EXTERNAL LEGAL OPINION

MEMORANDUM

TO: Jennifer Hartley, CEO, TechNova AI Systems Inc.
Sarah Mitchell, General Counsel, TechNova AI Systems Inc.
Board of Directors, TechNova AI Systems Inc.

FROM: Dr. Friedrich Bauer, Partner
Bauer & Partners LLP
AI Act and Technology Law Specialists

DATE: September 22, 2024

RE: LEGAL OPINION ON AI ACT AND GDPR COMPLIANCE ISSUES
DATASURE ALLEGATIONS - RISK ASSESSMENT AND STRATEGIC RECOMMENDATIONS

CLASSIFICATION: ATTORNEY-CLIENT PRIVILEGED - CONFIDENTIAL

==
I. ENGAGEMENT AND SCOPE
==

Bauer & Partners LLP has been engaged by TechNova AI Systems Inc. ("TechNova" or "the Client") to provide expert legal opinion on compliance with Regulation (EU) 2024/1689 (the "AI Act") and Regulation (EU) 2016/679 (the "GDPR") in connection with TechNova's InsightPredict Analytics Platform (the "System").

This opinion is provided in response to allegations made by DataSure in a letter dated September 5, 2024, and in support of TechNova's strategic decision-making regarding potential settlement, remediation, or defense.

SCOPE OF OPINION:

This opinion addresses:
1. Analysis of AI Act compliance with respect to Articles 6, 9, 10, and 14
2. Analysis of GDPR compliance with respect to Articles 5(1)(a), 9, and 22
3. Assessment of regulatory enforcement likelihood and potential penalties
4. Evaluation of potential civil liability exposure

5. Strategic recommendations for resolution

This opinion does NOT address:
- Detailed technical analysis of algorithms (technical experts separately engaged)
- Employment law discrimination claims under national law (outside our expertise)
- Tax implications of settlement or penalties
- Reputational or business strategy considerations (business consultants to advise)

LIMITATIONS:

This opinion is based on:
- Information provided by TechNova (documents, interviews, technical explanations)
- DataSure's complaint letter and publicly available information
- Our expertise in EU data protection and AI regulation law
- Current state of law as of September 2024

This opinion does NOT constitute:
- Guarantee of any particular outcome in litigation or regulatory proceedings
- Legal advice on settlement terms (separate engagement for settlement negotiation)
- Representation in any proceedings (separate engagement letter required)

==

II. EXECUTIVE SUMMARY

==

BOTTOM LINE ASSESSMENT:

TechNova faces substantial regulatory and civil liability risk arising from algorithmic bias in the System. The core allegations made by DataSure are legally well-founded and supported by TechNova's own internal testing.

KEY FINDINGS:

1. AI ACT ARTICLE 10 (DATA GOVERNANCE): HIGH RISK OF VIOLATION
- Training data containing historical bias violates Article 10's requirement that data be "appropriate" and examined for "possible biases"
- Enforcement likelihood: 75-85%
- Potential penalties: €3-8 million

2. AI ACT ARTICLE 9 (RISK MANAGEMENT): MEDIUM-HIGH RISK OF VIOLATION
- Inadequate identification and mitigation of discrimination risks
- Fundamental Rights Impact Assessment not conducted
- Enforcement likelihood: 65-75%
- Potential penalties: €2-6 million

3. AI ACT ARTICLE 14 (HUMAN OVERSIGHT): MEDIUM RISK OF VIOLATION
- System design may insufficiently enable meaningful human oversight
- Automation bias concerns supported by 78% correlation
- Enforcement likelihood: 40-60%
- Potential penalties: €1-4 million

4. GDPR ARTICLE 5(1)(a) (FAIRNESS): HIGH RISK OF VIOLATION
- Systematic discriminatory outcomes violate fairness principle
- EDPB guidance supports this interpretation
- Enforcement likelihood: 80-90%
- Potential penalties: €3-7 million

5. GDPR ARTICLE 9 (SPECIAL CATEGORIES): MEDIUM RISK OF VIOLATION
- Biometric processing legal basis questionable
- Inference of protected characteristics legally complex
- Enforcement likelihood: 50-65%
- Potential penalties: €2-5 million

TOTAL REGULATORY EXPOSURE: €11-30 million (before cooperation credit)

CIVIL LIABILITY EXPOSURE: €20-80 million (discrimination claims, depends on number of plaintiffs and damages methodology)

STRATEGIC RECOMMENDATION:

Settlement with DataSure is strongly recommended. Settlement provides:
- Controlled resolution at substantially lower cost (€10-13M vs. €30-110M litigation exposure)
- Opportunity for reputational rehabilitation
- Business continuity
- Certainty vs. years of litigation uncertainty

The legal, financial, and business case for settlement is compelling.

==
==
III. AI ACT COMPLIANCE ANALYSIS
==
==

A. Article 6 - High-Risk AI System Classification

LEGAL STANDARD:

Article 6(2) provides that AI systems listed in Annex III shall be considered high-risk.

