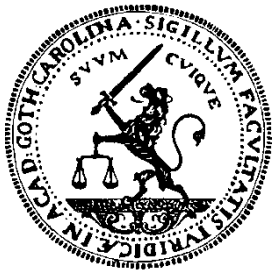

FACULTY OF LAW

Lund University

Benjamin Golding

High-Risk AI in Life and Health Insurance Underwriting

Balancing Underwriting with Data Protection and Non-Discrimination

LAGF03 Essay in Legal Science

Bachelor Thesis, Master of Laws program

15 higher education credits

Supervisor: Mariya Senyk

Term: Autumn term 2025

Contents

Summary

Since the inception of artificial intelligence (AI), technological advancements have rapidly increased in intensity and scope, often outpacing the speed at which regulatory frameworks can preserve the rights on which the European Union (EU) is founded. The insurance industry is a sector in which technological advancements are vital for profitability, a fact seemingly exponentially compounded with the rapid development of AI. The EU has tried to curb the potential infringements on human rights in the deployment of AI systems by introducing the AI Act. This regulatory act has been subject to criticism, especially from the insurance industry.

This thesis narrows in on the definition of AI, its legal constituent parts, and the practical functionalities on which the legal prerequisites are based. When that foundation is laid and combined with an examination of how AI systems are employed in the insurance sector, the study proceeds to analyse the ordinances in the AI Act regarding high-risk AI systems. It also examines how insurance companies, particularly in the case of risk assessment and pricing for life and health insurance, should preferably adapt their use of such systems based on these legal frameworks to comply with the right to data privacy and the right to non-discrimination.

Findings include practical difficulties of tracing the data input and steps, both technical and overarching, by which an AI system operates and reaches its conclusions. Combined with the system's frequent tendency toward bias and discrimination, these factors provide regulatory and rights-based challenges. However, with regulatory understanding, adaptation to the technicalities of the systems in question, and a willingness for compliance and innovation, these challenges can be addressed.

Sammanfattning

Sedan framväxten av artificiell intelligens (AI) har de teknologiska framstegen snabbt ökat i både intensitet och omfattning, ofta i en takt som överstiger den hastighet med vilken regelverk kan upprätthålla de rättigheter på vilka Europeiska unionen (EU) är grundad. Försäkringsbranschen är en sektor där teknologiska framsteg inom AI är avgörande för lönsamhet. EU har försökt begränsa potentiella kränkningar av mänskliga rättigheter vid användningen av AI-system genom att införa AI-förordningen. Regelverket har delvis varit föremål för negativ kritik, särskilt från försäkringsbranschen.

Uppsatsens fokus snävar in på definitionen av ”AI”, dess rättsliga beståndsdelar samt tekniska funktioner på vilka de rättsliga förutsättningarna vilar. När denna grund väl är lagd och kombineras med en undersökning av hur AI-system används inom försäkringssektorn, analyserar uppsatsen därefter bestämmelserna i AI-förordningen om högrisk-klassade AI-system. Den undersöker också hur försäkringsbolag, särskilt vid riskbedömning och prissättning av liv- och hälsoförsäkringar, lämpligen bör anpassa sin användning av sådana system utifrån dessa rättsliga ramar för att uppfylla rätten till dataskydd och rätten till icke-diskriminering.

Uppsatsens slutsatser omfattar de praktiska svårigheterna att inventera det dataunderlag och de steg – både tekniska och övergripande – baserat på vilka ett AI-system grundar sina slutsatser. I kombination med systemets frekventa benägenhet till *bias* och diskriminering innebär dessa faktorer regleringsmässiga och rättighetsbaserade utmaningar. Med teknisk kompetens, förståelse för regelverken och anpassning till de tekniska förutsättningarna i de aktuella systemen, tillsammans med en vilja till efterlevnad och innovation, kan dessa utmaningar emellertid hanteras.

Abbreviations

ADM	Automated decision-making
AI	Artificial Intelligence
AI Act	Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828
BDA	Big Data Analytics
CJEU	Court of Justice of the European Union
CFR	Charter of Fundamental Rights of the European Union
CORE	Common Opportunities Results Experiences (Wells Fargo front-end workflow tool)
DPA	Data Protection Authority
ECLI	European Case Law Identifier
EIOPA	European Insurance and Occupational Pensions Authority
EU	European Union
FRA	European Agency for Fundamental Rights
FRIA	Fundamental Rights Impact Assessment

GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC
IB	Responsible administrative body within the Dutch authority that implemented the SyRI-system
PNR	Passenger Name Record
SyRI	Systeem Risico Indicatie
TFEU	Treaty on the Functioning of the European Union
UW	Underwriting
XAI	Explainable Artificial Intelligence

1 Introduction

1.1 Background

The insurance sector has increasingly sought and implemented tools for artificial intelligence (AI) throughout its businesses in order to remain competitive and gain market leverage.[1] This is potentially at the cost of adequate data privacy and to the detriment of the EU's pursuit of preventing, combating, and minimising undue discrimination.[2] On 1 August 2024, legislation was implemented by the European Union (EU) to ensure that this potential downside of the insurance sector's approach to AI is limited in scope and severity—the AI Act.[3]

On 19 November 2025 the European Commission proposed a postponement of the implementation of certain obligations concerning high-risk AI systems. The proposal has been the subject of debate and criticism. Whether or not the postponement ultimately materialises, the debate and criticism illustrate the tension between market incentives for automation and the EU's rights-based insistence that systems with legal or similarly significant effects remain contestable and non-discriminatory.[4] In life and health underwriting (UW), this is particularly evident because pricing and eligibility decisions are supported by extensive data-driven inferences, which form the basis for stratification of risk.

UW is the process by which insurance companies assess the financial risk of a prospective client, investment, or loan, and determine the pricing thereof if the risk is acceptable. The scale and degree of dependency on sensitive data in the process of UW for life and health insurance make it a particularly relevant area for AI-automation- and innovation. The AI Act serves to

[1] EIOPA, *Big Data Analytics in Motor and Health Insurance: A Thematic Review* (April 2019) p. 29; cf. Article 22 GDPR.
[2] Economist Impact, *Underwriting the future: the role of artificial intelligence in insurance* (2025).
[3] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (AI Act).
[4] Euronews, 'European Commission delays full implementation of AI Act to 2027' (19 November 2025); TechPolicy.Press, 'What's driving the EU's AI Act shake-up' (2025).

highlight the tension between innovation and the preservation of consumers' fundamental rights and freedoms, particularly with regard to data privacy and non-discrimination.[5]

1.2 Purpose and Research Questions

The thesis aims to propose ways of reconciling the insurance industry's interest in innovation with the protection of customers' fundamental rights and freedoms, in particular regarding UW, by answering the question below.

To what extent, and under which conditions, can insurance companies' deployment of high-risk AI systems in underwriting for life and health insurance be reconciled with the requirements of the EU AI Act and GDPR, as interpreted in light of the rights to data protection and non-discrimination under the EU Charter of Fundamental Rights?

