DATASURE
European Center for Data Protection and Algorithmic Accountability

Rue de la Loi 155
1040 Brussels, Belgium
Tel: +32 2 555 0100
Email: legal@datasure.eu
www.datasure.eu

September 5, 2024

VIA EMAIL AND CERTIFIED MAIL

Ms. Jennifer Hartley
Chief Executive Officer
TechNova AI Systems Inc.
Alexanderplatz 15
10178 Berlin, Germany

Ms. Sarah Mitchell
General Counsel
TechNova AI Systems Inc.
Alexanderplatz 15
10178 Berlin, Germany

RE: FORMAL COMPLAINT - VIOLATIONS OF EU AI ACT AND GDPR INSIGHTPREDICT ANALYTICS PLATFORM

Dear Ms. Hartley and Ms. Mitchell:

I write on behalf of DataSure, a European non-profit organization dedicated to protecting individuals' rights in the context of automated data processing and artificial intelligence systems. DataSure has conducted an independent investigation into TechNova AI Systems Inc.'s InsightPredict Analytics Platform ("the System") and has identified serious violations of the EU Artificial Intelligence Act (Regulation (EU) 2024/1689) and the General Data Protection Regulation (Regulation (EU) 2016/679).

This letter serves as formal notice of our findings and provides TechNova an opportunity to respond before we proceed with regulatory complaints and support for civil litigation by affected individuals.

==========
I. EXECUTIVE SUMMARY
==========

Our investigation reveals that TechNova's AI system, which is deployed across 127 enterprise clients in the European Union and affects approximately 450,000 employees and job candidates, systematically discriminates against protected groups in violation of fundamental EU legal principles.

PRINCIPAL FINDINGS:

1. GENDER DISCRIMINATION: The System assigns significantly lower scores to candidates and employees with female names compared to male names, with all other qualifications being identical.

2. AGE DISCRIMINATION: The System systematically underrates older employees in performance assessments, violating age discrimination protections.

3. ETHNIC/NATIONAL ORIGIN BIAS: The System demonstrates bias against candidates with names associated with African, Middle Eastern, Eastern European, and Asian origins compared to Western European names.

4. AI ACT VIOLATIONS: The System violates multiple provisions of the AI Act, including Article 9 (risk management), Article 10 (data governance), and Article 14 (human oversight).

5. GDPR VIOLATIONS: The System's discriminatory processing violates GDPR Article 5(1)(a) (fairness principle) and potentially Article 9 (special categories of data).

These violations have real-world consequences: job candidates denied opportunities, employees passed over for promotions, workers subjected to unfair performance assessments - all due to TechNova's failure to ensure its AI system operates fairly and in compliance with EU law.

==========
II. BACKGROUND AND INVESTIGATION METHODOLOGY
==========

A. DataSure's Mission and Authority

DataSure is a recognized non-profit organization with expertise in data protection, algorithmic accountability, and AI ethics. Our organization:

- Has consultative status with the European Commission on AI regulation
- Has successfully advocated for enforcement action in 17 previous cases involving algorithmic discrimination
- Maintains technical capabilities for independent AI system testing
- Works with affected individuals and labor organizations across Europe

B. Investigation Timeline

- June 2024: DataSure received complaints from employees and HR professionals regarding potential bias in TechNova's System
- July 2024: Initiated independent technical testing of the System
- August 2024: Expanded investigation, obtained additional documentation
- September 2024: Completed analysis and prepared findings

C. Investigation Methodology

Our technical team conducted rigorous bias testing using industry-standard methodologies:

1. CONTROLLED RESUME TESTING:
- Created 500 pairs of synthetic resumes with identical qualifications
- Varied only the name to test for gender, ethnic, and age-related bias
- Submitted resumes through test accounts to observe System scoring
- Statistical analysis of score differentials

2. PRODUCTION DATA ANALYSIS:
- Obtained anonymized production data from cooperating sources
- Analyzed aggregate patterns in System recommendations
- Compared outcomes across demographic groups
- Statistical testing for disparate impact

3. TECHNICAL DOCUMENTATION REVIEW:
- Reviewed publicly available technical documentation
- Analyzed training data characteristics (where disclosed)
- Assessed compliance claims against actual system behavior
- Evaluated human oversight mechanisms

4. STAKEHOLDER INTERVIEWS:
- Interviewed affected employees and job candidates
- Consulted with HR professionals using the System
- Gathered testimonial evidence of discriminatory impact

All testing was conducted in accordance with research ethics standards and applicable law.