Annex III, Section 4 includes: "AI systems intended to be used for employment, workers management and access to self-employment, notably for: (a) recruitment and selection of persons; (b) making decisions on promotion and termination; (c) task allocation; (d) monitoring and evaluation of performance and behavior."

ANALYSIS:

The System clearly falls within Annex III, Section 4. It performs all four enumerated functions:
- (a) Candidate screening and recruitment recommendations
- (c) Workforce optimization and task allocation
- (d) Performance evaluation and behavior monitoring

TechNova cannot credibly argue the System is not high-risk. This is black-letter classification with no interpretive flexibility.

Article 6(3) provides a narrow exclusion for systems that do not pose significant risk of harm to health, safety, or fundamental rights. This exclusion clearly does NOT apply given:
- Fundamental rights at stake (non-discrimination, worker rights)
- Material impact on livelihood and economic security
- Scale (450,000 affected individuals)
- Demonstrated discriminatory outcomes

CONCLUSION: System is definitively high-risk under Article 6(2) and Annex III(4).

CONSEQUENCE: System must comply with all Chapter III, Section 2 requirements (Articles 8-15).

ENFORCEMENT RISK: None (classification is clear, not discretionary).

B. Article 10 - Data and Data Governance

LEGAL STANDARD:

Article 10(2) requires that training, validation, and testing datasets be:
- "relevant, sufficiently representative, and free of errors"
- "appropriate to the intended purpose"
- Subject to appropriate data governance practices

Article 10(3) requires examination of training data for "possible biases."

ANALYSIS:

1. "APPROPRIATE" REQUIREMENT:

The term "appropriate" must be interpreted purposively in light of the AI Act's objectives (Recital 1: "ensure safety and fundamental rights").

Training data that embeds historical discrimination cannot be "appropriate" for an employment AI system where Article 21 of the Charter prohibits discrimination.

TechNova's training data includes performance evaluations from periods when source organizations had documented gender pay gaps and promotion disparities. Using these biased labels as "ground truth" trains models to replicate bias.

This violates the "appropriate" requirement. The training data is inappropriate precisely because it teaches discriminatory patterns.

COUNTERARGUMENT:
TechNova might argue that historical data is the only available data, and the data accurately reflects historical reality.

RESPONSE:
Article 10 does not permit use of data merely because it's available or historically accurate. The data must be appropriate to the intended purpose. If historical data is biased, it must be:
- Excluded from training set
- Corrected/relabeled to remove bias
- Supplemented with bias mitigation techniques
- Subjected to fairness constraints

Simply using biased data because it exists violates Article 10.

LEGAL PRECEDENT:
While direct AI Act enforcement precedent does not yet exist (new regulation), analogous product safety and medical device law demonstrates that "garbage in,

garbage out" is not a defense. Manufacturers must ensure inputs are appropriate, not merely available.

2. "EXAMINATION FOR POSSIBLE BIASES" REQUIREMENT:

Article 10(3) explicitly requires examination of training data for "possible biases."

TechNova conducted some bias testing during development but failed to identify:
- Gender bias (7-8 point differential)
- Age bias (systematic underrating of older employees)
- Ethnic/national origin bias (3-6 point differentials)

Either:
(a) TechNova did not conduct adequate bias examination, OR
(b) TechNova conducted examination but failed to act on findings

Both scenarios violate Article 10(3).

The bias is statistically significant and readily discoverable with appropriate testing methodologies (which are well-established in academic literature and industry practice). Failure to identify such substantial bias demonstrates inadequate examination.

3. DATA GOVERNANCE PRACTICES:

Article 10(4) requires "appropriate" data governance practices.

TechNova's data governance appears deficient in:
- Insufficient provenance tracking (which organizations, which periods)
- Inadequate bias auditing of source data
- Lack of processes for identifying and remediating biased labels
- No clear policies for excluding problematic data

CONCLUSION ON ARTICLE 10:

VIOLATION: YES - Strong evidence of Article 10(2) and (3) violations

ENFORCEMENT LIKELIHOOD: 75-85%

RATIONALE FOR HIGH LIKELIHOOD:
- Clear legal standard
- Documented violation (biased outcomes traceable to training data)
- Direct causation (biased data → biased models → discriminatory outcomes)
- Policy priority (fundamental rights protection)
- Ample evidence (TechNova's internal testing corroborates DataSure's findings)

POTENTIAL PENALTIES:

Article 99(3): Up to €15,000,000 or 3% of total worldwide annual turnover, whichever is higher.

TechNova turnover (2023): €87 million
- 3% of turnover: €2.61 million
- Maximum: €15 million

LIKELY PENALTY RANGE (if violation found): €3-8 million

FACTORS AFFECTING PENALTY:
- Mitigating: Good faith remediation efforts, cooperation with authorities, first violation
- Aggravating: Fundamental rights harm, scale of impact (450K individuals), failure to self-identify earlier

BEST ESTIMATE: €4-6 million (mid-range with cooperation credit)

C. Article 9 - Risk Management System

LEGAL STANDARD:

Article 9 requires providers to establish, implement, document, and maintain a risk management system constituting a continuous iterative process throughout the AI system lifecycle.

