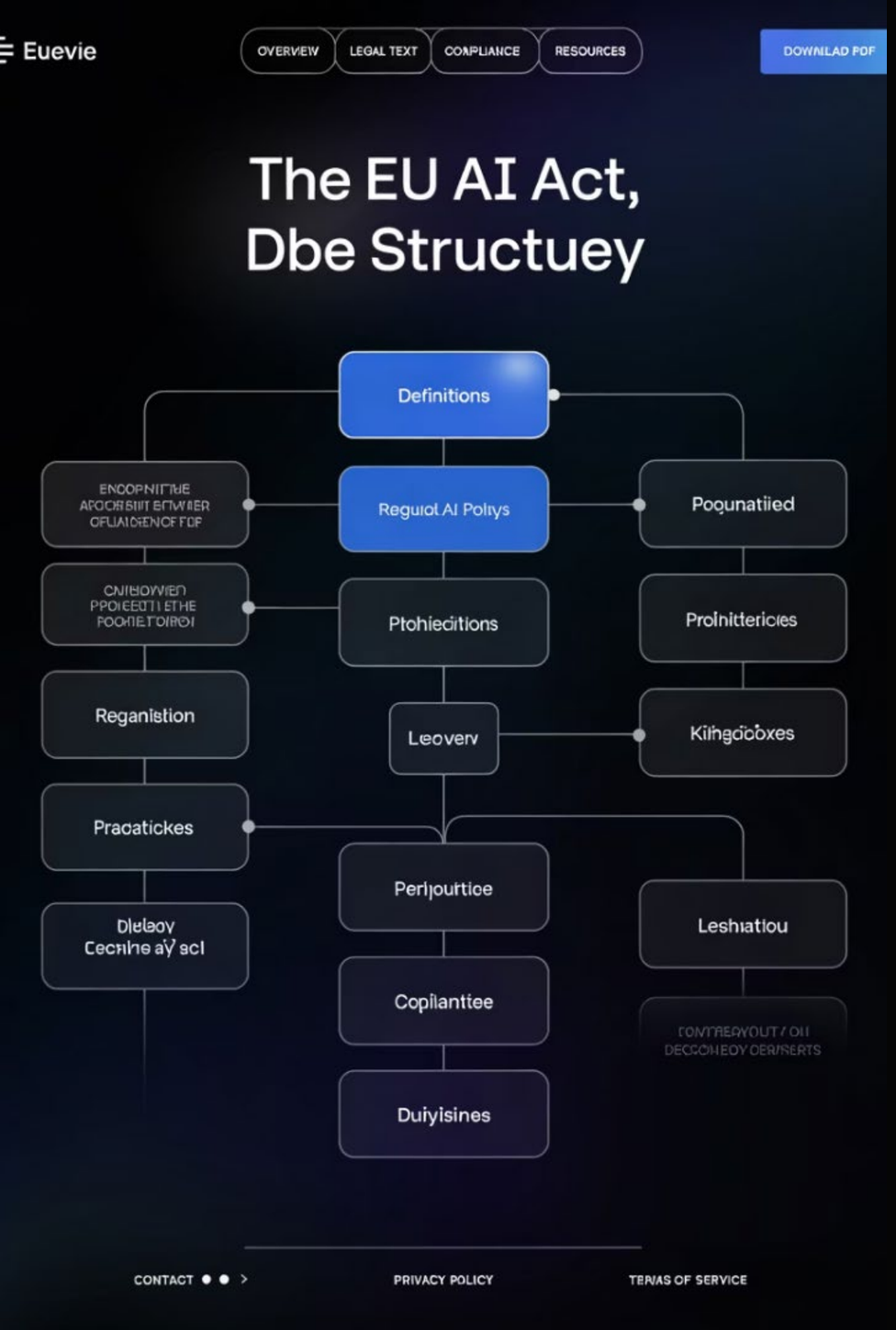
歐盟人工智慧法（AI Act）與資料治理法制之關聯

兼論德國現行法制在AI系統／生成式AI模型發展下的調適狀況與趨勢

該法為全球首部全面規範人工智慧之專法，立法目的在於確保AI技術符合人權、民主原則及法治要求，同時促進創新與市場成長。以下將探討該法之其風險分類方法、高風險AI系統的義務要求、通用型AI的特別規定，以及與現行資料治理法制的複雜互動關係，以及德國在AI系統發展下之法制調適面向。

