NO AI WITHOUT US!

A DOCKWORKER BARGAINING TOOLKIT ON AI

José Luis Gallegos
Jannes Ten Berge

NO AI WITHOUT US! A DOCKWORKER BARGAINING TOOLKIT ON AI

José Luis Gallegos
Jannes Ten Berge

Rotterdam, May 2025.

Why This Document Matters —and How to Read It

Dockworkers' unions at the Port of Rotterdam are no strangers to negotiating technological change. But AI isn't just another workplace tool—it introduces new forms of control, decision-making, and value extraction, often with less transparency and a faster impact than previous waves of automation.

This document is a tool for action. It's designed to help unions think ahead, ask sharper questions, and build strategies for before, during, and after AI systems are introduced. Some proposals here are immediately actionable. Others are more ambitious or deliberately bold—meant to stretch the boundaries of negotiation, clarify priorities, and draw clear "red lines" around uses of AI that should be off the table.

AI is already making its way onto the terminal floor. The sooner unions claim their seat at the table, the better their chances of shaping how it's used, so that technological change strengthens, rather than undermines, workers' collective power.

Step 1.

AI Scope: Set the Purpose, Draw the Lines

Dockworkers know what it means when new technologies arrive on the terminal floor: change often comes fast, and not always in workers' favor. AI is no different, unless unions take the lead from the very beginning.

That's why dockworkers' unions must ensure that formal consultation rights are clearly established—ideally written into the collective bargaining agreement (CBA). Even if consultation has been common practice in the past, it is always safer when there's a binding commitment: "The Employer shall consult the Union in writing [...] before the intended introduction of any AI-based or automated technology."

(See CBA Template - 3. Mandatory Consultation)

Consultation rights must be clearly defined, so employers are required to provide detailed information on:

- What kind of AI (or other technologies) do they plan to introduce?
- How will these technologies affect current workflows and port operations?
- What does this mean for dockers' jobs—task changes, workload, safety risks?
- And what training or new skills will be needed?

AI might sound technical, but its consequences are very real: fewer hands on deck, faster-paced shifts, and more surveillance on the job. That's why consultation can't be left to chance—it must be secured in writing. No AI without consultation.

Use Independent Experts to Back You Up

Unions shouldn't be expected to take the company's word for it when they say "AI will help everyone." Ensure that, along with your "consultation clause," you can bring in your own experts and that there is a budget for it. Data scientists, legal advisors, or AI ethics specialists can help cut through the technical talk and explain what's really at stake.

You can also reference legal foundations like Article 25(1)(n) of the Dutch Works Councils Act, which allows for external expert advice when new technologies are introduced. Even if the union doesn't have representatives in the works council, this shows there's a precedent for demanding independent insight.

Works Council Faculties

The Dutch Works Councils Act provides legal foundations for claiming the right to consultation:

Article 25(1)(c): Grants the Works Council the right to be consulted when an employer plans to terminate all or part of business operations—relevant when AI leads to job elimination.

Article 25(1)(d): Requires consultation on major changes in company activities—applicable when AI triggers workforce reorganizations or restructurings.

Article 25(1)(e): Mandates consultation for significant organizational structure or technology changes, directly relevant when introducing AI or automation systems.

Article 27(1)(l): Grants the power to approve or reject employer proposals regarding employee monitoring and performance-tracking systems.

Set the Purpose of AI Clearly

Once consultation is on the table, the first question dockworkers' unions should raise is: What is the goal of this AI? Is it truly about making port operations safer or more efficient? Or is it really about cutting labor costs and reducing headcount?

Technologies like AI are flexible—they can serve many different purposes, depending on who's in control. That's why unions need to push for clarity upfront:

1. What kind of AI tools are being considered?
2. What specific goals is the employer trying to achieve?

Without clear answers, any talk of consent, implementation, and work readjustments should be regarded as premature. The 'why' of AI must come before the 'how.'

(See CBA Template - 3. Mandatory Consultation)

Draw the Line: What AI Uses Are Not Acceptable

Once the goals are clear, unions need to be ready to draw boundaries. Some uses of AI might be acceptable —if they truly improve safety and efficiency or reduce physical strain. But others should be off the table completely or allowed only after serious bargaining and with proper compensation.