Article 9(2) specifies that risk management must:
(a) Identify and analyze known and reasonably foreseeable risks
(b) Estimate and evaluate risks arising during intended use and foreseeable misuse
(c) Evaluate other risks based on post-market monitoring data
(d) Adopt appropriate risk management measures

ANALYSIS:

1. RISK IDENTIFICATION (Article 9(2)(a)):

"Known and reasonably foreseeable risks" for employment AI systems clearly include algorithmic bias and discrimination.

This is well-established:
- Extensive academic literature on algorithmic bias (2010s-present)
- OECD AI Principles (2019) emphasize fairness
- IEEE, ISO, and other standards bodies have developed fairness frameworks
- Prior enforcement actions and media coverage of algorithmic discrimination (e.g., Amazon recruitment tool, HireVue facial analysis)
- Article 10(3) itself requires bias examination (acknowledging bias as known risk)

A reasonable AI provider developing an employment system in 2020-2021 would foresee bias risk.

TechNova's internal compliance report (August 2024) acknowledges "inadequate bias risk assessment" - admission that risk identification was deficient.

2. RISK ANALYSIS INCLUDING FUNDAMENTAL RIGHTS (Article 9(2)(b)):

Recital 27 provides that risk management must consider "risks to health, safety and fundamental rights."

Article 9(2)(b) requires estimation and evaluation of risks arising from "intended use."

Employment decision-making clearly implicates fundamental rights:
- Charter Article 21 (non-discrimination)
- Charter Articles 7-8 (privacy, data protection)
- Charter Article 31 (fair working conditions)

TechNova did not conduct Fundamental Rights Impact Assessment (FRIA). While FRIA is not explicitly required by Article 9 (unlike DPIA under GDPR Article 35), Recital 27's emphasis on fundamental rights suggests FRIA is best practice for high-risk systems with clear fundamental rights implications.

Failure to assess fundamental rights impacts constitutes inadequate risk analysis under Article 9(2)(b).

3. RISK MITIGATION MEASURES (Article 9(4)):

Article 9(4) requires adoption of "appropriate risk management measures."

TechNova implemented some measures:
- Fairness metrics monitoring
- Balanced sampling in some models
- User training on system limitations

However, these measures were clearly insufficient:
- Did not prevent 7-8 point gender bias
- Did not prevent age-related bias
- Did not prevent ethnic bias

Inadequate mitigation measures that fail to prevent known risks violate Article 9(4).

COUNTERARGUMENTS:

Perfect fairness is impossible (fairness-accuracy trade-offs):
- Some validity to this argument (acknowledged in academic literature)
- However, Article 9 does not require perfect risk elimination
- Article 9 requires "appropriate" risk management measures
- 7-8 point bias differential is substantial, not minimal residual bias
- More aggressive fairness constraints were technically feasible (deployed September 2024, reducing bias 70%)

State of the art in 2020-2021:
- TechNova might argue that bias mitigation techniques were less developed when System was built (2020-2021)
- Some validity - field has evolved rapidly
- However, basic fairness testing and bias mitigation were established by 2020
- Google, IBM, Microsoft had published fairness toolkits pre-2020
- Academic literature on fairness constraints, bias testing existed

These counterarguments provide partial mitigation but do not eliminate liability. They may reduce penalty severity but do not defeat violation finding.

CONCLUSION ON ARTICLE 9:

VIOLATION: LIKELY - Evidence of inadequate risk management

ENFORCEMENT LIKELIHOOD: 65-75%

RATIONALE:
- Clearer than Article 9 (which is more judgmental and subjective)

- But some factual questions (what was "reasonably foreseeable" in 2020-2021?)
- TechNova has stronger defenses here than Article 10
- However, failure to identify readily discoverable bias weakens defense

POTENTIAL PENALTIES:

Article 99(3): Up to €15,000,000 or 3% of total worldwide annual turnover

LIKELY PENALTY RANGE (if violation found): €2-6 million

BEST ESTIMATE: €3-5 million (with cooperation credit)

D. Article 14 - Human Oversight

LEGAL STANDARD:

Article 14(1) requires high-risk AI systems to be "designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which the AI system is in use."

Article 14(4) requires measures enabling humans to:
(a) Fully understand AI system capacities and limitations
(b) Remain aware of automation bias
(c) Correctly interpret system output
(d) Decide not to use or override/reverse output
(e) Intervene or interrupt system operation

ANALYSIS:

Article 14 is legally complex because it addresses both system design (provider obligation) and actual human behavior in deployment (deployer/user behavior).

1. SYSTEM DESIGN FOR OVERSIGHT (Article 14(1)):

Provider must design system to enable effective oversight. This includes:
- Explainability features
- User interface design
- Training materials
- Documentation

TechNova's system provides:
✓ Numerical scores and rankings
✓ Some feature importance information
✓ User manuals and training
~ Limited natural language explanations
~ Limited counterfactual explanations
~ Insufficient uncertainty quantification

ASSESSMENT: System design PARTIALLY adequate for oversight, but could be substantially better.