佛光大學公共事務學系助理教授
彭睿仁



法律架構

歐盟《人工智慧法》為第一部全面規範AI之專法，其立法目的為：「確保AI技術符合人權、民主原則及法治要求，同時促進創新與市場成長。」

序言（Preamble）
說明背景、目標、立法依據（特別是歐盟基本權憲章）

第1-5條
適用範圍、定義、禁止行為

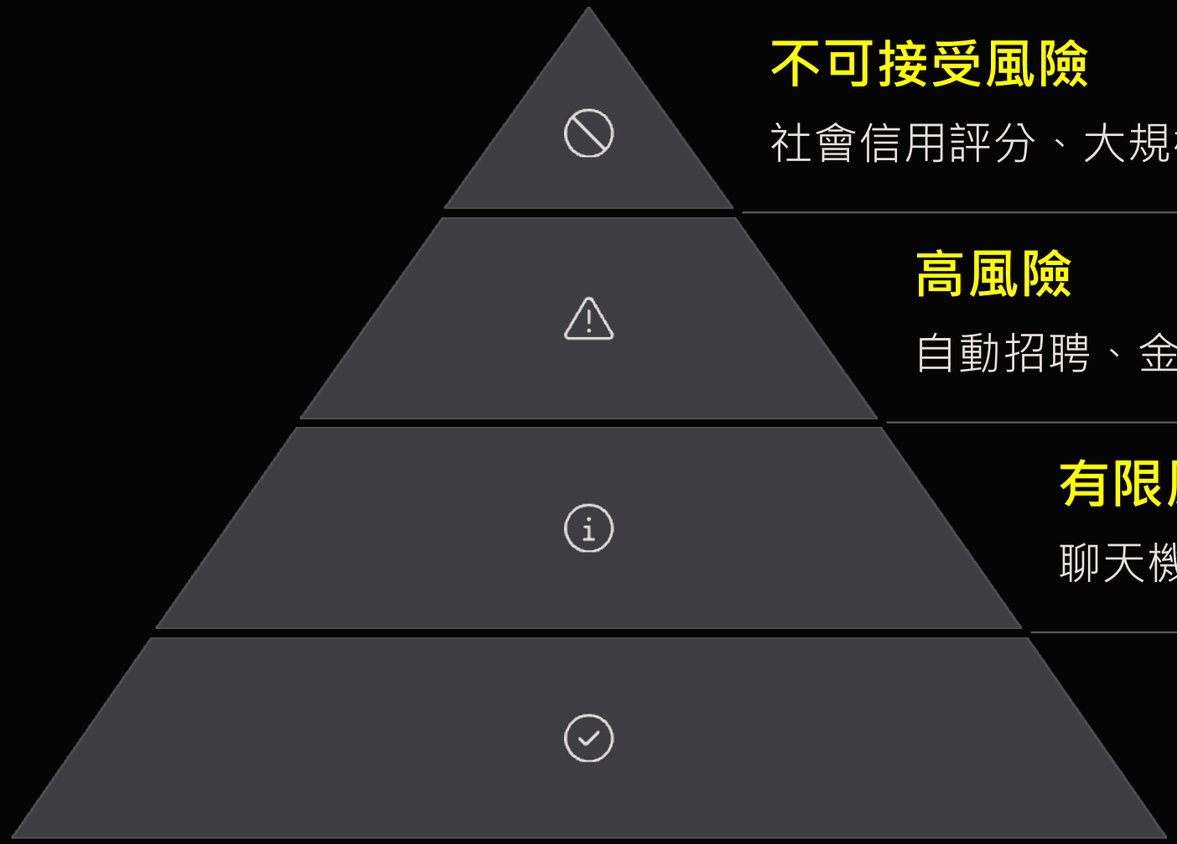
第6-51條
風險分類、高風險AI系統之要求、紀錄、人為監督與合法合規義務

第52-54條
有限風險（透明義務）系統的要求、AI模型供應商之義務

第55-74條為規範通用型AI（GPAI，包含生成式AI）之特別規定，第75-89條則處理市場監督、執行與裁罰。附錄I-IV則提供高風險AI系統分類清單與符合標準指引。

規範重點：風險基礎分類

歐盟AI法採用風險基礎分類（Risk-based Approach）方法，依據風險程度區分規範強度，從不可接受風險到最小風險，規範要求各不相同。



不可接受風險

社會信用評分、大規模情緒操控

高風險

自動招聘、金融風控、醫療診斷

有限風險

聊天機器人、虛擬助理

最小風險

遊戲推薦系統

不可接受風險AI系統完全禁止使用；高風險AI系統須符合嚴格要求，包括風險管理、透明度和可追溯性；有限風險AI需告知使用者「與AI互動」；最小風險AI則無特殊規範要求。

高風險AI系統監管

人為監督要求