Here are some AI uses dockworkers' unions should flag early:

AI Use Case	Common Applications	Red Line	Rationale
Job-Displacing Automation	Replacing core roles like crane driving or vessel planning with AI systems.	No automation of core tasks without prior union consultation and agreement	Undermines employment security and violates 'just transition' principles
Biometric Surveillance	AI tracking of heart rate, eye movement, facial expressions, or stress levels to monitor productivity	Absolutely no biometric or emotion-tracking systems in the workplace	Violates dignity and creates psychological harm and trust erosion. Also likely an 'unacceptable risk' under EU AI Act.
AI-Enforced Work Intensification	AI optimizing workflows to eliminate pauses, speed up task pacing, or micro-manage actions	No AI-driven work acceleration that removes natural breaks or pressures workers to move faster	Increases injury risk, harms well-being, reduces autonomy
Opaque Algorithmic Decision-Making	Use of AI in hiring, shift scheduling, or promotion without explainability or human recourse	No deployment without transparency, audit trails, and right to human review and appeal	Classified as high-risk under EU AI Act; risks bias, discrimination, and undermines procedural fairness
Wearable-Based Monitoring	Use of smart watches, helmets, vests, or tags to track worker location, movement, or physiological data	No wearables for individual-level monitoring or performance evaluation	Enables covert surveillance, increases stress, and risks misuse of sensitive data without transparency or consent

(See CBA Template - 5. AI Risk Classification)

The earlier these red lines are made clear, the better positioned unions are to defend dockworkers' rights and shape how AI is used on the terminal floor.

Job Transition Principles

Just Transition is a framework developed by the **International Labour Organization (ILO)** to ensure that workers are treated fairly during periods of major economic and technological change, such as the introduction of AI and automation.

It is based on four core principles:

Social dialogue and participation. Workers and unions must have a seat at the table when decisions about new technologies are made.

Job protection and security. Transitions should not lead to sudden job losses. Employers must negotiate changes, provide advance notice, and explore alternatives like retraining or internal redeployment.

Decent work and fair conditions. AI systems must not erode workers' rights, increase surveillance, or speed up work at the cost of health and safety.

Access to support and skills development. Workers should be offered training, upskilling, or reskilling to adapt to changing job roles or transition to new positions.

Additional resources:

European AI Act provides a list of forbidden, high-risk, and non-risk AI uses

Step 2.

Data Management: Demand Transparency and Control

To build AI, you need data. A lot of it. And in many cases, that data comes directly from workers. For instance, if a company wants to develop AI to operate a crane, it needs to be trained on large amounts of data from real crane operations—data mostly produced by dockworkers on the job.

Because this data is so valuable, unions must take a clear stance on what types of data collection are acceptable, how that data should be managed, and where the boundaries lie.

We propose bargaining around two key points:

Data Management Clauses

Unions should push employers to be fully transparent about data collection practices. Unions should ask questions like:

- What types of worker data are being collected? (e.g., biometric, behavioral, location-based, or performance-related)
- Why is this data being collected? (e.g., safety, efficiency, training AI systems)
- How intrusive are the collection methods? (e.g., surveillance cameras, wearables, biometric tracking)
- Who has access to the data, and under what conditions?
- Does the collection process comply with laws and ethical standards? (e.g., European General Data Protection Regulation (GDPR), European AI Act)

(See CBA Template - 6. Transparency and Oversight of AI Systems)

Data collection should be limited to what's strictly necessary for the goals that have been explicitly agreed on.

For example: In Sweden, the union successfully negotiated an agreement with a mining company that limited the use of worker-generated data strictly to safety improvements—explicitly banning its use for performance evaluations or disciplinary measures.

Lock In the Purpose of Data Use

One common issue is 'function creep'—when data that was collected for one purpose ends up being used for something entirely different. For example, a logistics company could install AI tracking to optimize delivery routes, but later use it to discipline workers for minor delays, without informing or consulting them.

To prevent this:

- Employers must notify union reps about any changes in data collection practices.
- This includes what new data will be collected, how it will be used, and who will have access. Incliuding a notification period before any changes take effect.
- Information should be provided in plain language—no technical jargon or legal confusion.