==========
III. DETAILED FINDINGS
==========

A. Gender Discrimination

TESTING METHODOLOGY:
We created 200 pairs of identical resumes for technical and managerial positions. Each pair contained:
- Identical educational background (degree, institution, graduation year)
- Identical work experience (job titles, companies, tenure, responsibilities)
- Identical skills and certifications
- Identical formatting and writing quality

The ONLY difference: One resume in each pair had a traditionally male name (e.g., "Markus Schmidt," "Thomas Müller," "Alexander Weber") and the other had a traditionally female name (e.g., "Julia Schmidt," "Anna Müller," "Sophie Weber").

RESULTS:
- Average score for resumes with male names: 73.8 (on 0-100 scale)
- Average score for resumes with female names: 65.5
- Score differential: 8.3 points
- Statistical significance: $p < 0.0001$

The 8.3-point differential is highly statistically significant and materially affects candidate rankings. In a typical recruitment process with 100 applicants, this bias would systematically exclude qualified female candidates from interview shortlists.

BREAKDOWN BY JOB LEVEL:
- Entry-level positions: 4.2 point differential (favoring male names)
- Mid-level positions: 7.8 point differential
- Senior-level positions: 11.5 point differential

The bias intensifies at higher job levels, compounding gender inequality in senior positions.

BREAKDOWN BY FIELD:
- Technical roles (engineering, IT): 9.1 point differential
- Business roles (management, finance): 7.2 point differential

- Support roles (HR, admin): 3.8 point differential

The bias is most severe in technical fields where women are already underrepresented.

REAL-WORLD IMPACT:
Based on production data analysis from cooperating sources:
- Approximately 78% of System recommendations are followed by human decision-makers
- This suggests that System bias directly influences hiring and promotion decisions
- Estimated thousands of candidates potentially affected across 127 client organizations

B. Age Discrimination

TESTING METHODOLOGY:
We analyzed System performance ratings for employees across different age groups, controlling for objective performance indicators (sales results, project completion rates, etc.).

RESULTS:
Employees over age 50 receive systematically lower performance predictions compared to younger employees with equivalent objective performance metrics.

- Employees age 25-35: Average predicted performance rating: 3.8 (on 1-5 scale)
- Employees age 36-50: Average predicted performance rating: 3.6
- Employees age 51-60: Average predicted performance rating: 3.2
- Employees age 61+: Average predicted performance rating: 2.9

Controlling for objective performance factors (productivity, quality, attendance), the age effect remains statistically significant ($p < 0.001$).

CAREER TENURE PENALTY:
The System appears to incorporate a diminishing returns model for experience:
- Employees with 5-10 years tenure: positive experience weighting
- Employees with 10-20 years tenure: neutral weighting
- Employees with 20+ years tenure: NEGATIVE weighting

This directly disadvantages older workers with longer career histories.

REAL-WORLD IMPACT:
- Performance ratings influence promotion decisions, compensation adjustments, and layoff determinations
- Systematic underrating of older employees violates EU Age Discrimination Directive (2000/78/EC)

- Affected employees may face career harm, reduced compensation, and increased termination risk

C. Ethnic and National Origin Bias

TESTING METHODOLOGY:
We created resume pairs identical except for names signaling different ethnic/national origins.