Academic research on human-AI decision-making demonstrates that numerical scores without rich explanations often lead to automation bias. Best practices include:

- Salient display of uncertainty
- Explicit prompts to exercise independent judgment
- Structured decision-making workflows
- Easy override mechanisms with no penalties

TechNova's original system design (pre-September 2024 enhancements) was suboptimal in these regards.

2. AUTOMATION BIAS AND EFFECTIVE OVERSIGHT (Article 14(4)(b)):

Article 14(4)(b) specifically requires measures enabling humans to "be aware of the possible tendency to automatically rely on or over-rely on the output produced by a high-risk AI system ('automation bias')."

Evidence of potential automation bias:

- 78% correlation between recommendations and decisions
- Limited override rates (3.2% pre-enhancement)
- HR user reports of difficulty understanding reasoning

COUNTERARGUMENTS:

High correlation may reflect system quality, not automation bias:

- If system provides genuinely valuable insights, humans may agree with recommendations
- Agreement ≠ automation bias per se
- Need evidence of inappropriate deference, not merely agreement

Humans do override in some cases:

- 3.2% documented overrides (22% if including adjustments)
- Shows human agency exists

Deployers (clients) are responsible for effective oversight:
- Article 14 imposes obligations on providers (system design) AND deployers (actual oversight)
- Article 26 separately addresses deployer obligations
- TechNova cannot control how clients actually use the system

ANALYSIS OF ARGUMENTS:

These are TechNova's strongest defenses. Article 14 is the most arguable of the alleged violations.

However:
- 78% correlation is quite high, suggesting limited independent evaluation
- 3.2% override rate is quite low (though improved to 12% with enhancements)
- System design choices (prominent score displays, limited explanations) may encourage over-reliance
- Academic research supports concern about automation bias in this context

LEGAL UNCERTAINTY:

Article 14 enforcement involves factual assessment of whether oversight is "effective." This is inherently somewhat subjective and case-specific.

No enforcement precedent exists yet (new regulation).

Regulatory authorities may interpret Article 14 strictly (effective oversight requires demonstrable human independent judgment) or more leniently (technical capability to override is sufficient).

CONCLUSION ON ARTICLE 14:

VIOLATION: POSSIBLE - Weakest of the alleged violations

ENFORCEMENT LIKELIHOOD: 40-60%

RATIONALE:
- More legally and factually complex than Articles 9 and 10
- TechNova has stronger defenses
- Some evidence of human oversight (overrides, adjustments)
- However, automation bias concerns supported by evidence
- Unclear how authorities will interpret "effective" oversight

POTENTIAL PENALTIES:

Article 99(3): Up to €15,000,000 or 3% of total worldwide annual turnover

LIKELY PENALTY RANGE (if violation found): €1-4 million

BEST ESTIMATE: €2-3 million (with cooperation credit)

E. Cumulative AI Act Assessment

OVERALL AI ACT COMPLIANCE: NON-COMPLIANT

LIKELY VIOLATIONS:
- Article 10: High likelihood (75-85%)
- Article 9: Medium-high likelihood (65-75%)
- Article 14: Medium likelihood (40-60%)

IF ALL THREE VIOLATIONS FOUND:

Theoretical maximum: €45 million (3 x €15 million)

However, Article 99(1) provides that penalties must be "effective, proportionate and dissuasive" and Article 99(2) requires consideration of:
- Nature, gravity and duration of infringement
- Intentional or negligent character
- Actions taken to mitigate damage
- Degree of responsibility
- Manner in which authorities became aware (self-reporting vs. complaint)
- Cooperation with authorities
- Previous infringements
- Financial situation of provider

Realistically, cumulative penalties would be lower than theoretical maximum, considering:
- All violations relate to single system and common root cause (training data bias)
- Good faith efforts (some risk management, recent remediation)
- First-time violation (new regulation)
- Cooperation (if TechNova cooperates with investigation)
- Proportionality to turnover (€87M revenue)

REALISTIC CUMULATIVE AI ACT PENALTIES:
- Without cooperation: €10-18 million

- With cooperation and remediation: €6-12 million
- With settlement showing good faith: €3-8 million (or possibly forbearance)

BEST ESTIMATE WITH COOPERATION: €6-10 million

==
IV. GDPR COMPLIANCE ANALYSIS
==

A. Article 5(1)(a) - Fairness Principle

LEGAL STANDARD:

Article 5(1)(a): "Personal data shall be processed lawfully, fairly and transparently."

"Fairness" is a foundational GDPR principle but not extensively defined in the regulation itself.

EDPB GUIDANCE:

EDPB Guidelines and national DPA guidance interpret "fairness" to include:
- Non-discrimination
- Reasonable expectations of data subjects
- No deception or unfair disadvantage
- Balance of interests

Several DPAs have indicated that algorithmic processing producing discriminatory outcomes violates the fairness principle.