Unions should also negotiate the right to independent audits—to ensure the company is following the rules, respecting the agreements, and staying compliant with European data laws like the General Data Protection Regulation (GDPR).

(See CBA Template - 6.1 Disclosure and Explainability Requirements)

Step 3.

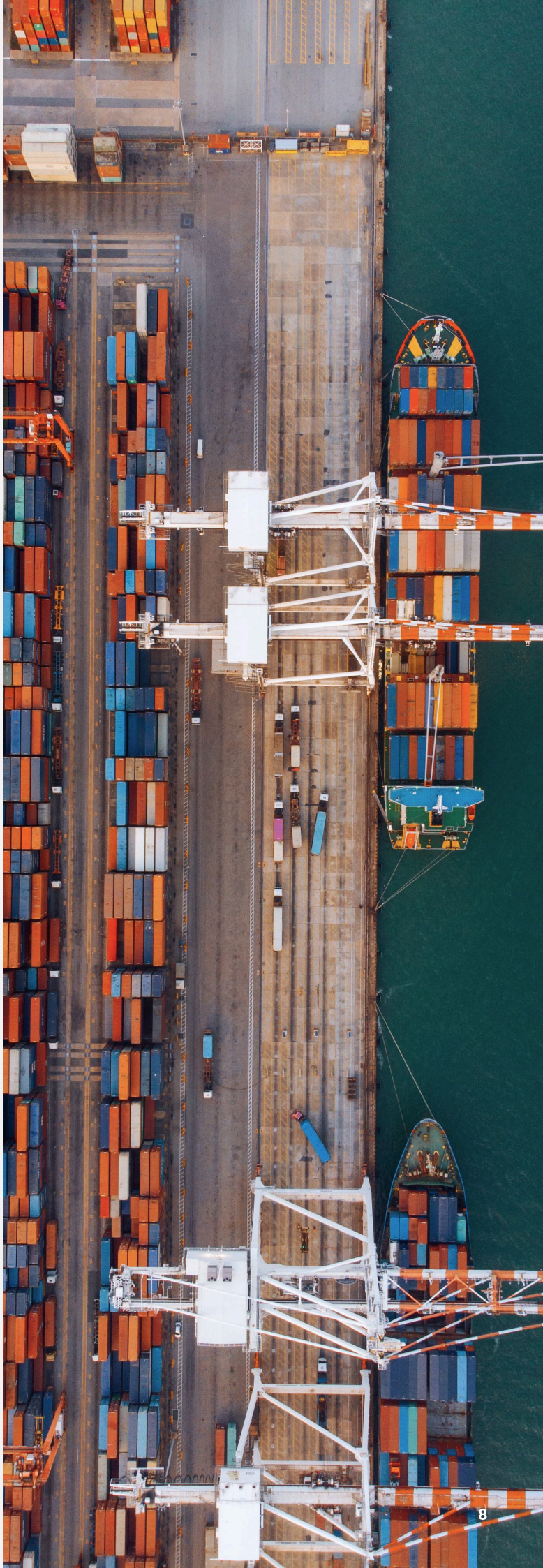
Compensation Models: Ensure that the benefits of AI are fairly distributed

When dockworkers operate machines, like cranes, their movements, decisions, and timing are often recorded as data. These data points can then be used to train AI systems to replicate or simplify the same tasks. But here's the problem: these data reflect your skills, experience, and judgment—what's often called tacit knowledge. And every time you override a machine's decision or give feedback to a smart system, you're helping improve that system by providing your expertise. It's like having an invisible apprentice watching your every move and learning your tricks—except you're not getting paid for training them.

Let's be clear: you're paid to move containers, not to build the very machine that might one day take over your job. If the company is using your tacit knowledge to build valuable systems, then you deserve compensation for that. The union should make it clear that these unconsented forms of data extraction are exploitative.