1.3 Review of Relevant Scholarship

1.3.1 State of the Art

Current scholarship on data privacy and non-discrimination under the GDPR is extensive and overlaps with the AI Act, particularly regarding *ex-ante* (pre-deployment) impact assessments.[6] Much of it is mainly oriented toward public administrative law and public actors.[7] However, in Hofmann's examination of how responsibility for automated decision-making (ADM) is distributed, compliance with GDPR is posited as a cornerstone for securing

[5] Recitals (1) and (8) AI Act.
[6] Regulation (EU) 2016/679 (GDPR); Article 35 GDPR; Article 27 AI Act; Hands, L. A. (2024) *Just(ifying) Algorithms: Data-Driven Automated Predictions About Unobservable Targets and the General Data Protection Regulation* (PhD thesis, University of Cambridge) pp. 117–118.
[7] Mir, O. (2024) (pp. 54, 59–60) in Hofmann, H. C. H. & Pflücke, F. (eds), *Governance of Automated Decision-Making and EU Law* (Oxford University Press 2024); Hofmann & Pflücke (2024) p. 289; Pesch, J. & Boehm, F. (2024) pp. 163–164 (chapter 6) in Hofmann & Pflücke (eds), *Governance of Automated Decision-Making and EU Law* (OUP 2024).

accountability and contestability without prejudice to the private sector.[8] This is echoed by Liga, Pesch & Boehm, and Demková.[9]

Bias and discrimination are likewise significantly highlighted in scholarly contributions. Hofmann highlights weaknesses in prevailing practices of human oversight in public administration. He attributes them to 'automation bias' and to structural limits on meaningfully contesting outputs derived from vast and complex data and data inferences.[10] Biber underscores similar concerns.[11] Pesch & Boehm further link these problems to the CFR, stressing how risks concerning both privacy and discrimination become intertwined through large-scale data processing, entrenched historical bias, and the discriminatory potential of risk indicators and inferred attributes.[12]

Explainability in ADM, including AI systems, and the tension between actuarial and legal fairness—sometimes framed as irreconcilable ("impossibility theorem"), is parallel literature.[13] Hofmann and Biber also flag explainability as a obstacle.[14] Explainability, under for example the AI Act (including Article 13), is noted in relevant literature but seldom developed into operational measures that clarify how compliance can be ensured.[15] This with the possible exception of Liga who suggests generally applicable XAI-tools (Explainable AI) which could address the issue of insufficient explainability concerning the GDPR and, recently, the AI Act.[16]

[8] Hofmann, H. (2024) pp. 7 and 15 (chapter 1) in Hofmann, H. C. H. & Pflücke, F. (eds), *Governance of Automated Decision-Making and EU Law* (Oxford University Press 2024).
[9] Liga, D. (2024, pp. 241, and 248–249, chapter 9); Pesch & Boehm (2024, pp. 172–173, chapter 6); Demková, S. (2023, pp. 181–183). *Automated Decision-Making and Effective Remedies: The New Dynamics in the Protection of EU Fundamental Rights in the Area of Freedom, Security and Justice*, Edward Elgar Publishing.
[10] Hofmann (2024, pp. 16–17, 22–23 and 26–29, chapter 1).
[11] Biber, S. (2024, pp. 199–201 and 209, chapter 7).
[12] Pesch & Boehm (2024, p. 161–162 and 169, chapter 6).
[13] Hands (2024, pp. 84, 86 and 88).
[14] Hofmann (2024, pp. 19–21, chapter 1); Biber (2024, p. 188, chapter 7).
[15] Hands (2024, pp. 84–98).
[16] Liga (2024, p. 254, chapter 9); Mir (2024, p. 76, chapter 3).

1.3.2 Contribution

The distinguishing mark of this thesis is its sectoral recommendations for commercial insurers to achieve compliance based on the highlighted concerns in *State of the Art*. Life and health UW is a useful testcase because price optimisation and efficient stratification of risk incentivise extensive data collection and processing through opaque AI models.

1.4 Method and Material

A doctrinal legal method is used to set out the applicable law and explain how insurance companies' UW practices can comply with the resulting requirements.[17] The AI Act delimits the regulatory scope, while the GDPR serves as an essential guideline due to the expanse of case law related to its regulation on ADM and profiling, and the related provisions relevant for UW, especially Articles 5, 6, 9 and 22.[18]

Cases are selected where they involve ADM, profiling and/or AI systems, and highlight generally applicable legal considerations for data privacy and the balancing of fundamental rights. In addition, decisions made by Data Protection Authorities (DPAs) in Member States will be used as supplementary sources of information.

Due to the overrepresentation of state authorities as defendants in case law on the right to data privacy in the context of ADM, profiling and/or AI systems, the section *EU's AI Act in the Insurance Sector* includes a subsection addressing differences between state authorities and private enterprises in the stringency with which applicable regulatory ordinances are applied.

Case law by the Court of Justice of the European Union (CJEU) and courts in the Member States are used as sources of law due to the breadth of the interpretative scope within which the relevant fundamental rights may

[17] Kleineman, J. (2018, p. 21). "Rättsdogmatisk metod" in Nääv, M. & Zamboni, M. (eds). *Juridisk metodlära*, Norstedts Juridik.
[18] Article 27(4), AI Act.

reasonably be understood.[19] To the extent that sufficient guidance is lacking or supplementary information is warranted, case law from other jurisdictions whose legal systems largely share the EU's foundational values and the legal norms derived from them is drawn upon.[20]

1.5 Limitations

High-risk AI systems in the insurance sector are explored due to the extent to which such tools are applied therein. The thesis is further limited to life and health insurance, as commercial operations in these areas require the processing of more sensitive data and therefore call for closer consideration of potential intrusions into privacy and non-discrimination. In consideration of the scope of the thesis, the thesis will assume that the insurance companies for which the suggested compliance measures are purposed to be relevant are "deployers" of AI systems, not "providers" in the terminology of the AI Act. In addition, regulations overlapping with the AI Act and GDPR as it regards insurance companies, such as the Data Governance Act and the Solvency II Directive, will not be analysed.[21]

1.6 Disposition

The thesis first defines "AI system" as per the AI Act and subsequently explain how infringements into privacy and non-discrimination may arise in UW. After that, applicable legal rules and limitations concerning the use of AI as derived from a selection of illustrative ordinances in the AI Act and relevant case law are set out. The *Analysis* identifies risks in light of these limitations and proposes measures to ensure compliance for insurance companies, followed by a synthesis of its findings in the *Conclusion.*

[19] Hofmann (2024, p. 1, chapter 1).
[20] District Court of The Hague (Rechtbank Den Haag) *SyRI* ECLI:NL:RBDHA:2020:865, para 6.68.
[21] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance (Data Governance Act); Consolidated text: Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II).

2 Artificial Intelligence System' constituents and functionality

2.1 What is an AI system?

The definition of an "AI system" is specified in Article 3 in the AI Act.

> "'AI system' means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments[.]"

To fulfil the above-mentioned definition, the system must possess three essential constituents: machine-based inference, autonomous operation, and output influence.