高風險AI系統需人為進行監督，確保人類得有效監控系統運作。

安全性設計標準

系統必須具備健全的安全性設計，保證系統的穩健性與準確性。

合法合規框架

法定義務共同構成高風險AI系統之合法合規框架。

通用型AI（GPAI）與生成式AI特別規定

隨著ChatGPT等大型生成式AI模型之快速發展，歐盟AI法對通用型AI制定了特別規定，以應對其獨特風險與挑戰。

此等規定著重於透明度、內容標記與系統性風險管理。

公開訓練資料來源摘要

開發者必須提供模型訓練資料的來源概述，增加透明度

標記AI生成內容

AI模型生成文本、影像、音訊等內容，必須明確標示為AI生成

系統性風險級別評估

大型模型達到「系統性風險級別」（如GPT-4、Gemini），須接受外部合規評估

模型安全檢查

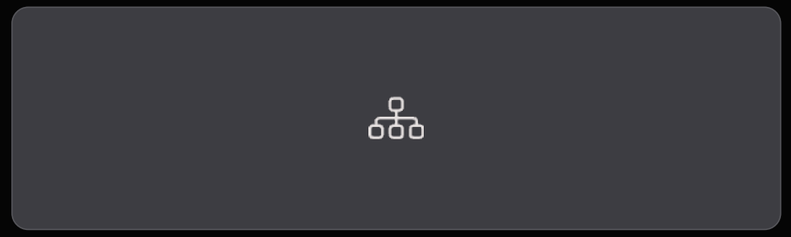
建置安全性、偏見測試、濫用風險評估等全面檢查機制

執行與裁罰

歐盟AI法建立了嚴格的執行機制與裁罰標準，確保法規得到有效實施。該機制由各國市場監管機構與歐盟AI辦公室共同構成，形成多層次監管網絡。

各國市場監管機構

負責執行日常監管與檢查



歐盟AI辦公室

統籌協調跨國監管行動

高額罰款

最高達全球年營收7%或3,500萬歐元

這種分層執行機制確保了從地方到歐盟層級的全面監管。罰款金額之高（取全球年營收的7%或3,500萬歐元中較高者）反映了歐盟對AI合規的嚴肅態度，為企業提供了強大的遵法動機。