Start Bargaining Over Worker Data

It's time for unions to treat data generated by workers as a form of labor in its own right. If your knowledge is being captured and turned into training data for AI, then it becomes part of your job—and it's something that should be bargained over. Think about it: if you were asked to train a new worker, you'd expect to be paid. Now imagine that instead of a person, a machine is learning from your every move, quietly, through sensors and software, and that the data it collects becomes company property. Would you just give that away? Of course not



How Unions Can Bargain for Compensation

There are innovative proposals that dockworkers' unions can put on the table to ensure fair compensation when workers' skills and experience are turned into data.

Ownership model

One approach is to treat the data itself as something workers own. Under this model, employers would need formal permission to use that data through clear agreements that guarantee fairness, transparency, and forms of revenue sharing. This could include data stewardship agreements or royalty systems, where workers receive ongoing payments whenever their data is reused or monetized in AI systems.

Transition funds

Unions can also push for union-controlled AI transition funds. These funds would capture a share of the value created by AI (or other forms of technologies) and redirect it back to the workforce through training and upskilling programs, pension boosts, or direct payments to workers. This approach recognizes that dockers' labor doesn't just move goods—it's also helping to build the digital systems that shape the future of work.

Premium work

Another approach is to push for the recognition that contributing to AI development, by generating training data through your daily work, is an added responsibility. If dockers are helping to build these systems, that effort deserves compensation. Unions can push for updated job descriptions that reflect AI-related tasks and negotiate for wage premiums, bonuses, or even reduced working hours to account for the value added of their data. Whether it's a one-time payment or a bonus linked to productivity gains, the principle remains the same: if your data improves the system, it should be acknowledged and fairly rewarded.

Whatever model you choose, the message is the same: if your work helps build the technology, you deserve a fair share of the added value your labor creates.

Step 4.

AI Design: Influence the Goals and Guard Against Bias

Remember how we said AI can serve different purposes? Well, it's not just about optimizing machinery or speeding up container flows. AI can also step into management roles—deciding how dockers are scheduled, supervised, or even evaluated. That's why **dockworkers' unions need to be involved in how AI models are being trained.**

What does "training the model" mean?

Training an AI model means teaching a system how to make decisions by feeding it large amounts of data, usually from real-world operations. Think of it as showing the system thousands of examples so it can spot patterns and "learn" how to make similar decisions in the future.

Take recruitment as an example. If a company trains an AI tool using data from past hiring decisions, like resumes, interview notes, and who got hired, the system starts to recognize what kinds of candidates were typically selected. Over time, it begins recommending similar profiles. But here's the problem: an AI system only learns from what it's shown. If the training data is biased, the AI will be biased too. One famous case involved Amazon's attempt to build a recruitment AI. The system ended up discriminating against women because it was trained on ten years of hiring data that favored male candidates. The AI simply copied those patterns, even downgrading resumes that mentioned the word "women's."

Why does this matter at the port

If an AI system is trained on data from a narrow group—say, experienced day-shift workers—it could set unfair benchmarks for others, like new hires or night-shift crews. This can lead to unfair evaluations, penalize workers who operate under different conditions, or even encourage unsafe practices as workers push to meet poorly designed targets. That's why unions must engage in the technical decisions behind AI training. This includes questions like:

- What data is used to train the system?
- What does the AI define as "success"?
- Whose performance is it modeling?

(See CBA Template – 3.2 Required Impact Assessment)

These choices will directly shape how the system behaves on the terminal floor. If unions aren't involved in this stage, the risks may not be clear until it's too late, when schedules are being set in an opaque way, evaluations are discriminating against workers, and safety is on the line.

If the process becomes too technical, don't hesitate to bring in outside expertise. You wouldn't be expected to fix a crane's hydraulics on your own—AI systems are no different. Unions should have access to independent data scientists or technical advisors who can help unpack what's happening behind the scenes.

(See CBA Template - 3.3 Union Review and External Expertise)

What Should the AI Optimize For?

Every AI system is designed to "optimize" something—to do a task better, faster, or more efficiently. But what it's optimizing for isn't a neutral decision—it's a political one. A company might want AI to speed up cargo handling. Dockworkers, on the other hand, might want it to prioritize safety and reduce accidents. Those goals aren't always compatible. So ask clearly:

- What exactly is the model being trained to achieve?
- What degree of autonomy does the model have?
- Are any of those goals in conflict, like speed vs. safety, or efficiency vs. well-being?
- If so, how is AI decision-making expected to react?