2.1.1 'Machine-based inference'

'Machine-based inference' means that the system is technologically constituted and is capable of drawing conclusions based on computational or statistical preconditions by algorithmic means. [22] A commercially used scoring-system to measure creditworthiness fulfilled the essential constituent "machine-based inference" by producing predictions based upon neutral data-inputs processed by automated algorithms.[23]

2.1.2 'Autonomous operation'

'Autonomous operation' requires that the machine-based system's functionality, and the executions thereof, are not entirely dependent on human oversight and intervention and is capable of adapting its parameters or rules based on data-driven feedback, within the scope of its design.[24] What is often referred to as the 'black-box effect', refers to phenomenon in which the output

[22]Case C-817/19 *Ligue des droits humains* EU:C:2022:257, paras 98–100; Case C-806/24 *'YETTEL BULGARIA' EAD v FB*, request for a preliminary ruling (OJ C/2025/1080, 24.2.2025).
[23] Case C-634/21 *SCHUFA* EU:C:2023:950, paras 14, 46–47 and 73.
[24] *Ligue des droits humains* EU:C:2022:257, paras 171–173 and 180–181.

of an AI system cannot be fully traced back to the original input data and design parameters.[25]

2.1.3 'Output influence'

'Output influence' means that the system produces outputs that can form the basis for a decision that extends beyond the mere technological environment in which it is trained and customised. This distinguishes an AI system from an 'AI model'. An AI model is an essential part of the former but is not sufficient to independently qualify as an AI system, without an applied context and human-invented purpose.[26]

2.2 High-Risk Classification

High-risk AI systems have their regulatory basis in Article 6 of the AI Act, which states that AI systems listed in Annex III are to be considered high-risk, including "[…] AI systems intended to be used for risk assessment and pricing in relation to natural persons in the case of life and health insurance." The recitals describe that such systems may serve as a catalyst for harm to public interests and fundamental rights to such a degree that they must be subject to stricter legal requirements.[27]

2.3 AI Systems' Deficiencies

2.3.1 Lack of Data Traceability

A central threat to data privacy and non-discrimination is the use of AI models in which outputs are based on non-traceable inputs and non-auditable weightings (*black-box effect*).[28] In a ruling by the CJEU, systems that can change predetermined criteria of analysis and the weightings pertaining

[25] Hofmann (2024, pp. 16 -17 and 21-22, chapter 1; Biber (2024, pp. 188-189, chapter 7).
[26] Recital (12), AI Act.
[27] Recitals (5)–(7), AI Act.
[28] *Ligue des droits humains*; Hofmann (2024, pp. 3–4, chapter 1).

thereto, without human intervention or oversight, are seemingly presumed to be incompatible with contestability and effective remedy.[29]

2.3.2 The Problem of Fabrication

AI systems do not have inherent functions for fact-checking. They operate on the basis of statistical probability which means that outputs may be mathematically plausible but also completely incorrect. [30] This is colloquially referred to as "hallucinations". *Overfitting*, bias or inaccuracy in the training data, and high model complexity can contribute to unreliable inferences when a trained system is inputted with new data.[31] In UW this has significant consequences because inaccurate inferences can exacerbate risks regarding privacy and fairness for individuals.[32]

2.4 Usage of AI Systems in Insurance Underwriting

The AI systems applied in UW can be grouped into three different but overlapping functions: automated data collection and pre-fill, predictive risk modelling and pricing, and eligibility determination.

2.4.1 'Automated data collection and pre-fill'

'Automated data collection and pre-fill' streamlines administrative tasks by prefilling application forms, reducing manual analysis of inputted information, and generally scaling down manual tasks for arranging a packaged insurance proposal. This is contingent upon large-scale access to public records and third-party data, such as non-smoker models, credit

[29] *Ligue des droits humains* EU:C:2022:257, paras 98–100, 111–113, 176–177, 203–205, 210–211; Case C-203/22 *CK v Magistrat der Stadt Wien* (Dun & Bradstreet Austria) EU:C:2025:117, paras 58–62 and 64–66; SyRI (ECLI:NL:RBDHA:2020:865) paras 6.61–6.65, 6.90, 6.100, 6.106.
[30] OpenAI (2023). "Why Language Models Hallucinate", OpenAI Blog.
[31] IBM Institute for Business Value (2025). "From Underwriting to Claims Management, Artificial Intelligence Will Transform the Insurance Industry", IBM Corporation.
[32] Walters v OpenAI, LLC, No 23-13843 (11th Cir 2024).

reports, and outstanding loans.[33] A relevant example of an automated UW processes is the controversial CORE system used by Wells Fargo Bank.[34]

2.4.2 'Predictive risk modelling and pricing'

'Predictive risk modelling and pricing' use extensive datasets of sensitive data points to very precisely hedge against a potential future loss and price risk.[35] Examples would include biometric data, health data, behavioural data, socioeconomic data, and medical records (see Supplement A) .[36]

2.4.3 'Eligibility determination'

'Eligibility determination' simplifies and accelerates the time efficiency of UW processes by reducing traditional assessments and using diverse data sources to estimate eligibility. This phase is particularly relevant for Article 22 GDPR where automated outputs strongly influence the final UW decision.[37] The previously mentioned CORE system, though not EU based, is an apt example of the inherent risks in such systems.[38]

2.4.4 Highly Sensitive Data and the EU

The deployment of high-risk AI systems in life and health UW within the EU becomes more contentious when it includes processing of health data or health-related outputs. Under the GDPR, health data fall within the legal category *special categories of personal data* and are by default prohibited to subject to processing unless a specific derogation applies. In UW operations, explicit consent is often treated as the most realistic legal route. However, explicit consent is difficult to treat as 'informed' where the data subject

[33] Swiss Re Institute (2025) 'An Expanded Role for AI in Life & Health Predictive Underwriting'; Salesforce (2025) 'AI in Insurance Underwriting: A Complete Guide'.
[34] *In re Wells Fargo Mortgage Discrimination Litigation*, No. 3:22-cv-00990-JD (N.D. Cal.), Order Re Class Certification, 5 August 2025 (Judge James Donato), Section II.A.
[35] EIOPA (2019) p. 15.
[36] CDW (BizTech Magazine), 'How Artificial Intelligence Is Transforming the Insurance Underwriting Process' (2025).
[37] EIOPA (2019) p. 10–13M; Swiss Re Institute (2025); McKinsey & Company (2025); Economist Impact (2025).
[38] *In re Wells Fargo Mortgage Discrimination Litigation*, No. 3:22-cv-00990-JD (N.D. Cal.), Order Re Class Certification, 5 August 2025, Section II.A., paras. 9, 10 and 45.

cannot reasonably understand the purposes, data categories, enrichment practices, and inferences that drive the decision.[39]

This strain is compounded by the fact that high-risk AI systems are to a certain degree opaque as a prerequisite of their technical functionality.[40] Deficiencies regarding traceability and fabrication often entails that relevant pathways for weightings and decisions cannot be meaningfully explained or audited.[41] The more complex and inference-driven the system, the less feasible it becomes to rely on consent.

This argument is supported by the operation practices of insurers within the EU. Data concerning health are predominately collected via questionaries and granular consent forms, sometimes supplemented by medical wearables.[42] Insurers are also highly cautious of black-box-systems with reference to discriminatory risks, but, additionally, the difficulty of explaining the outcome of ADM-tools to customers.[43]

[39] Article 9(2)(a) and 22(2)(c) GDPR.
[40] Alejandro Barredo Arrieta et al. (2020, p. 83 and p. 100), "Explainable Artificial Intelligence (XAI): Concepts, Taxonomies, Opportunities and Challenges toward Responsible AI," Information fusion 58.
[41] Articles 4(11) and 6(1)(a) GDPR; Article 29 Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (WP251 rev.01); Recital 42 GDPR; DSB (Austria) DSB-D124.909, ECLI:AT:DSB:2020:2020.0.436.002 (8 September 2020); Integritetsskyddsmyndigheten (Sweden), 'Administrative Fine against Klarna after Investigation' (DI-2019-4062, 2022).
[42] EIOPA (2019) pp. 9, 10 and 45.
[43] EIOPA (2019) pp. 42–43 *Big Data Analytics in Motor and Health Insurance: A Thematic Review* (April 2019).