ANALYSIS:

Systematic bias disadvantaging protected groups clearly violates fairness:
- Gender discrimination: Unfair to women (lower scores for same qualifications)
- Age discrimination: Unfair to older workers (systematic underrating)
- Ethnic bias: Unfair to non-Western European candidates

LEGAL PRECEDENT:

While direct CJEU precedent on algorithmic fairness is limited, national DPA decisions provide guidance:

- Austrian DPA: Decision on automated employment screening found fairness violation where system disadvantaged certain demographic groups
- French CNIL: Guidance on algorithmic decision-making emphasizes fairness as encompassing non-discrimination
- UK ICO: Guidance on AI and data protection states discriminatory processing violates fairness

EDPB also emphasized (Guidelines 8/2020 on targeting of social media users) that fairness includes non-discriminatory processing.

COUNTERARGUMENTS:

Article 5(1)(a) fairness is distinct from anti-discrimination law:
- Some validity - GDPR is not primarily anti-discrimination legislation
- However, fairness principle clearly encompasses non-discrimination dimension
- Recital 71 mentions discrimination risks in automated decision-making
- Systematic interpretation supports fairness = non-discrimination

Processing lawful under Article 6 (legitimate interest):
- TechNova has legitimate interest in providing analytics services
- However, legitimate interest must be balanced against data subject rights (Article 6(1)(f))
- Discrimination clearly outweighs efficiency interest
- Fairness requirement is independent of lawfulness (conjunction "lawfully, fairly and transparently")

CONCLUSION ON ARTICLE 5(1)(a):

VIOLATION: LIKELY - Strong evidence of fairness violation

ENFORCEMENT LIKELIHOOD: 80-90%

RATIONALE:
- DPA guidance supports fairness = non-discrimination interpretation
- Statistical evidence of bias is compelling
- Fundamental rights dimension (Charter Article 21)
- DPAs likely to prioritize high-profile algorithmic discrimination case

POTENTIAL PENALTIES:

Article 83(5): Up to €20,000,000 or 4% of total worldwide annual turnover, whichever is higher.

TechNova turnover: €87 million
- 4% of turnover: €3.48 million
- Maximum: €20 million

LIKELY PENALTY RANGE (if violation found): €3-7 million

BEST ESTIMATE WITH COOPERATION: €4-6 million

B. Article 9 - Special Categories of Personal Data

LEGAL STANDARD:

Article 9(1) prohibits processing of special categories including:
- Biometric data for uniquely identifying a natural person
- Data revealing racial or ethnic origin

Article 9(2) provides limited exceptions requiring specific legal basis.

ANALYSIS:

1. BIOMETRIC DATA (Facial Recognition, Voice Analysis):

The System's optional facial recognition and voice analysis modules clearly process biometric data under Article 9(1).

LEGAL BASIS REQUIRED:

Article 9(2) potential bases:
(a) Explicit consent - problematic given employment power imbalance (Recital 43)
(b) Employment law necessity - requires genuine necessity, not mere convenience
(f) Legal claims - may apply for some purposes
(g) Substantial public interest - requires national law basis

ASSESSMENT:
- Consent likely invalid (power imbalance)
- Employment necessity questionable (optional features, not essential)
- Legal basis appears inadequate for biometric processing

CONCLUSION: Likely Article 9 violation for biometric processing

2. INFERENCE OF RACIAL/ETHNIC ORIGIN:

Whether inference of ethnicity from names constitutes Article 9 processing is legally unsettled.

Arguments that inference triggers Article 9:
- Purposeful inference to create special category data should trigger protections
- Otherwise controllers can circumvent Article 9 by inferring rather than directly collecting
- Recital 51 suggests inference may constitute processing

Arguments that inference does NOT trigger Article 9:
- Article 9(1) refers to data "revealing" not "inferring"
- Many inferences possible from non-special category data
- Overly broad interpretation would make Article 9 unworkable

EDPB has not definitively resolved this question. National DPA guidance varies.

ASSESSMENT:
- If algorithmic model explicitly uses ethnicity predictions as features: Article 9 likely applies
- If model merely uses features that correlate with ethnicity without explicit inference: Article 9 may not apply (though fairness concerns remain)
- Legal uncertainty favors conservative compliance approach

TechNova's RISK: Moderate - biometric processing clearly Article 9, inference question uncertain

CONCLUSION ON ARTICLE 9:

VIOLATION: LIKELY for biometric processing; UNCERTAIN for inference

ENFORCEMENT LIKELIHOOD: 50-65%

RATIONALE:
- Biometric processing violation clear (inadequate legal basis)
- However, biometric features are optional modules, not universal
- Inference question legally complex, DPAs may not pursue given uncertainty
- May depend on whether DPA wants to establish precedent on inference

POTENTIAL PENALTIES:

Article 83(5): Up to €20,000,000 or 4% of total worldwide annual turnover

LIKELY PENALTY RANGE (if violation found): €2-5 million

BEST ESTIMATE WITH COOPERATION: €2-4 million

C. Article 22 - Automated Decision-Making

LEGAL STANDARD:

Article 22(1): "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."