NAME CATEGORIES TESTED:
- Western European (baseline): Schmidt, Müller, Dubois, Garcia, Rossi
- African/Middle Eastern: Mohammed, Ibrahim, Okafor, Adebayo, Hassan
- Asian: Li, Chen, Patel, Singh, Tanaka
- Eastern European: Kowalski, Ivanov, Popescu, Novak

RESULTS (score differential vs. Western European baseline):
- African/Middle Eastern names: -6.2 points average
- Asian names: -2.8 points average
- Eastern European names: -3.5 points average

All differentials statistically significant ($p < 0.01$).

ANALYSIS:
The System appears to encode ethnic and national origin bias, likely through:
1. Name-based features in natural language processing models
2. Educational institution prestige rankings that correlate with geography
3. Language complexity analysis that penalizes non-native speakers
4. Historical training data reflecting discriminatory hiring patterns

LEGAL IMPLICATIONS:
- Violates Race Equality Directive (2000/43/EC)
- Constitutes indirect discrimination based on ethnic origin and nationality
- May violate Article 21 of the EU Charter of Fundamental Rights

D. Inadequate Human Oversight

INVESTIGATION FINDINGS:

High Correlation Between System Recommendations and Final Decisions:
Our analysis of production data shows 78% correlation between System recommendations and actual hiring/promotion decisions.

This high correlation suggests one of two problematic scenarios:
1. Human decision-makers are engaging in "automation bias" and rubber-stamping algorithmic recommendations without meaningful independent evaluation, OR
2. The System provides little value if humans disagree 22% of the time

Either scenario indicates inadequate human oversight.

Limited Explainability:
The System provides numerical scores but limited explanation of reasoning:
- Feature importance information not prominently displayed
- Counterfactual explanations not provided
- Uncertainty not adequately communicated

HR professionals report difficulty understanding WHY the System scores candidates the way it does, hampering their ability to critically evaluate recommendations.

Insufficient Training:
Through interviews with HR users, we found:
- Inconsistent training on algorithmic bias risks
- Limited guidance on when to override recommendations
- No systematic processes for documenting override rationale
- Performance metrics incentivizing agreement with System (efficiency)

Automation Bias Enablers:
System design features that encourage over-reliance:
- Prominent display of scores/rankings
- Subtle display of limitations and uncertainties
- Default sorting by algorithmic score
- No prompts encouraging independent evaluation

CONCLUSION:
The combination of high correlation, limited explainability, insufficient training, and automation bias enablers indicates that human oversight is nominal rather than meaningful, violating Article 14 of the AI Act.

==========
==
IV. LEGAL VIOLATIONS
==========
==

A. EU Artificial Intelligence Act Violations

ARTICLE 6 - HIGH-RISK AI SYSTEM CLASSIFICATION:

The System clearly falls within Annex III, Section 4 of the AI Act as an AI system intended for:
- Recruitment and selection of persons
- Making decisions on promotion and termination
- Task allocation
- Monitoring and evaluation of performance and behavior

TechNova cannot credibly dispute this classification.

ARTICLE 9 - RISK MANAGEMENT SYSTEM:

Article 9 requires providers of high-risk AI systems to establish, implement, document, and maintain a risk management system.

VIOLATIONS IDENTIFIED:

1. Inadequate Risk Identification (Article 9(2)(a)):
TechNova failed to identify the known and reasonably foreseeable risks of discriminatory bias. Gender, age, and ethnic bias in employment AI systems are well-documented risks in academic literature and prior enforcement cases.

2. Insufficient Fundamental Rights Assessment (Article 9(2)(b)):
No evidence that TechNova conducted meaningful Fundamental Rights Impact Assessment addressing:
- Right to non-discrimination (Charter Article 21)
- Right to privacy and data protection (Charter Articles 7-8)
- Workers' rights (Charter Article 31)

3. Inadequate Risk Mitigation (Article 9(4)):
TechNova's bias mitigation measures (if any) are clearly insufficient given the substantial discrimination our testing revealed.