3 EU's AI Act in the Insurance Sector

3.1 Applicable Rules

The central provision governing deployment of high-risk AI systems in this context is Article 27. It requires a Fundamental Rights Impact Assessment (FRIA) before an insurance entity may deploy a relevant AI system. The focal points of the FRIA are the following: (i) identification of the categories of individuals likely to be impacted by the AI system (including the particularised risks to which these identified categories of individuals are likely to be subjected); and (ii) mitigation measures should these risks materialise.

Articles 11–13, in particular Article 12, set out the steps by which adequate levels of traceability are ensured for outputs produced by a deployed high-risk AI system. Article 9 proscribes the implementation of a risk management system wherein foreseeable risks posed by high-risk AI systems vis-á-vis the relevant fundamental rights are practically considered, requiring a sufficient availability of technical knowledge about the deployed AI system. Human oversight is also regulated in Article 14, which proscribe the application of measures tailored in due consideration of the deployed AI system's autonomy and context for deployment.

The FRIA is an expression of Recital 58, which describes the significant risks AI systems can pose in UW for life and health insurance with respect to fundamental rights, mentioning financial exclusion and discrimination.[44]

Article 86 raises the contested issue regarding the right to meaningful explanations about the AI system's operation and results. In this regard, a request for a preliminary ruling is pending before the CJEU.[45]

[44] EIOPA (2019) pp. 29–30 and 43.
[45] Case C-806/24 *'YETTEL BULGARIA' EAD v FB*, request for a preliminary ruling (OJ C/2025/1080, 24.2.2025).

3.2 Requirements and Balancing in Case Law under the Charter of Fundamental Rights of the European Union

3.2.1 Extensive Definition of Personal Data

The Court's case law supports an extensive definition of personal data, including indirect technical markers—such as a string of letters and characters in a digital environment—which, when combined become identifying. Data that are on the surface are non-personal may, cumulatively with other data points, constitute personal data if they can be used to identify the person to whom the data pertain.[46] Because ADM-models can generate extensive inferences, inferred attributes may constitute personal data where they relate to the individual by content, purpose or effect.

It is also to be noted that if the processing of personal data is liable indirectly to reveal special category data, then that data is subject to the GDPR's more restrictive regime under Article 9, regardless of the purpose of processing.[47]

3.2.2 The Applicability of the Right to Privacy and the Corollary Right to Non-Discrimination

The right to protection of personal data is legally relevant for conformity assessment as soon as a legal person retains or has access to personal data from another legal person. This applies irrespective of the data's sensitivity, its subsequent usage, or the intrusion that such retention or access might pose to the individual to whom the data pertains.[48] Article 21 CFR is analysed in light of Article 8 CFR.[49]

[46] Case C-604/22 *IAB Europe* EU:C:2024:170, paras. 45, and 51.
[47] Case C-184/20 *OT v Vyriausioji tarnybinės etikos komisija* EU:C:2022:601.
[48] Case C-311/18 *Schrems II* EU:C:2020:559, para 171.; Joined Cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk and Others* EU:C:2003:294, paras 74 and 75.; Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Others* EU:C:2014:238, paras 33–36; *Ligue des droits humains*, paras. 124 and 126.
[49] *SyRI*, paras. 6.46 and 6.91.

Article 22 GDPR is also applicable when 'automated decision-making' strongly influences a subsequent decision that produces legal or similarly significant outputs, such as credit scoring when it is subsequently used decisively to enter or abstain from entering into a contract.[50] 'Decision' can therefore be a single decision in the context of a string of decisions of which the ultimate decision outwardly affects the individual.[51]

3.2.3 Balancing Legitimate Interests

The right to the protection of personal data is not an absolute right. It needs to be balanced against the functional and contextual purpose of the data processing. [52] However, case law establishes that the purpose must be precise and circumscribed. [53] It also assigns the burden of proof to the processor of the data to demonstrate the purpose and necessity of the processing.[54]

In underwriting, risk assessment and pricing can serve legitimate purposes, including from a societal perspective, insofar as underwriting functions to allocate and spread financial risk.[55] But legitimacy in itself does not negate requirements of contestability and effective remedy where outputs significantly affect individuals.[56] As Hands notes in relation to prediction-based systems for decision-making, the 'objectives of prediction' must be identified and justified, because what appears 'efficient' from a market perspective can still conflict with other goals and rights of consumers. In UW this matters because risk indicators can embed value choices about which correlations count as relevant. This is precisely because those choices can systematically burden certain groups of people unless constrained by law and safeguards.[57]

---

[50] *Schufa*, para. 48–49 and 73.
[51] Ibid. para. 46.
[52] *Schrems II*, para. 172.
[53] *Volker und Markus Schecke and Eifert*, para. 48; *Schwarz*, paras. 33–34; *Ligue des droits humains* para. 136.
[54] *Schrems II*, para. 82.
[55] Recital (4), GDPR; Case C-645/19, *Facebook Ireland and Others* EU:C:2021:483, para. 3.
[56] Recital (4), GDPR; Case C-645/19, *Facebook Ireland and Others* EU:C:2021:483, para. 3.
[57] Hands (2024) p. 88.

3.2.4 Explainability

In this thesis, 'explainability' is used as an umbrella term encompassing 'understandability', 'interpretability', and 'transparency', unless the context requires a more precise distinction. In the context of AI systems, explainability concerns making the decisions or outputs of such systems clear or understandable to humans. In legal discussions on AI and data protection, the term is often associated not only with explaining outputs, but also with broader goals such as 'justification', 'accountability', 'fairness', and 'privacy'.[58]

The Dutch SyRI case is used to clarify the concept of explainability vis-á-vis AI systems. The AI system used by the relevant Dutch authority for public benefits has features corresponding to or similar to those used in life and health insurance (see). The data categories established by the Dutch authority, on which the AI system partially focused, are set out in the list in Supplement C.[59]

Even though the deployer in the case could provide a non-technical explanation of the general process by which outputs were generated and the main categories of data used, it was deemed insufficient.[60] In operational terms, this implies that deployers should be able to provide, at minimum:

- Transparency of the risk indicators utilised, including their purpose, weighting, validation, and objective empirical rationale,
- Auditability and verifiability of the data points and their empirical basis,
- Explainability of the scoring system, and the algorithmic logic by which conclusions are reached.

[58] Hofmann & Pflücke (eds) (2024) p. 241.
[59] *SyRI*, para. 6.45.
[60] Ibid., paras. 6.5(f), 6.54, and 6.94; Article 22(3), GDPR, under which UW measures are generally justified with reference to paragraph 2(a) therein.