AI Act與資料治理法制之關係

AI Act並非單獨存在之法典，而係與現行歐盟資料治理法制密切相關，其主要規範間之關連如下：

法律	主要內容	與AI Act之關係
GDPR	個資保護、資料主體權利、合法資料處理基礎	高風險AI需確保資料處理符合GDPR（如合法基礎、資料最小化）
Data Governance Act（DGA）	促進資料共享，建立資料中介與信託服務框架	AI系統若基於共享資料運作，須遵守DGA下的資料管理規則
Data Act（DA）	商業資料流通、資料可攜權（特別是物聯網資料）	AI訓練資料若來自產品/服務產生數據，受Data Act管轄
Digital Services Act（DSA）	平台透明度、違法內容管理	若AI系統涉及內容生成或推薦，須符合DSA關於透明度與風險管理要求

AI Act與GDPR的互動

AI Act與GDPR的互動特別值得關注，因為AI系統的訓練與運作往往涉及大量個人資料處理，必須同時符合兩部法律的要求。

資料來源合法性

AI訓練與運作所使用的個人資料必須符合GDPR第6條（合法處理基礎），確保資料取得合法。

特殊類別資料（如種族、健康、宗教等敏感資料）適用GDPR第9條，須符合額外合法性條件，對AI系統構成更高合規要求。

自動決策與資料最小化

若AI導致自動化決策（例如信用拒絕），須符合GDPR第22條要求，必須建立人類干預機制，確保決策可被審查。

資料最小化原則要求AI系統必須避免過度收集，僅限於必要之資料進行訓練與推論，這對大型模型構成挑戰。

AI Act與資料法規之互補

簡而言之，AI Act是應用之行為規範（管理AI產品與服務），而GDPR/DGA/Data Act則是個資及非個資利用合法化（AI利用資料之合法要求），兩者需互為補充。

小結：歐盟人工智慧法之核心架構與目標

歐盟人工智慧法建立全面人工智慧監管框架，平衡創新與基本權保障，為全球AI治理提供重要參考模型。

風險分級架構

以風險為基礎，從禁用到最小規範

高風險AI規範

風險管理、透明度、人為監督

平衡發展目標

兼顧創新與基本權保障

資料法制整合

與GDPR、DGA、Data Act規範連結

歐盟人工智慧法之整體立法目標為平衡技術創新與基本權保障，建立可信賴的AI市場環境。透過整合風險分級管理、明確合法合規要求及現有資料法制，為全球AI治理建立重要規範依據。

德國現行法制在AI統 / 生成式AI模型發展下的調適狀況與趨勢

德國作為歐盟重要成員國，其法制對AI技術的調適具有重要參考價值。德國法制調適呈現出務實而漸進的特點，一方面保持法律穩定性，另一方面針對新技術帶來之挑戰進行部分修正。