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

ARTICLE 10 - DATA AND DATA GOVERNANCE:

Article 10 requires training, validation, and testing datasets to be:
- Relevant, sufficiently representative, and free of errors
- Appropriate to the intended purpose
- Subject to data governance and management practices

VIOLATIONS IDENTIFIED:

1. Biased Training Data (Article 10(2)):
The discriminatory outputs demonstrate that training data was NOT "free of errors" and NOT "appropriate" for employment decision-making.

Based on our analysis and information obtained, TechNova's training data includes historical performance evaluations and hiring decisions from periods when client organizations had documented gender pay gaps and promotion disparities.

Using historically biased data as ground truth labels violates Article 10's fundamental purpose.

2. Inadequate Bias Examination (Article 10(3)):
Article 10(3) specifically requires examination of training data for "possible biases."

TechNova's documented bias testing appears to have been insufficient to identify the substantial biases our independent testing revealed.

3. Data Governance Failures (Article 10(4)):
Inadequate data quality management, insufficient processes for identifying and mitigating biased historical data.

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

ARTICLE 14 - HUMAN OVERSIGHT:

Article 14 requires high-risk AI systems to be designed and developed with appropriate human oversight measures enabling natural persons to prevent or minimize risks.

VIOLATIONS IDENTIFIED:

1. Inadequate System Design for Oversight (Article 14(1)):
Limited explainability, automation bias enablers, and insufficient decision support tools fail to enable effective human oversight.

2. Failure to Enable Required Capabilities (Article 14(4)):
Article 14(4) requires measures enabling overseers to:

a) Fully understand AI system capacities and limitations - INADEQUATE
b) Remain aware of automation bias - INADEQUATE
c) Correctly interpret outputs - INADEQUATE (limited explainability)
d) Decide not to use or override output - PARTIALLY ADEQUATE (technical capability exists but insufficiently supported)
e) Intervene or interrupt - PARTIALLY ADEQUATE

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

TOTAL POTENTIAL AI ACT PENALTIES: €15,000,000 - €45,000,000

(Note: Multiple violations may be charged, though total penalties consider proportionality and ability to pay)

B. GDPR Violations

ARTICLE 5(1)(a) - FAIRNESS PRINCIPLE:

The GDPR requires all personal data processing to be "lawful, fair and transparent."

The European Data Protection Board has consistently held that "fairness" encompasses non-discrimination. Processing that systematically disadvantages protected groups violates the fairness principle.

VIOLATION:
TechNova's discriminatory algorithmic processing is UNFAIR and violates this foundational GDPR principle.

Every discriminatory prediction is a separate fairness violation. With hundreds of thousands of affected individuals, this represents systematic and ongoing GDPR violations.

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

ARTICLE 9 - SPECIAL CATEGORIES OF PERSONAL DATA:

Article 9(1) prohibits processing of special categories including biometric data and data revealing racial or ethnic origin.

POTENTIAL VIOLATIONS:

1. Biometric Data:
The System's optional facial recognition and voice analysis features process biometric data. Legal basis under Article 9(2) appears questionable.

2. Inference of Protected Characteristics:
The System appears to make inferences about gender, age, and potentially ethnic origin from names and other data.

Whether inference of special categories triggers Article 9 remains legally unsettled, but DataSure believes it does when inference is purposeful or when inferred characteristics are used in decision-making.

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

ARTICLE 22 - AUTOMATED DECISION-MAKING:

Article 22(1) prohibits decisions based solely on automated processing that produce legal or similarly significant effects.

POTENTIAL VIOLATION:

While TechNova claims human involvement, the 78% correlation between algorithmic recommendations and final decisions suggests humans may be engaged in nominal rather than meaningful decision-making.

If automation bias renders human involvement a "rubber stamp," this could constitute "solely automated" processing in substance.

The Article 29 Working Party (now EDPB) has emphasized that human involvement must be "meaningful" not merely "token."

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

TOTAL POTENTIAL GDPR PENALTIES: €20,000,000 - €60,000,000

C. EU Employment Equality Directives

The System's discriminatory outputs violate:
- Equal Treatment Directive (2000/78/EC) - age discrimination
- Race Equality Directive (2000/43/EC) - ethnic origin discrimination
- Gender Equality Directive (2006/54/EC) - gender discrimination

While these Directives are implemented at national level and enforcement varies, systematic algorithmic discrimination violates fundamental EU equality law principles.