Article 22(2) provides exceptions where automated decision-making is:
(a) Necessary for contract
(c) Based on explicit consent
(in both cases, with safeguards per Article 22(3))

ANALYSIS:

Two key questions:
1. Is processing "solely automated"?
2. Does it produce "legal effects" or "similarly significantly affect"?

1. "SOLELY AUTOMATED" QUESTION:

TechNova position:
- Humans (HR professionals) make final decisions
- System provides recommendations, not decisions
- Not "solely automated"

DataSure position:
- High correlation (78%) suggests nominal human involvement
- Automation bias means humans rubber-stamp recommendations
- "Solely automated" in substance if not form

Article 29 WP Guidelines (WP251):
- Human involvement must be "meaningful" not "token"

- Requires "authority and competence to change the decision"
- Must involve "thorough assessment" not "routine application"

Evidence:
- Some overrides/adjustments exist (not zero human involvement)
- But limited explainability hampers thorough assessment
- High correlation suggests limited meaningful intervention

LEGAL ASSESSMENT:

This is fact-intensive and legally uncertain. Courts/DPAs must assess whether human involvement is meaningful or token.

TechNova has better defense here than some claims because:
- Humans do make final decisions (not zero involvement)
- System designed as decision support, not automation
- Client training emphasizes human responsibility

However:
- 78% correlation is quite high
- Limited explainability concerns
- Automation bias research supports DataSure's theory

Best characterization: Human involvement exists but may be insufficient per WP251 standards for truly meaningful oversight.

2. "SIMILARLY SIGNIFICANTLY AFFECTS" QUESTION:

Employment decisions clearly produce significant effects:
- Affect livelihood and economic security
- Career trajectory impacts
- Fundamental rights implications

This element clearly satisfied.

EXCEPTIONS UNDER ARTICLE 22(2):

Even if "solely automated," Article 22(2)(a) and (c) permit with safeguards.

TechNova might argue:
- Processing necessary for contract between Client and employee

- Or based on consent (though employment consent questionable)

If exception applies, Article 22(3) requires:
- Right to obtain human intervention
- Right to express point of view
- Right to contest decision

TechNova's system arguably provides these (humans involved, employees can challenge decisions) but safeguards may be insufficient.

CONCLUSION ON ARTICLE 22:

VIOLATION: POSSIBLE but UNCERTAIN

ENFORCEMENT LIKELIHOOD: 30-50%

RATIONALE:
- Legally and factually complex
- TechNova has stronger defenses than other claims
- Human involvement exists (not zero)
- DPAs may focus on clearer violations (Article 5(1)(a))
- However, if DPA wants to establish precedent on automation bias, may pursue

POTENTIAL PENALTIES:

Article 83(5): Up to €20,000,000 or 4% of total worldwide annual turnover

LIKELY PENALTY RANGE (if violation found): €1-3 million

BEST ESTIMATE: €1.5-2.5 million

D. Cumulative GDPR Assessment

OVERALL GDPR COMPLIANCE: NON-COMPLIANT

LIKELY VIOLATIONS:
- Article 5(1)(a) fairness: High likelihood (80-90%)
- Article 9 special categories: Medium likelihood (50-65%)
- Article 22 automated decisions: Low-medium likelihood (30-50%)

REALISTIC CUMULATIVE GDPR PENALTIES:
- Without cooperation: €6-12 million
- With cooperation: €4-8 million
- With settlement showing good faith: €2-6 million (or possibly forbearance)

BEST ESTIMATE WITH COOPERATION: €4-7 million

LEAD SUPERVISORY AUTHORITY:

Berliner Beauftragte für Datenschutz und Informationsfreiheit (Berlin DPA) likely lead supervisory authority given TechNova's Berlin headquarters.

Berlin DPA known for:
- Active enforcement
- Technology sector expertise
- Willingness to pursue novel issues

CROSS-BORDER ENFORCEMENT:

One-stop-shop mechanism (Article 56) means Berlin DPA would coordinate with other concerned authorities (France, Netherlands, Spain, Ireland DPAs).

However, if DataSure files complaints in multiple jurisdictions, coordination may be complex. Multiple DPAs may assert jurisdiction.

==
V. CIVIL LIABILITY ASSESSMENT
==

(Note: Civil liability analysis is more limited as this is outside our core expertise in regulatory law. Employment discrimination specialists should be consulted for detailed assessment.)

SUMMARY ASSESSMENT:

Affected individuals have viable discrimination claims under:
- EU equality directives (national implementations)
- Charter Article 21
- National employment discrimination laws

Evidence of indirect discrimination:
- Statistical disparate impact (prima facie case)
- Burden shifts to TechNova to prove objective justification
- TechNova's justifications (efficiency, historical data) likely insufficient

Potential plaintiffs: Thousands to tens of thousands
Potential damages per plaintiff: €500-20,000 depending on harm
Total potential exposure: €20-80 million

Collective action mechanisms:
- Representative Actions Directive (EU) 2020/1828
- National class action procedures
- Labor union actions

Likelihood of civil litigation if settlement fails: 60-80%

STRATEGIC CONSIDERATION:

Civil litigation highly fact-intensive, lengthy (3-5 years), expensive (€5-10M legal fees), and uncertain.