德國民法典（BGB）

在傳統民法架構下處理AI智能合約、法律行為及責任歸屬等問題

德國產品責任法（ProdHaftG）

擴展產品概念以涵蓋AI系統，強化開發者與製造商責任

德國著作權法（UrhG）

調適著作權保護機制以適應AI生成內容的挑戰

德國聯邦資料保護法（BDSG）

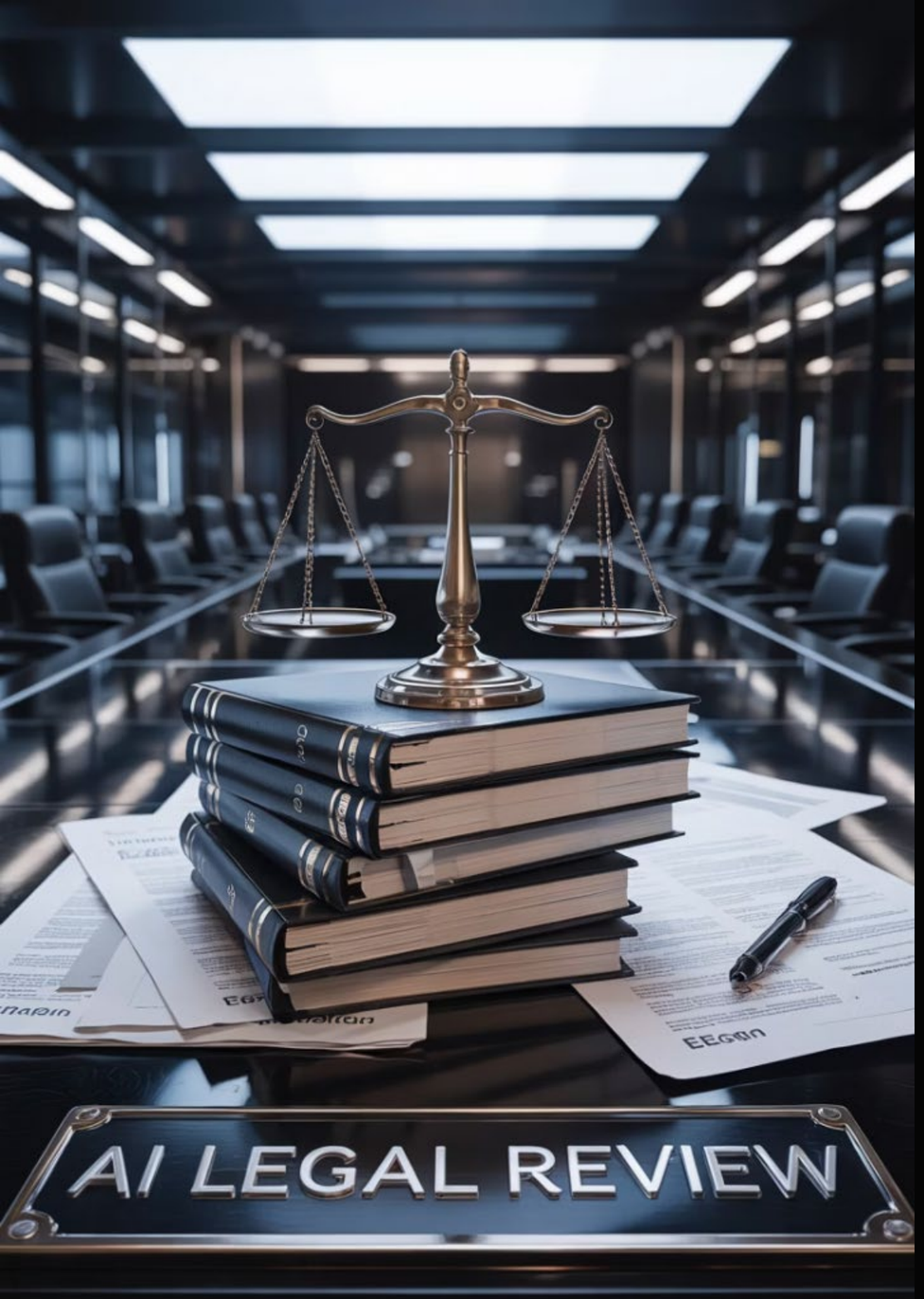
強化個人資料在AI系統中的處理規範與保障機制

德國道路交通法（StVG）

修正法規以適應自動駕駛技術的發展與應用

德國反不正當競爭法（UWG）

規範AI應用於市場行銷、定價等可能產生的競爭問題



德國民法典（BGB）因應AI技術應用之調適

德國民法（Bürgerliches Gesetzbuch）作為私法基礎，在AI發展下面臨侵權責任與契約責任的調適挑戰。

現況

侵權法（§ 823 BGB）仍是AI引發損害求償的基礎，適用於自動駕駛事故、AI醫療錯誤等情境。契約責任（§§ 280、241 BGB）則適用於生成式AI作為服務（SaaS模型）時的系統性錯誤或服務中斷。