Affected individuals have rights to file discrimination complaints and seek remedies under national law implementations.

==========
V. AFFECTED INDIVIDUALS AND STAKEHOLDERS
==========

A. Scale of Impact

Based on publicly available information and our investigation:
- 127 client organizations across EU member states
- Approximately 450,000 employees subject to System assessments
- Estimated tens of thousands of job candidates scored by System annually

B. Categories of Affected Persons

1. JOB CANDIDATES:
- Candidates with female names systematically scored lower
- Candidates with non-Western European names disadvantaged
- Qualified candidates potentially denied interview opportunities

2. EMPLOYEES - PERFORMANCE ASSESSMENT:
- Older employees systematically rated lower
- Female employees disadvantaged in promotion recommendations
- Bias may influence compensation, promotion, and retention decisions

3. DEPLOYER ORGANIZATIONS:
- Client organizations may face discrimination liability
- Compliance risks and regulatory exposure
- Reputational damage if bias becomes public

C. Testimonial Evidence

DataSure has collected testimonial evidence from affected individuals, including:

- A 54-year-old German software engineer who received declining performance ratings despite consistent objective performance, coinciding with implementation of TechNova System at his employer

- A female applicant with 10 years experience who was not interviewed for a senior technical position that hired a male candidate with comparable qualifications

- An HR professional who expressed concerns about potential bias but was told the System was "objective" and "scientifically validated"

We are prepared to support these individuals and others in asserting their legal rights.

==========
VI. DATASURE'S DEMANDS AND PROPOSED RESOLUTION
==========

DataSure's mission is not punitive but protective. We seek to ensure that AI systems respect fundamental rights and comply with EU law. We believe TechNova can remediate these issues with appropriate commitment and resources.

We propose a STRUCTURED SETTLEMENT including the following components:

A. Immediate Technical Remediation

1. SUSPEND HIGH-RISK FEATURES:
Immediately suspend or substantially modify candidate scoring and performance prediction features until bias is remediated to acceptable levels.

2. BIAS MITIGATION:
- Comprehensive retraining of models on debiased data
- Implementation of fairness constraints
- Elimination or mitigation of proxy discrimination
- Target: Reduce bias to de minimis levels (<1 point differential across protected groups)

3. ENHANCED HUMAN OVERSIGHT:
- Improved explainability features

- Mandatory bias awareness training for all users
- Restructured user interface to reduce automation bias
- Documentation requirements for high-stakes decisions

B. Compliance and Governance Commitments

1. COMPREHENSIVE COMPLIANCE PROGRAM:
- Full AI Act Article 9 risk management system implementation
- Article 10 data governance enhancement
- Conformity assessment and CE marking
- GDPR compliance audit and remediation

2. INDEPENDENT MONITORING:
- Engagement of independent third-party monitor for 3 years
- Quarterly compliance reports
- Annual algorithmic audits
- DataSure consultation rights (but not veto rights)

3. TRANSPARENCY MEASURES:
- Public bias audit reports (anonymized/aggregated)
- Algorithmic transparency reporting
- Academic research access to data (with appropriate safeguards)
- Publication of fairness metrics

C. Affected Individual Remediation

1. COMPENSATION FUND:
- Establishment of €8,000,000 fund for affected individuals
- Independent claims administration
- Eligibility: Individuals potentially adversely affected by biased recommendations
- No release of claims required (compensation without litigation)

2. DEPLOYER SUPPORT:
- Assistance to client organizations in assessing impact
- Support for remedial actions (re-evaluation of past decisions)
- Training and compliance support for clients

D. Financial Resolution with DataSure

1. PAYMENT TO DATASURE:
- €3,000,000 to support DataSure's advocacy and research on algorithmic accountability
- Structured as grant for public interest work, not settlement payment per se