The direct implication is that 'human oversight after the fact' may be insufficient where the human reviewer cannot meaningfully examine the system's inputs and weightings, and where 'automation bias' makes such auditing difficult.[61] Meaningful oversight therefore requires access to all relevant data, the ability to understand that data, and the ability to change or significantly influence the decision based thereon. [62]

This point is particularly relevant to UW without prejudice to other varieties of insurances than for life and health, where individuals must be able to understand the reasons for adverse outputs such as higher premiums or denial of coverage. The insurers must be able to audit whether relevant data-based indicators and practices of enrichment produce unfair outputs. [63]

Explainability can, though, potentially lock heads with the protection of intellectual property rights and business secrets.[64] In the case above, The Court has abstained from weighing the interest of intellectual property in relation to explainability.[65] Nevertheless, supplementary guidance can be found in decisions by national courts and DPAs. For example, business interest has been legitimatised as relevant in determining the scope of rendering information regarding personal data processing.[66]

In addition, the commercial interest that is addressed by allowing companies to process data if they gather a customer's consent is also relevant for the adaptation of AI systems in underwriting. It is seemingly presumable that the price optimisation achieved by efficient ADM in underwriting reaches the

[61] Hofmann (2024, pp. 16–17, 21–22 and 27, chapter 1); Biber (2024, p. 189 and pp. 200–201, chapter 7); Hands (2024, p. 213).
[62] Amsterdam Court of Appeal (Gerechtshof Amsterdam), ECLI:NL:GHAMS:2023:793, 4 April 2023, para 3.24; Article 29 Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (WP251 rev.01) p. 21.
[63] *SyRI*, para. 6.87–6.90.
[64] Hofmann (2024, pp. 21 and 29); Article 339 TFEU.
[65] *Schufa Holding AG and Others.*
[66] LG Traunstein, Endurteil vom 22.05.2024 – 6 O 2465/23 **(**GRUR-RS 2024, 12349).

legal threshold for being 'necessary for entering into […] a contract', but not such processing of medical data before providing health or life insurance.[67]

3.2.5 Human Oversight

Human oversight of high-risk AI systems must be meaningful rather than formal. Human intervention that merely corrects errors after the fact may be inadequate where the system's weightings, indicators, and processed data cannot be qualitatively scrutinised, and where automation bias leads to undue deference to the machine's outputs, thereby preserving the underlying risks.[68]

Operational oversight should be performed by personnel who can access the data underlying the output, understand its weightings and implications, and steer the resulting decision-making, if necessary. Domain-specific competencies on the part of the auditing person(s) are therefore essential, meaning expertise not only in the AI system's operation but also in the substantive decision-making context in which it is deployed.[69]

3.2.6 The Right to Non-Discrimination

Explainability serve as a safeguard to avoid, prevent, or minimise the effects of discriminatory or exclusionary practices, whether intentional or not. Even where an individual's circumstances may justify further measures, reliance, wholly or partly, on outputs from an AI system that processes large amounts of data, of which a considerable amount is legally considered sensitive, may violate Article 21 CFR. AI systems, with or without self-learning capabilities, that are trained on large data sets for profiling purposes are inherently prone to producing discriminatory or biased outputs. This occurs when ostensibly neutral factual data give rise to improper false positives or false negatives, particularly in relation to certain categories of people.[70] The right to equal

[67] Article 6(1)(b) and Article 22(2)(a) GDPR; Article 29 Working Party, *Opinion 06/2014* p. 18.
[68] Parasuraman and Manzey (2010, pp. 382–383 and 404–406); Zerilli et al. (2019, pp. 556–558).
[69] Sterz et al. (2024, pp. 2495–2496); Zerilli et al. (2019, pp. 556–557).
[70] SyRI (ECLI:NL:RBDHA:2020:865), paras 6.91–6.93.

treatment in comparable cases is therefore part and parcel of the right to privacy in the context of the processing of personal data.[71]

3.2.7 The Difference in Compliance Requirements between State and Private Entities

Public authorities are generally subject to stricter requirements than private entities. This is illustrated by the original exclusion of processing for functions overlapping with criminal law or motivated by national security interests from the scope of the GDPR in favour of stricter *lex specialis*, such as the Directive 2016/680 and the directive regarding Passenger name record (PNR) data. While the GDPR is largely applicable to private enterprises, state authorities fall under it only insofar as they are not subject to other, stricter laws.[72] A case in point is individual consent: while it may be viable for private actors when individuals often have alternative providers, it is generally unsuitable for public authorities, which typically exercise monopolistic functions in society.

Irrespective of the above, processing of sensitive data is considered a serious interference with Article 8 CFR regardless of the deployer of the relevant processing.[73] Operators of search engines can even be held responsible via verification *post factum* at the request of the data subject, although they merely index and display links without publishing content. Similarly, credit-scoring agencies can produce legal or similarly significant effects for data subjects.[74] The interference of this variety must be balanced against other rights recognised by EU law, such as the right to freedom of information under Article 11 CFR.[75] On this basis, the Court seemingly imposes requirements on certain private actors similar to those to which state authorities are subject, including actors to which insurance companies are comparable in the case of life and health insurance. A key factor justifying

[71] SyRI (ECLI:NL:RBDHA:2020:865), para 6.24.
[72] *Ligue des droits humains* EU:C:2022:257, paras 66–72; Recitals (7), (11), (15) GDPR; Article 6(1), second subparagraph, GDPR.
[73] Case C-136/17 *GC and Others v CNIL* EU:C:2019:773, paras 37, 42, 44.
[74] *GC and Others*, paras. 45–47; *Schufa Holding AG and Others*, paras. 40–49.
[75] *GC and Others*, paras. 57, and 66.

higher scrutiny for private companies, specifically insurance companies in the case of life and health insurance, is their processing of sensitive data. The equation with state authorities is relaxed though for private actors in that 'only' suitable safeguards must be imposed where ADM is applied and fulfils the legal requirements of contractual necessity or consent.[76] Nevertheless, ADM entails particular risks, including discrimination. Decisions in UW resemble the processes by which a private company provided credit scores to customers such as banks.[77] The Court required that the actuarial procedures by which the ADM was driven must be subject to qualitative human oversight and render data subjects a genuine opportunity to contest the output.[78] The following requirements can be assumed to apply equally to insurance companies concerning life and health insurance, or even more so given the heightened sensitivity of the data they process:

- Input data used,
- Parameters and their influence on the rating,
- Links between inputs and outputs,
- Explanation of the rating's implications.

The extent to which the practicalities of the exercising of these rights stretches, can be limited to the rights and freedoms of others, including the freedom to conduct commercial operations. This does not justify a *carte blanche* refusal to disclose meaningful information that ensures contestability but allow insurance entities to prevent disproportionate sharing of trade secrets or intellectual property. In UW, insurers often treat the selection, number and weighting of rating factors as commercially sensitive. The question, therefore, is how to provide sufficiently meaningful information while proportionately limiting disclosure by masking or omitting commercially sensitive information.[79]

[76] Article 6(1), second subparagraph, GDPR.
[77] *Schufa Holding AG and Others*, para. 14.
[78] *CK v Magistrat der Stadt Wien*, para. 33.
[79] EIOPA (2019) p. 34.

4 Analysis

This analysis examines the extent to which AI-supported underwriting in life and health insurance can be conducted within the constraints imposed by the AI Act's high-risk regime and the GDPR, as interpreted in light of the CFR. It is structured around two overlapping themes:

- Ordinary personal data and derived inferences used for profiling, enrichment and risk-scoring.

- Special categories of personal data, especially health data, whose processing triggers raised restrictions to the deployment of high-risk AI systems.

Within each theme the analysis identifies risks, groups of persons who are particularly identified as affected, and compliance measures that translate the legal requirements into operational recommendations of constraint.

4.1 Ordinary Personal Data

High-risk UW AI systems often rely on broad ordinary data (such as credit-related information, transaction patterns, behavioural indicators, and externally sourced datasets), combined with inferences that are not always traceable or explainable to the individual. Risks that are of primary note here is loss of transparency and discriminatory outputs.