調適趨勢

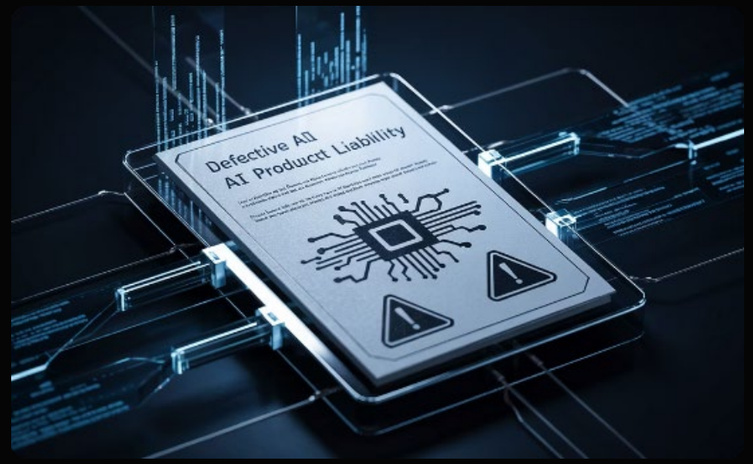
德國法學界正在討論「AI代理人」（Agent）的法律地位，例如ChatGPT、Copilot作為輔助工具，其錯誤是否歸屬於使用者。民事責任將更趨向於客觀過失（objektive Fahrlässigkeit）標準，對採用AI的企業提高注意義務。

挑戰

舉證難度高，例如生成內容與瑕疵造成之損害間，不易證明因果關係），成為當前最大實務障礙。責任歸屬與舉證問題需要立法與司法實踐共同解決。

德國產品責任法（ProdHaftG）的AI調適

產品責任法（ProdHaftG）規範瑕疵產品的無過失責任，在AI系統被視為「產品」時適用，但面臨多項調適挑戰。

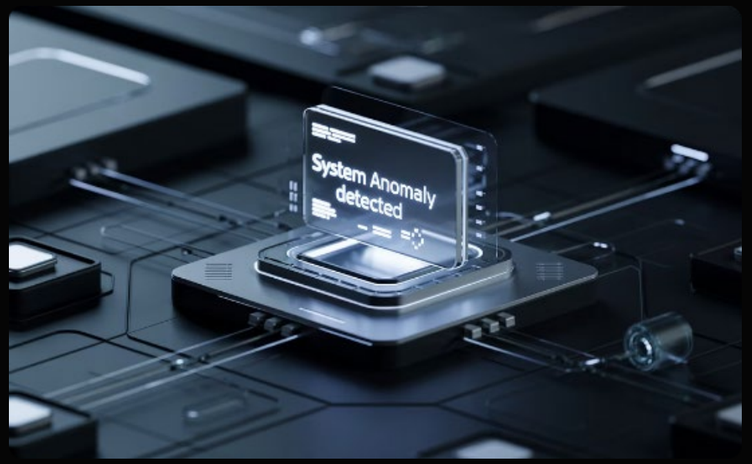


現況

生成式AI（例如自動生成醫療建議系統）若屬「產品」（Produkt），開發商需負產品瑕疵無過失責任。這為受害者提供了較為直接的求償途徑，但適用範圍存在爭議。

調適趨勢

配合歐盟推動修正《產品責任指令》（預計2025通過），德國也會同步修改ProdHaftG，擴大適用到軟體產品（包括AI系統）及AI自我學習過程後的新行為，強化消費者保護。