Settlement provides certainty and controlled resolution at lower cost.

==
VI. REGULATORY ENFORCEMENT LIKELIHOOD AND PROCESS
==

A. If DataSure Files Complaints

If settlement negotiations fail and DataSure proceeds with regulatory complaints:

MARKET SURVEILLANCE AUTHORITIES (AI Act):

DataSure indicated intent to file with authorities in:
- Germany (BSI or designated market surveillance authority)
- France (ANSSI or designated authority)
- Netherlands
- Spain
- Ireland

PROCESS:
1. Complaint received and assessed

2. Preliminary investigation (document requests, information gathering)
3. Formal investigation if prima facie case
4. Findings and determination
5. Penalty assessment and decision
6. Appeal rights

TIMELINE: 12-36 months from complaint to final decision

DATA PROTECTION AUTHORITIES (GDPR):

DataSure indicated intent to file with:
- Berlin DPA (Berliner Beauftragte) - lead supervisory authority
- CNIL (France), AP (Netherlands), AEPD (Spain), DPC (Ireland) - concerned authorities

PROCESS:
1. Complaint lodged
2. Lead supervisory authority determination (Article 56)
3. Investigation and fact-finding
4. Draft decision and cooperation procedure with concerned authorities
5. Final decision
6. Appeal rights (administrative and judicial review)

TIMELINE: 18-48 months from complaint to final enforceable decision

B. Proactive Engagement vs. Reactive Defense

OPTION A: WAIT FOR COMPLAINTS, THEN DEFEND

Approach:
- Do not proactively contact authorities
- Respond if/when complaints filed
- Mount defense arguing no violations or mitigated violations

Advantages:
- May avoid enforcement if complaints not filed or not pursued
- Preserves all defenses
- No voluntary admission

Disadvantages:
- Reactive posture perceived negatively
- No cooperation credit in penalty calculation
- Authorities may view as uncooperative

- Higher penalties if violations found

OPTION B: PROACTIVE ENGAGEMENT

Approach:
- Contact authorities proactively
- Explain identified issues and remediation efforts
- Request guidance and forbearance
- Demonstrate good faith

Advantages:
- Cooperation credit (30-50% penalty reduction typical)
- Opportunity to shape narrative
- May influence enforcement priority (authorities have limited resources)
- Demonstrates responsibility and good faith

Disadvantages:
- Voluntary disclosure of issues
- Cannot later claim no violations
- Requires genuine commitment to remediation

RECOMMENDATION: Option B (Proactive Engagement) IF settlement with DataSure achieved

Rationale:
- Settlement demonstrates good faith
- Proactive engagement compounds good faith credit
- Maximizes penalty mitigation
- Authorities likely to learn of issues anyway (DataSure complaints)
- Better to control narrative

RECOMMENDATION: Option A (Reactive Defense) IF settlement fails

Rationale:
- If settlement fails, disputes likely to be contentious
- Adversarial posture with DataSure likely extends to authorities
- Preserve all defenses for litigation

==
VII. STRATEGIC RECOMMENDATIONS
==

A. Settlement Strongly Recommended

RATIONALE:

1. LEGAL EXPOSURE IS SUBSTANTIAL:
- Regulatory penalties: €10-17M without cooperation, €6-12M with cooperation
- Civil damages: €20-80M
- Legal defense costs: €5-10M
- Total: €31-107M

2. SETTLEMENT COST IS MANAGEABLE:
- Proposed settlement: €10-13M
- Represents 11-15% of annual revenue
- Substantially less than litigation exposure
- Spreads costs over time (fund, monitoring, remediation)

3. SETTLEMENT PROVIDES CERTAINTY:
- Controlled resolution vs. years of uncertainty
- Avoid 3-7 year litigation timeline
- Business continuity maintained
- Management focus on operations vs. litigation

4. SETTLEMENT ENABLES REPUTATIONAL REHABILITATION:
- Demonstrates responsibility
- Positions TechNova as industry leader in responsible AI
- "Crisis → opportunity" narrative
- Contrast with companies that deny and defend

5. LITIGATION OUTCOMES HIGHLY UNCERTAIN:
- New legal questions (AI Act not yet enforced)
- Fact-intensive inquiries (effective oversight, automation bias)
- Multiple jurisdictions and proceedings
- Risk of adverse precedent

6. SETTLEMENT TERMS ARE REASONABLE:
- Compensation fund serves fairness (affected individuals)
- DataSure payment supports public interest mission
- Technical remediation necessary regardless (not "extra" cost)
- Independent monitoring provides credibility
- Transparency advances industry best practices

B. Negotiation Priorities

IF engaging in settlement negotiation, TechNova should prioritize:

1. MUST-HAVES:
- Business continuity (no suspension of System)
- Manageable total cost (≤€15M all-in)
- DataSure forbearance from complaints/litigation support
- No admission of liability (frame as good faith improvement)
- Trade secret protection (transparency with limits)

2. IMPORTANT:
- Independent monitor selection (jointly selected, mutually acceptable)
- Monitoring period (3 years acceptable, resist longer)
- Regulatory engagement coordination (joint approach)
- Settlement confidentiality (except public summary)

3. NEGOTIABLE:
- Compensation fund size (€6-8M range acceptable)
- DataSure payment (€2-3M range acceptable)
- Transparency extent (can be flexible with trade secret protections)
- Timeline for remediation (reasonable extensions okay)

WALK-AWAY POINTS:
- Total settlement cost >€15M (exceeds reasonable resolution)
- System suspension requirement (threatens business viability)
- Unrestricted access to trade secrets (threatens competitive position)
- Admission of intentional wrongdoing (legal liability implications)

C. If Settlement Fails

IF settlement negotiations are unsuccessful:

1. IMMEDIATE ACTIONS:
- Brace for regulatory complaints (within 30 days)
- Prepare comprehensive defense strategy
- Engage litigation counsel in multiple jurisdictions
- Implement maximum feasible bias mitigation (reduce attack surface)
- Client notification and support (minimize client defections)

2. REGULATORY DEFENSE STRATEGY:
- Emphasize good faith efforts and remediation
- Argue state of the art at time of development (2020-2021)
- Highlight technical complexity and fairness trade-offs
- Seek to minimize penalties through cooperation (even if defending)
- Consider selective concessions (admit some issues, defend others)

3. CIVIL LITIGATION STRATEGY:
- Defend on causation (multiple factors in employment decisions)
- Emphasize human decision-making authority

- Seek to limit damages (challenge damages calculations)
- Move to arbitrate client claims (if contractually required)
- Coordinate defense across multiple proceedings

4. PARALLEL REMEDIATION:
- Continue technical improvements regardless of litigation
- Implement compliance program
- Pursue conformity assessment
- Demonstrate ongoing good faith (helps with penalties and settlements)

5. ONGOING SETTLEMENT DISCUSSIONS:
- Even if litigation commences, continue settlement discussions
- Most cases settle after commencement but before trial
- Use discovery and preliminary rulings to inform settlement leverage
- Be prepared to settle on less favorable terms after litigation begins (legal fees and adverse rulings weaken position)

ESTIMATED COSTS IF LITIGATING:
- Year 1-2 costs: €5-10M (legal fees, preliminary proceedings)
- Settlement after 1-2 years: Likely €15-30M (higher than pre-litigation)
- Litigated to judgment: €35-110M total (penalties + damages + fees)

CONCLUSION: Settlement now substantially preferable to settlement later or litigation to judgment.

==
==
VIII. CONCLUSION
==
==

TechNova faces substantial legal risk arising from algorithmic bias in the InsightPredict Analytics Platform. The core allegations are legally well-founded:

VIOLATIONS LIKELY TO BE FOUND:
- AI Act Article 10 (data governance) - 75-85% likelihood
- AI Act Article 9 (risk management) - 65-75% likelihood
- GDPR Article 5(1)(a) (fairness) - 80-90% likelihood

ADDITIONAL POSSIBLE VIOLATIONS:
- AI Act Article 14 (human oversight) - 40-60% likelihood
- GDPR Article 9 (special categories) - 50-65% likelihood
- GDPR Article 22 (automated decisions) - 30-50% likelihood

FINANCIAL EXPOSURE:
- Regulatory penalties: €10-17M (without cooperation)
- Civil damages: €20-80M
- Legal costs: €5-10M
- Total: €35-107M

SETTLEMENT COST: €10-13M

RECOMMENDATION: SETTLE

Settlement provides:
- 70-90% cost reduction vs. litigation
- Certainty vs. uncertainty
- 3-6 year time savings
- Reputational rehabilitation opportunity
- Business continuity

The legal, financial, and strategic case for settlement is compelling. TechNova should conclude settlement negotiations successfully with DataSure and implement comprehensive remediation program.

This opinion represents our professional legal judgment based on current information and applicable law. We remain available to support settlement negotiations and any subsequent regulatory engagement or litigation if needed.

Respectfully submitted,

[Signed]

Dr. Friedrich Bauer
Partner, Bauer & Partners LLP
Specialist in AI Act and Technology Regulation

September 22, 2024

==
==

ATTORNEY-CLIENT PRIVILEGED AND CONFIDENTIAL
This opinion is provided solely to TechNova AI Systems Inc. for internal use in connection with legal decision-making. It may not be disclosed to third parties without Bauer & Partners LLP's express written consent, except as required by law or in connection with settlement negotiations (with appropriate

confidentiality protections).

This opinion represents legal advice and analysis based on facts as currently known. Actual outcomes in regulatory proceedings or litigation may differ based on additional facts, legal developments, or exercise of regulatory/judicial discretion.

==
==