4.1.1 Article 22 GDPR and Meaningful Human Oversight

Insurance companies should preferably avoid the applicability of Article 22 GDPR by implementing measures that ensure functional engagement with practical operations where automated outputs decisively shape the steps of UW decisions culminating in legal or similarly significant effects, as back-up to the exemptional ground in Article 22(2)(a). Otherwise, the requirement of consent and its underpinnings have to be fulfilled, which is very difficult. The human reviewer should be able to qualitatively audit the relevant inputs and indicators, assess their influence, identify errors and indirect effects, and modify or halt the ADM whenever necessary. The likelihood of exercised human oversight to be deemed legally inadequate is considerable unless it satisfies the previously stipulated recommendations

4.1.2 Explainability as Contestability

Explainability must function as a vehicle for contestability and effective remedy. This does not require full disclosure of the deployed AI model, including the exposure of intellectual property or business secrets. It does, however, require that the individual(s) affected can understand why an adverse output occurred. This necessitates that the insurer is able to audit the model's logic, including perceived undue bias in inferences or indirect correlations by the means of weightings and enrichment. Tailored XAI-tools for explainability should therefore preferably be applied to make the output and undergirds of the deployed AI model sufficiently intelligible for auditing and contestability.

4.1.3 Framework for Compliance

The compliance structure set out in this study is most workable if it is organised around three overlapping and intertwined pillars—an operational foundation for both the AI Act's ordinances regarding high-risk AI systems and the principles of the GDPR.

The three pillars below operationalise the AI Act's requirements on traceability (Article 13), human oversight (Article 14) and FRIA-grounded mitigation (Article 27) with alignment to the above-referred principles of the GDPR (Article 5).

- Risk indicator governance: The insurer must specify which concrete indicators are used and motivate and explain their purpose, both individually and cumulatively. They must also explain why particular correlations are treated as relevant and how indicators are validated. Where indicators in UW carry obvious risk (such as socioeconomic variables, neighbourhood-based proxy markers, or behavioural data that correlates with protected characteristics), governance must include constraints that prevent biased correlations. Operationally, predetermined indicators with clearly delimited boundaries should be applied. This will safeguard the system from deviating into unbounded enrichment that would potentially undermine fairness.

- Data traceability: Traceability requires that the insurer can verify the existence and accuracy of the relevant input data and meaningfully map how data is sourced, enriched, weighted and used for the output. This would entail logging and other forms of documentation that can be used to achieve explainability. Without systematic functions for adequate contestation of traceability, auditing to ensure non-discrimination becomes illusory. Traceability is also vital to encourage ethical meticulousness in how personnel operate high-risk AI systems in UW; data is used when necessary.

- Algorithmic decision logic: The AI system must produce a coherent logic that understandably connects inputs to outputs in a way that can be validated. In UW, this means that adverse outputs, such as higher premiums or denials, should be explainable through decision-relevant drivers. The insurer needs to be able to show how those drivers objectively relate to the purpose and aims of the UW. The purpose here is not to deliver a technical lecture, but to explain the decision

pathway in a way the affected individual can understand. This enables contestability and facilitates the detection of biased logic affecting protected groups.

While these steps cannot remove all risk, they make compliance verifiable by enabling meaningful oversight and contestability when outputs in underwriting affect individuals in a legally adequate way.

4.1.4 Interim Conclusion

Compliance is best achieved when profiling and data enrichment are restrained by boundaries for what is necessary. Explainability should be implemented at an operationally relevant level for decision-making and meaningful human oversight exercised when outputs considerably affect individuals.

4.2 Special Categories of Personal Data

UW pertaining to life and health insurance entails processing of particularly sensitive data—health data. Health data qualifies as ‘special categories of data’ in the GDPR and is therefore subject to more stringent requirements for compliance. Subsequently, operational safeguards for compliance must be more meticulous due to the certain extent of opacity in AI systems.

4.2.1 The Problem of Consent and AI

The only viable ground upon which processing of health data in UW can be based is consent from the customer. It is similarly assumable here that the achievement of adequate consent is unrealistic (see also). Adequate consent is unrealistic because it requires individuals to understand the scope of processing—specifically how data are enriched, weighted, and used to generate inferences, and how these shape the output and any decision fully or partly based on it. AI systems should therefore in light of the above not include processing of health data to determine the eligibility and pricing of life and health insurance.

4.2.2 A Hybrid Pathway for Compliance

Based on the conditions set out in *Analysis*, warrants, preferably for the insurance entities within the bounds of law, a hybrid application of AI systems. Health data is collected through questionnaires and granular consent mechanisms and assessed in a manner that remains seamlessly documentable and contestable, while ordinary data can be used for administrative verification and checks for inconsistencies.

Ordinary data can also be usefully subject to the deployment of AI systems to measure the assumed health of the prospective insurer since vast sets of non-health-related data, can cumulatively surmise the health of the individual in question. This could enhance price optimisation to the benefit of the pool of consumers. To viably operationalise this hybrid pathway, the inferences drawn from ordinary data that have a considerable effect on determining the applicant's health must strike a fine, but presumably achievable, balance. This balance must ensure that the inferences are not liable to reveal health data while remaining objectively justifiable (e.g., justifiable in terms of their relevance and reasonableness in affecting the outcome of the UW).

4.2.3 Particularly Affected Categories of Persons

AI systems that optimise for higher accuracy in predictions, can perpetuate historical bias by the usage of seemingly neutral indicators or data points. This is why the risk of discrimination risk is inseparable from requirements concerning data privacy, especially regarding explainability. Without clear explanations of the logic behind how the system aggregates, enriches, and infers from large datasets, biases can remain hidden.

As established by the SyRI case, socioeconomic data and social origins, beyond the relevance of, in particular, age and disability in the case of life and health insurance, suscept certain groups of individuals to negative impact by health-related inferences. It is therefore advisable to implement technical

measures to flag certain outcomes if they are considerably influenced by potentially discriminatory data points or inferences.

4.2.4 Interim Conclusion

In the context of special categories of data—specifically health data—insurers should avoid the usage of AI systems and instead rely on human-led assessment. AI systems can nevertheless be used within certain boundaries if it is based on ordinary data in combination with rigorous auditing for undue bias.

5 Conclusion

In conclusion, high-risk AI systems in UW can be reconciled with the AI Act and GDPR, in light of CFR, under specified conditions. These conditions need to variously prioritise contestability, necessity, traceability, and non-discrimination over commercially desirable price optimisation. Technical systems cannot be treated as mere technical tools when they affect access to significant financial protection through pricing and prerequisites for eligibility.

Concerning ordinary personal data, fulfilment of legal conditions for compliance is best achieved if insurers define the boundaries for data enrichment to that which is necessary, not available. In addition, insurers should tailor and implement XAI-tools for comprehensibility of the underlying data of outputs. Meaningful human oversight where automated outputs decisively influence UW has to be integrated with these measures. In context of special categories of data, a hybrid pathway should aptly be applied in which decisive health assessments are human-led, and AI systems are used as supporting functions that enhance efficiency, including for the purpose of price optimisation.

Certain risks regarding data privacy, including the risk of insufficient traceability, are not fully reversible. However, a robust structure around risk-indicator governance, data traceability, and algorithmic decision rationale, reduces the margin of error and aligns operations in UW with the EU's normative pillars of data protection and non-discrimination.

Future research should further investigate the parameters delimiting the definitions of provider and deployer, as these distinctions entail divergent compliance requirements. Additionally, further legal clarity is needed on how to balance providing meaningful information about a deployed AI system's logic to the data subject with masking or omitting commercially sensitive information. The definition of AI system also merits investigation since interpretative ambiguities may enable circumvention of desirable requirements in the AI Act.