If trade-offs exist, unions need a say in how they're managed. That could mean prioritizing safety in the model's training, or setting limits on how much efficiency can come at the cost of job quality.

(See CBA Template – 6.1 Disclosure and Explainability Requirements)

Transparency and Accountability

AI is often described as a "black box." It makes decisions, but no one can fully explain how. That's a major problem for unions. Why? Because if you don't understand the system, you can't challenge it. If an AI system assigns shifts, monitors performance, or flags workers for "low productivity," management can easily say: "It's the algorithm's call." That's simply not acceptable.

Unions should demand transparency from day one. That includes:

- A clear explanation of how the system makes decisions.
- A requirement to use explainable AI methods (like LIME or SHAP), which help make the model's choices traceable and understandable.
- A commitment that workers and unions can contest AI-driven decisions—and that accountability stays with management, not the machine.

(See CBA Template – 6.2 Worker Rights to Audit, Challenge, and Explanation)

AI Bias – Fix It Before It Hurts Workers

AI systems learn from data. As we stated, if that data is biased, unbalanced, or incomplete, the system will be too, and that can have real consequences on the job. For example, if the AI was trained mostly on crane operations in clear weather, it might fail during storms. Or if most of the data comes from one type of crew, the system might treat others unfairly.

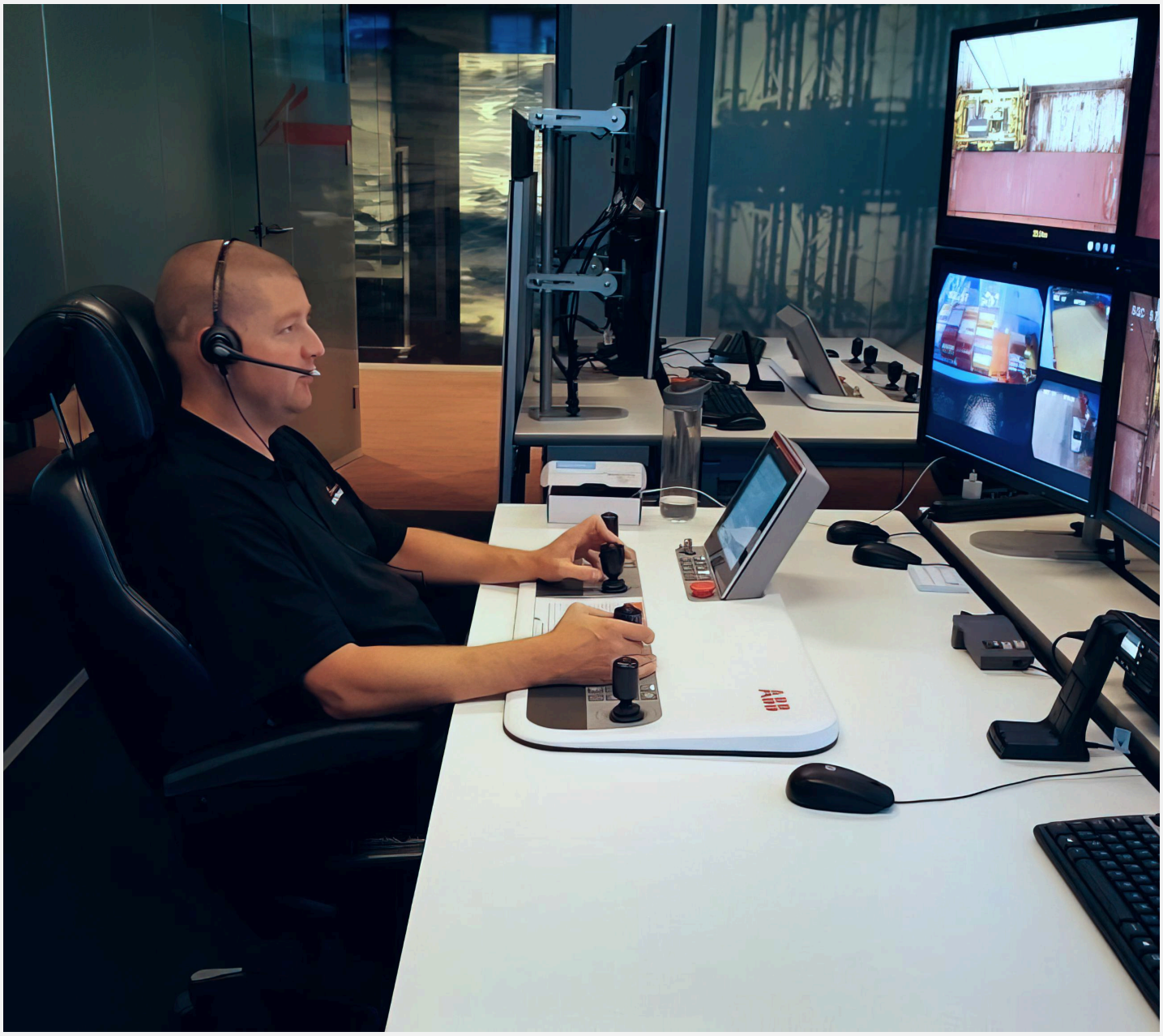
Unions should demand proof that the system is fair before it goes live. That means:

- Showing that different worker profiles, job types, and working conditions were used in training.
- Demonstrating that the model performs reliably across different shifts, crews, and environments.
- Involving independent experts to test for hidden biases before deployment.

Bias isn't just a technical issue—it's a fairness issue. If the system is flawed, it shouldn't be used. Full stop.

In summary: if the model is going to make decisions about work, workers must help shape how that model is built. Because once it's trained, it becomes much harder to undo the problems baked in.

(See CBA Template – 6.1 Disclosure and Explainability Requirements)



Step 5.

AI Deployment: Keep the System in Check

So the AI system is going live. Now what?

This is when things get real. Once deployed, the system begins interacting with live data, reshaping task flows, influencing decisions, and embedding itself into everyday operations. And just because it worked in a test lab doesn't mean it will hold up on the terminal floor. In fact, performance often drops in real-world conditions—a well-known problem called the training-test drop.

Hence, without strong union oversight, AI systems can quickly:

- Drift from their intended goals
- Accelerate work in unsafe ways
- Shrink teams through silent attrition
- Undermine accountability, with management hiding behind "the system made the call."

Let's be clear: your role doesn't end when the system is deployed. That's exactly when vigilance becomes essential.

(See CBA Template – Sections 4.2.c, 6.2, and 8.2)

Key Union Demands During Deployment

Stay aligned with the goals you negotiated. Every AI system is introduced for a reason—whether that's improving safety, reducing errors, or streamlining logistics. However, those goals can easily get lost once the system is live. If the AI begins pushing faster workflows, misclassifying workers, or operating in ways that were never agreed upon, it must be paused or rolled back.

- Unions should demand routine performance reviews with clear benchmarks. If performance slips or new risks emerge, workers must have the right to suspend or renegotiate their use.
- Be especially vigilant about silent automation, where jobs aren't cut but simply vanish through attrition and non-replacement. The effect is the same.

(See CBA Template – 3.2 Technology Impact Assessment, 4.2.a Pre-Deployment Review)

Focus on job quality.

Not every consequence of AI shows up in productivity metrics. The system may eliminate natural breaks, push pacing beyond safe limits, or fragment tasks so severely that skilled jobs become mechanical. These shifts erode dignity, safety, and long-term employability—even if output stays stable.

That's why deployment must include a post-launch check-in—not just "is it working," but what is it doing to the experience of work?

(See CBA Template – 6.1.a. Explainability Requirements, 6.4 Monitoring and Accountability)

Keep humans in command.

Once embedded, AI systems often become the default authority—unless safeguards are in place. Can a worker override the system? Who's responsible when it fails: the employer, the vendor, or the worker stuck in the middle?

Accountability cannot be automated. If a worker is penalized due to an algorithmic error, someone must answer for it—and that someone cannot be the worker themselves. These aren't technical footnotes; they're governance questions. Address them before deployment—or risk being told later that "it's out of our hands."