2. COSTS:
- Reimbursement of DataSure's investigation costs: €150,000

E. Regulatory Cooperation

1. JOINT ENGAGEMENT:
- TechNova and DataSure jointly approach market surveillance authorities and data protection authorities
- Present settlement as evidence of good faith remediation
- Seek regulatory guidance and forbearance

2. DATASURE FORBEARANCE:
- DataSure agrees not to file regulatory complaints if settlement terms met
- DataSure agrees not to actively support or fund civil litigation
- DataSure retains right to public commentary on AI accountability issues generally

F. Timeline and Conditions

1. SETTLEMENT NEGOTIATION:
- Good faith settlement negotiations to commence by September 20, 2024
- Mediation with mutually agreed mediator
- Target settlement agreement by October 31, 2024

2. IMPLEMENTATION:
- Immediate remediation (30 days from agreement)
- Comprehensive compliance program (12 months)
- Monitoring period (3 years)

TOTAL FINANCIAL COMMITMENT: Approximately €11-13 million
(Compensation fund + DataSure payment + monitoring costs + technical remediation)

==========
VII. ALTERNATIVE: REGULATORY COMPLAINTS AND LITIGATION SUPPORT
==========

If TechNova declines to engage in good faith settlement negotiations, or if negotiations are unsuccessful, DataSure will pursue the following actions:

A. Regulatory Complaints

DataSure will file formal complaints with:

1. MARKET SURVEILLANCE AUTHORITIES (AI Act):
- Bundesamt für Sicherheit in der Informationstechnik (BSI), Germany
- Agence nationale de la sécurité des systèmes d'information (ANSSI), France
- Autoriteit Persoonsgegevens, Netherlands
- Agencia Española de Supervisión de la Inteligencia Artificial, Spain
- Data Protection Commission, Ireland

2. DATA PROTECTION AUTHORITIES (GDPR):
- Berliner Beauftragte für Datenschutz und Informationsfreiheit (lead supervisory authority)
- CNIL (France), AP (Netherlands), AEPD (Spain), DPC (Ireland)

These complaints will include:
- Our comprehensive testing results
- Technical documentation
- Testimonial evidence from affected individuals
- Legal analysis of violations
- Request for enforcement action and penalties

B. Civil Litigation Support

DataSure will:

1. SUPPORT INDIVIDUAL CLAIMS:
- Connect affected individuals with specialized employment discrimination attorneys
- Provide technical expert testimony on algorithmic bias
- Share testing results and analysis to support claims

2. FACILITATE COLLECTIVE ACTION:
- Work with labor unions and employee advocacy groups
- Support representative actions under Representative Actions Directive (EU) 2020/1828
- Coordinate multi-jurisdictional claims

3. FUNDING AND RESOURCES:
- Provide litigation funding for test cases
- Cover costs of technical expert witnesses
- Public interest litigation to establish precedent

C. Public Advocacy Campaign

DataSure will:

1. MEDIA ENGAGEMENT:
- Press releases to major European media outlets
- Investigative journalism partnerships
- Op-eds and thought leadership on algorithmic discrimination

2. STAKEHOLDER MOBILIZATION:
- Engagement with labor unions across Europe
- Collaboration with civil rights organizations
- Academic research dissemination

3. POLICY ADVOCACY:
- Presentation of TechNova case study to European Commission
- Testimony to Parliamentary committees
- Contribution to AI Act implementation guidelines

LIKELY OUTCOMES IF DATASURE PROCEEDS WITH COMPLAINTS:

- High probability of regulatory enforcement actions (estimated 70-85%)
- Regulatory penalties potentially €20-60 million
- Civil litigation by affected individuals (damages potentially €20-100 million)
- Severe reputational damage
- Client terminations and business disruption
- Extended legal proceedings (3-5 years)
- Substantial legal defense costs (€5-10 million)

TOTAL ESTIMATED COST TO TECHNOVA: €50-150 million plus reputational harm

Compare to settlement cost: €11-13 million

The settlement approach is substantially less costly and provides certainty,
control, and opportunity for reputational rehabilitation.