Supplement A

Group	Examples of rating factor included in this category	Influence on final premium
Health at underwriting	Medical condition at the time of underwriting	High
Age	Age of customer	High
Behavioural data	Behavioural data	Low
Claims and experience	Claims history	High
Cover	Sum insured, number of people insured, deductibles	High
Lifestyle	smoker, sports, dangerous activity, alcohol consumption	High
Affluence	Profession, salary, payment periodicity, education	High
Business	Number of employees, type of business	High
Community	Community rating	High
Location	Postal code, area of use, city of residence	High
Non-risk	Competition, segmentation, sales channel	Low
Other	Miscellaneous	Low

Source: EIOPA BDA thematic review

Supplement B

Description of the SyRI Risk Model

1. Overview and Regulatory Context

SyRI (Systeem Risico Indicatie) was an automated risk assessment system used by Dutch authorities to detect potential abuse and fraud in relation to social security, tax, and labour law schemes. The system is functionally similar to the type of high-risk AI systems referred to in Annex III, point 5(c), of the EU AI Act, namely systems used to assess the eligibility or compliance of individuals in relation to public benefits and related schemes. The SyRI model combined and analysed large volumes of administrative data to produce "risk reports" on natural and legal persons who were deemed to present an increased risk of unlawful use of public funds or non-compliance with legal obligations. The information in the current paragraph and below are extracted from paras. 4.17, 4.23, 4.29, and 4.30 Dutch SyRI.

2. Data Categories Used in SyRI

The risk model operated on predefined categories of data relating to both natural and legal persons. These categories included:

- Work data – Data used to establish the work performed by a person.
- Administrative measures and sanctions – Data evidencing that an administrative fine or other administrative measure has been imposed on a natural or legal person.
- Tax data – Data used to establish the tax obligations of a natural or legal person
- Movable and immovable property – Data used to establish the possession and use of certain property by a natural or legal person.

- Exclusion from benefits – Data proving that a person is not eligible for social assistance or other benefits.

- Trade data – Data used to establish the nature and activities of a legal person.

- Housing data – Data used to establish the actual or other place of residence or place of business of a natural or legal person.

- Identifying data:

    - For natural persons: name, address, city, postal address, date of birth, gender, and administrative characteristics.

    - For legal persons: name, address, postal address, legal form, place of business, and administrative characteristics.

- Civic integration data – Data used to establish whether an obligation to participate in a civic integration programme has been imposed on a person.

- Compliance data – Data used to establish the compliance history of a natural or legal person with legislation and regulations.

- Education data – Data used to determine financial support for the funding of education.

- Pension data – Data used to establish pension entitlements.

- Reintegration data – Data used to establish whether reintegration obligations have been imposed on a person and whether they have been, or are being, fulfilled.

- Debt burden data – Data used to establish any debts of a natural or legal person.

- Social benefits, allowances and subsidies – Data used to establish the financial support provided to a natural or legal person.

- Permits and exemptions – Data used to establish for which activities a natural or legal person has requested or obtained permission.

- Health care insurance data – Data used to establish whether a person is insured under the Healthcare Insurance Act.

3. Definition and Function of the Risk Model

For the purposes of the SyRI framework, a risk model was defined as a model composed of predetermined indicators designed to signal whether there is an increased risk of:

- unlawful use of government funds and schemes in the field of social security and income-dependent schemes,

- tax and social security fraud, or

- non-compliance with labour law obligations.

In other words, the risk model operationalised a set of abstract 'risk indicators' against the data categories listed above, in order to identify persons, entities, or addresses that should be flagged for further investigation.

4. Data Processing Phases

SyRI's data processing and risk assessment were structured in two distinct phases:

Phase 1 – Collation, Pseudonymisation, and Initial Risk Selection

Collation and pseudonymisation

- The responsible administrative body (IB) collated records from various sources.

Personal identifiers (such as names, company names, citizen service numbers, and addresses) were replaced with codes (pseudonyms).

Automated comparison with the risk model

- The pseudonymised source file was automatically checked against the risk model, using all predefined indicators.

- This automated comparison generated “potential hits”, i.e. cases indicating an increased risk of fraud or unlawful use of public funds.

Creation of key file

The IB created a separate key file linking each pseudonym to the corresponding personal or company identifiers (name, citizen service number, address, etc.).

Decryption of flagged cases

- Where the risk model flagged specific natural or legal persons or addresses as increased-risk cases, the relevant records were decrypted using the key file.

- All data related to these increased-risk cases (excluding the key file itself) were then transmitted to the Minister for the second phase of analysis, carried out by the analysis unit of the Social Affairs and Employment Inspectorate.

Destruction of SyRI project files

- The IB was required to destroy any SyRI project files remaining in its possession within four weeks of forwarding the data to the Minister.

This destruction was recorded in an official report.

Phase 2 – In-Depth Analysis and Definitive Risk Selection

Further analysis of decrypted data

- In the second phase, the analysis unit of the Social Affairs and Employment Inspectorate examined the decrypted data more closely.

Assessment of ‘worthiness of investigation’

- The data were evaluated to determine whether the cases were “worthy of investigation,” i.e. whether they warranted further enforcement or inspection steps.

Definitive risk selection and reporting

- This assessment resulted in a definitive risk selection, narrowing the set of cases to those considered sufficiently serious or credible.

- On the basis of this definitive selection, the Minister submitted risk reports to the competent authorities.

Supplement C

Overview of SyRI Data Categories by Functional Group

For ease of reference, the data categories used in SyRI can be grouped into three functional clusters: Employment & Trade Data; Financial Data; and Administrative & Legal Data.

- **Employment & Trade Data**
    - Work data
    - Trade data
    - Reintegration data
    - Compliance data
    - Identifying data
    - Health insurance data
- **Financial Data**
    - Tax data
    - Debt burden data
    - Benefits / subsidies
    - Pension data
    - Property data
    - Education funding

- **Administrative & Legal Data**
    - Grounds for exclusion
    - Permits & exemptions
    - Civic integration data
    - Housing data

Bibliography

EU Cases

Case C-136/17 GC and Others [2019].

Case C-184/20 OT v Vyriausioji tarnybinės etikos komisija [2022].

Joined Cases C-92/09 and C-93/09 Volker und Markus Schecke and Eifert [2010].

Joined Cases C-293/12 and C-594/12 Digital Rights Ireland Ltd and Others [2014].

Joined Cases C-465/00, C-138/01 and C-139/01 Österreichischer Rundfunk and Others [2003].

Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems (Schrems II) [2020].

Case C-604/22 IAB Europe ASBL v Gegevensbeschermingsautoriteit (IAB Europe) [2024].

Case C-634/21 SCHUFA Holding AG and Others [2023].

Case C-645/19 Facebook Ireland and Others [2021].

Case C-806/24 Yettel Bulgaria EAD [pending].

Case C-817/19 Ligue des droits humains ASBL [2022].

Case C-291/12 Schwarz [2013].

Case C-203/22 CK v Magistrat der Stadt Wien (Dun & Bradstreet Austria) [2025].

District Court of The Hague (Rechtbank Den Haag), judgment of 5 February 2020, ECLI:NL:RBDHA:2020:865 (SyRI).

Amsterdam Court of Appeal (Gerechtshof Amsterdam), judgment of 4 April 2023, ECLI:NL:GHAMS:2023:793.