挑戰

如何界定「瑕疵」是主要挑戰，例如生成式AI輸出有害內容時，是否視為「缺陷」？軟體更新後的新風險責任歸屬也是待解難題。

德國著作權法（UrhG）在AI應用之調適

著作權法（UrhG）在生成式AI時代面臨訓練資料合法性與AI生成內容著作權歸屬的雙重挑戰。

§§ 44b

資料探勘之例外

德國著作權法§§ 44b、60d UrhG（資料探勘例外條款）允許在特定條件下合法使用資料進行AI訓練，為創新提供法律空間。

0%

AI創作品之著作權

生成式AI創作的內容原則上不享有著作權保護，除非有明確人類精神力參與，這反映了「人類創作者」中心的傳統著作權觀念。

2025

標示義務

德國正討論在2025年前引入「生成作品標示義務」，要求AI產出內容標明「非人類創作」，增加透明度。

當前主要問題包括：權利人如何行使「opt-out」拒絕資料被訓練？使用侵權資料訓練的AI，其生成內容是否帶有「間接侵權責任」？

德國聯邦資料保護法（BDSG）於AI技術應用之調適趨勢

聯邦資料保護法（BDSG）結合GDPR，共同規範AI系統處理個資之法律依據，
面臨生成式AI模型被大量運用時的各種爭議與問題。

德國資料保護監管架構

德國資料保護主管機關（如BfDI）主張強化AI訓練資料的資料最小化（data minimization）原則，提升個資保護標準。

GDPR第22條自動化決策限制

生成式AI常會處理敏感資料（如個人資訊、臉部圖像），GDPR第22條規定禁止純自動化決策造成重大影響，需有人為介入或至少知情同意。

高風險AI評估要求

德國要求高風險模型（如人臉識別AI）進行資料保護影響評估（DPIA），確保符合法規要求。

匿名化與去識別化挑戰

主要挑戰包括：如何在生成式AI訓練過程中落實匿名化或去識別化？用戶輸入AI模型之資料是否屬個資？（例如在ChatGPT中輸入個人醫療資訊）

德國道路交通法（StVG）於AI應用之調適

道路交通法（StVG）在自動駕駛技術發展進行重要調適，透過立法允許Level 3自動駕駛。

現行法規

StVG § 1a允許「自動駕駛系統」行駛，但仍需駕駛人能隨時接管。這為自動駕駛技術的合法部署提供了法律基礎，同時保留人類監督責任。

調適趨勢

隨生成式AI（例如路況預測系統）的導入，未來修法趨勢包括：定義「行為系統」（Handlungssysteme）作為新責任主體，設立專屬事故責任基金（由自駕車製造商共同承擔）。

主要問題

自動駕駛車事故中，生成式AI判斷錯誤，車主與製造商間的責任比例如何分配？此需更精細之法律規範與司法實踐來釐清相關問題。

德國不正競爭防止法（UWG）於AI應用之調適方向

不正競爭防止法（UWG）規範市場行為公平性，在AI生成廣告與演算法決策之應用，面臨新的調適需求。

AI廣告標示 (75%)

使用AI生成廣告內容時須明確標示，避免消費者誤解。德國正積極完善相關規範，要求AI生成內容需標明「廣告性質」。

未成年保護 (60%)

禁止針對未成年人進行操縱性推薦，建立特殊保護機制。修正案將強化對未成年人在AI推薦系統中的保護措施。

演算法透明 (45%)

要求商業演算法決策過程具透明性，特別是影響消費者選擇的關鍵因素。相關法規仍在發展中。

自動評論規範 (30%)

生成式AI自動製作的商品評論是否屬「商業行為」，及如何標示才足夠清楚透明，仍是主要挑戰。

目前使用AI生成廣告、推薦內容時，若引導誤解或操縱消費者，可能構成違反UWG，此規範為AI之商業應用提供法律依據。在調適趨勢方面，德國正研議新修正案（配合歐盟DSA，明確要求AI推薦或生成內容需標示「廣告性質」，並禁止針對未成年人進行認知操縱性質之推薦。

✨ 德國AI法制調適總結

德國在AI法制調適上展現系統性與前瞻性之前瞻立法思維，各專法領域均有法規調適之規劃，但亦需面對AI技術用可能產生之共同問題。

法律	當前調適方向	主要挑戰
BGB	推高侵權責任門檻，客觀過失標準	舉證困難
ProdHaftG	納入軟體產品責任、AI瑕疵	瑕疵定義模糊
UrhG	保障資料探勘例外、規範生成作品	opt-out機制未明確
BDSG+GDPR	強化AI個資保護、DPIA強制化	訓練資料匿名化困難
StVG	自駕車責任細緻化、引入系統責任	人-機責任界線模糊
UWG	強制標示生成內容為廣告	自動生成評論合法性問題