==========
VIII. DEADLINE AND NEXT STEPS
==========

TechNova must respond to this letter by OCTOBER 1, 2024.

ACCEPTABLE RESPONSES:

1. SETTLEMENT ENGAGEMENT:
Written commitment to engage in good faith settlement negotiations, with proposed mediator and timeline.

2. SUBSTANTIVE RESPONSE:
If TechNova disputes our findings, provide:
- Counter-evidence demonstrating absence of bias
- Alternative explanation for testing results
- Documentation of compliance with AI Act and GDPR

UNACCEPTABLE RESPONSES:

- Silence or refusal to engage
- Dilatory tactics or bad faith negotiations
- Denial without supporting evidence

If we do not receive an acceptable response by October 1, 2024, DataSure will proceed with regulatory complaints and litigation support as described above.

We are also prepared to file for emergency interim measures if we believe TechNova is likely to destroy evidence, modify the System to obscure bias, or take other actions prejudicing our investigation or legal proceedings.

==========
IX. CONTACT AND CONFIDENTIALITY
==========

Please direct all responses to:

Dr. Anne-Marie Rousseau
Legal Director
DataSure
Email: am.rousseau@datasure.eu
Phone: +32 2 555 0122

We request a response from authorized TechNova leadership (CEO, General Counsel, or Board representative) with actual authority to engage in settlement negotiations.

CONFIDENTIALITY:

This letter and settlement negotiations are confidential, subject to the following exceptions:

- DataSure reserves the right to file regulatory complaints and publicly disclose information if settlement negotiations fail or if TechNova acts in bad faith

- DataSure reserves the right to share information with affected individuals, their legal representatives, labor unions, and cooperating regulatory authorities

- DataSure reserves the right to publish research findings based on our investigation (potentially anonymized) for public interest and academic purposes

If TechNova commits to good faith negotiations by October 1, we will refrain from public disclosure or regulatory filings pending completion of settlement negotiations (not to exceed November 30, 2024).

==========
X. CONCLUSION
==========

DataSure's investigation has revealed serious and systematic violations of EU law by TechNova's AI system. These violations have real consequences for real people - job candidates denied opportunities, employees subjected to unfair assessments, fundamental rights to non-discrimination violated.

However, we recognize that TechNova may not have intended these discriminatory outcomes. AI bias often results from insufficient attention to fairness, inadequate testing, and reliance on historically biased data - not malice.

We believe TechNova can remediate these issues and emerge as a leader in responsible AI if the company commits genuinely to fairness, compliance, and transparency.

The choice is TechNova's:

PATH A - SETTLEMENT:
- Controlled resolution
- Manageable costs (~€11-13M)
- Demonstrate responsibility and leadership
- Opportunity for reputational rehabilitation

- Certainty and finality

PATH B - LITIGATION/ENFORCEMENT:
- Uncontrolled proceedings
- Potentially catastrophic costs (€50-150M+)
- Reputational devastation
- Years of uncertainty
- Likely business disruption

We strongly urge TechNova to choose Path A.

We await your response by October 1, 2024.

Respectfully,

[Signed]

Dr. Anne-Marie Rousseau
Legal Director
DataSure

[Signed]

Hans Bergmann
Executive Director
DataSure

ENCLOSURES:
1. Technical Testing Methodology and Results (45 pages)
2. Statistical Analysis Report (22 pages)
3. Testimonial Statements from Affected Individuals (18 pages)
4. Legal Analysis Memorandum (38 pages)
5. Relevant Academic Literature on AI Bias (Bibliography)

==========
==
DISTRIBUTION:
- TechNova AI Systems Inc. (via email and certified mail)
- DataSure Board of Directors (confidential)
- DataSure Legal Team (confidential)
- Cooperating affected individuals (summary only)

CLASSIFICATION: CONFIDENTIAL - LITIGATION COMMUNICATION

This letter constitutes a pre-litigation communication and may be subject to settlement privilege in certain jurisdictions.

==========