Landgericht Traunstein, Endurteil of 22 May 2024, 6 O 2465/23, GRUR-RS 2024, 12349.

Tribunale ordinario di Firenze, Sezione imprese, order of 14 March 2025, RG 11053/2024, https://www.ambientediritto.it/giurisprudenza/tribunale-ordinario-di-firenze-sez-imprese-14-03-2025-ordinanza-rg-11053-2024/.

Datenschutzbehörde (Austrian Data Protection Authority), decision of 8 September 2020, DSB-D124.909, ECLI:AT:DSB:2020:2020.0.436.002.

Integritetsskyddsmyndigheten (IMY) (Swedish Authority for Privacy Protection), 'Administrative fine against Klarna after investigation' (DI-2019-4062, 2022), https://www.imy.se/en/news/administrative-fine-against-klarna-after-investigation/.

Third Countries Cases

United States Court of Appeals for the Eleventh Circuit, Mark Walters v OpenAI, L.L.C., No. 23-13843, judgment 1 April 2024, https://cases.justia.com/federal/appellate-courts/ca11/23-13843/23-13843-2024-04-01.pdf.

United States District Court for the Northern District of California, Williams v Wells Fargo Bank, (In re Wells Fargo Mortgage Discrimination Litigation), Case No. 3:22-cv-00990, filings 2022–[ongoing].

EU Regulations

Charter of Fundamental Rights of the European Union (2012/C 326/02).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing

of personal data and on the free movement of such data and repealing Directive 95/46/EC (GDPR).

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (AI Act).

Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act).

Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II).

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (Text with EEA relevance).

Literature

Barredo Arrieta, Alejandro, Natalia Díaz-Rodríguez, Javier Del Ser, Adrien Bennetot, Siham Tabik, Alberto Barbado, Salvador García, Sergio Gil-López, Daniel Molina, Richard Benjamins, Raja Chatila, and Francisco Herrera. "Explainable Artificial Intelligence (XAI): Concepts, Taxonomies, Opportunities and Challenges toward Responsible AI." Information Fusion 58 (June 2020): 82–115. https://doi.org/10.1016/j.inffus.2019.12.012

Demková, Simona, Automated Decision-Making and Effective Remedies: The New Dynamics in the Protection of EU Fundamental Rights in the Area of Freedom, Security and Justice (Edward Elgar Publishing 2023) (Elgar Studies in European Law and Policy).

Hands, Lily Alexandra, Just(ifying) Algorithms: Data-Driven Automated Predictions About Unobservable Targets and the General Data Protection Regulation (PhD thesis, University of Cambridge 2024).

Hofmann, Herwig C. H. & Felix Pflücke (eds), Governance of Automated Decision-Making and EU Law (Oxford University Press 2024).

Kleineman, Jan, 'Rättsdogmatisk metod', in Juridisk metodlära (2nd edn, Norstedts Juridik 2018) 21.

Nolan, Katherine Anne, 'The individual in EU data protection law' (PhD thesis, London School of Economics and Political Science 2023), .

Parasuraman, Raja, and Dietrich H. Manzey. "Complacency and Bias in Human Use of Automation: An Attentional Integration." *Human Factors* 52(3) (2010) 381–410, https://doi.org/10.1177/0018720810376055.

Sterz, Sarah, Kevin Baum, Sebastian Biewer, Holger Hermanns, Anne Lauber-Rönsberg, Philip Meinel, and Markus Langer. "On the Quest for Effectiveness in Human Oversight: Interdisciplinary Perspectives." In *Proceedings of the 2024 ACM Conference on Fairness, Accountability,*

and Transparency (Association for Computing Machinery 2024) 2495–2507, https://doi.org/10.1145/3630106.3659051.

Zerilli, John, Alistair Knott, James Maclaurin, and Colin Gavaghan. "Algorithmic Decision-Making and the Control Problem." *Minds and Machines* 29 (2019) 555–578, https://doi.org/10.1007/s11023-019-09513-7.

Articles

Allianz Research, Allianz Global Insurance Report 2025: Rising demand for protection
(2025), https://www.allianz.com/en/economic_research/insights/publications/specials_fmo/250527-global-insurance-report.html.

Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP 217, adopted 9 April 2014), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251 rev.01, 22 August 2018), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.

CDW Corporation, 'How Artificial Intelligence Is Transforming the Insurance Underwriting Process', BizTech Magazine (CDW 2025), https://biztechmagazine.com/article/2025/03/how-artificial-intelligence-transforming-insurance-underwriting-process.

Damien Charlotin, 'Hallucinations', DamienCharlotin.com (blog), accessed 9 December 2025, https://www.damiencharlotin.com/hallucinations/.

Economist Impact, Underwriting the future: the role of artificial intelligence in insurance (2025), https://impact.economist.com/new-

globalisation/underwriting-the-future-the-role-of-artificial-intelligence-in-insurance.

EIOPA, Big Data Analytics in motor and health insurance: A thematic review (EIOPA 2019), https://register.eiopa.europa.eu/Publications/EIOPA_BigDataAnalytics_ThematicReview_April2019.pdf.

EIOPA, Big Data Analytics in motor and health insurance: Fact sheet (EIOPA 2019), https://register.eiopa.europa.eu/Publications/EIOPA_BigDataAnalytics_Factsheet_April2019.pdf.

Euronews, 'European Commission delays full implementation of AI Act to 2027' (19 November 2025), https://www.euronews.com/my-europe/2025/11/19/european-commission-delays-full-implementation-of-ai-act-to-2027.

European Union Agency for Fundamental Rights (FRA), Bias in Algorithms, Artificial Intelligence and Discrimination— Report (Publications Office of the European Union 2022).

Fortune Business Insights, Health Insurance Market Size, Share & Industry Analysis (2024), https://www.fortunebusinessinsights.com/health-insurance-market-101985.

IBM, 'AI hallucinations', IBM Think, https://www.ibm.com/think/topics/ai-hallucinations.

IBM, 'Overfitting', IBM Think, https://www.ibm.com/think/topics/overfitting.

IBM Institute for Business Value, From Underwriting to Claims Management, Artificial Intelligence Will Transform the Insurance Industry (IBM Corporation 2025), https://www.ibm.com/thought-leadership/institute-business-value/report/ai-insurance.

McKinsey & Company, The Future of AI in the Insurance Industry (2025), https://www.mckinsey.com/industries/financial-services/our-insights/the-future-of-ai-in-the-insurance-industry.

OpenAI, 'Why language models hallucinate', OpenAI Blog (21 September 2023), https://openai.com/index/why-language-models-hallucinate/.

Salesforce, AI in Insurance Underwriting: A Complete Guide (Salesforce 2025), https://www.salesforce.com/financial-services/artificial-intelligence/ai-in-insurance-underwriting/.

SC World, 'EU proposes regulatory changes to ease compliance with AI Act and GDPR' (2025), https://www.scworld.com/brief/eu-proposes-regulatory-changes-to-ease-compliance-with-ai-act-and-gdpr.

Swiss Re Institute, An Expanded Role for AI in Life & Health Predictive Underwriting (Swiss Re 2025), https://www.swissre.com/reinsurance/insights/ai-predictive-underwriting-life-and-health.html.

TechPolicy.Press, 'What's driving the EU's AI Act shake-up' (2025), https://www.techpolicy.press/whats-driving-the-eus-ai-act-shakeup/.