(See CBA Template – 6.2 Worker Rights to Challenge and Explanation)

Co-Determination: Influence What Gets Deployed

Many systems aren't built in-house—they're bought from outside vendors. That often means less visibility, fewer guarantees, and limited transparency. But "off-the-shelf" AI doesn't get a free pass. If it's shaping your work, it must meet your standards.

Unions must engage in the procurement process. Demand full answers to critical questions:

- Who trained the system, and on what data?
- What assumptions and values are built into its design?
- Will it keep learning from workers?
- What happens to the data it collects?

Most importantly: Can it be stopped, adjusted, or audited once in place? Because once embedded, pushing back is much harder—unless you've secured those powers in advance.

(See CBA Template – 4.2.b Oversight of Vendors, 6.3 Data Stewardship Agreement)

Build Structures That Last

AI systems don't just roll out and stay the same—they evolve, retrain, and expand. That means risks can surface long after deployment. To keep pace, workers need more than a suggestion box no one checks or a survey that vanishes into management's inbox. They need clear, accessible channels to raise concerns, report harm, or flag system failures—and the assurance that those concerns will be taken seriously.

Just as importantly, they need durable, enforceable mechanisms that make oversight a permanent feature of the workplace. Unions should push for:

- A standing Joint Technology Review Committee (JTRC) with equal union representation
- Audit rights that include both scheduled reviews and on-demand investigations in response to worker concerns
- Guaranteed access to independent technical experts who can interpret how systems actually function
- Annual reports documenting which technologies are in use, what problems have been identified, and what corrective actions have been taken

Workers must also have safe, effective pathways to speak up. That means formal grievance procedures, anonymous reporting options, and strong protections for those who raise alarms.

Oversight isn't just about identifying problems—it's about having the standing power to fix them. Without these structures in place, even the strongest AI clauses risk becoming paper promises.

AI keeps learning. So the systems that govern it must be built to last.

(See CBA Template – 6.4.c Worker Feedback, 8.2 Grievance Mechanism, and 4.4 Monitoring and Audit Authority)

In Summary: Technology Is Not Destiny

AI is often presented as inevitable—something that just "arrives," reshapes the workplace, and leaves workers scrambling to adjust. But that narrative leaves out something essential: workers have power. Technology is not destiny. It is a set of choices about goals, design, deployment, and accountability. And every one of those choices can, and must, be negotiated.

This toolkit has laid out how: by asserting consultation rights early, demanding control over data, securing fair compensation, influencing how systems are built, and staying vigilant after deployment. Together, these steps form a strategy —not just for reacting to change, but for shaping it on workers' terms.

Unions have navigated waves of mechanization and automation before. AI is different in speed and scale, but not in principle. What matters now, as always, is who decides. Who defines what "optimization" means? Who benefits from increased efficiency? Who bears the risks?

When dockworkers organize around these questions, they make clear that the future of work is not something to be handed down from above —it is something to be built together.

No AI without us— because the future of work is still ours to shape.

SECTION [X]: TECHNOLOGY TRANSITIONS AND WORKER RIGHTS IN CARGO-HANDLING OPERATIONS

1. Purpose

This section establishes enforceable rights and joint governance procedures between the Employer and the Union to regulate the planning, deployment, and continued operation of Artificial Intelligence (AI), automated technologies, and data-driven systems in cargo-handling operations. It aims to ensure that technological innovation proceeds in a manner that **is** transparent, accountable, and legally compliant, while safeguarding workers' rights, dignity, and interests.

---

2. Definitions

For the purposes of this Article, the following terms shall have the meanings specified below:

- **Artificial Intelligence (AI):** Any system or particular tool that uses algorithmic logic, statistical models, or machine learning techniques to perform tasks that typically require human intelligence, such as classification, prediction, decision-making, or pattern recognition.
- **Automated Technologies:** Tools or systems that perform tasks with minimal or no human intervention, including robotics, automated scheduling systems, predictive maintenance, and autonomous vehicles used within cargo-handling operations.
- **Data-Driven Systems:** Digital systems that rely on the collection, analysis, or processing of data to guide operations or decision-making, including dashboards, optimization algorithms, or performance-monitoring software.
- **Cargo-Handling Operations:** All direct or supporting activities involved in loading, unloading, inspecting, transporting, or storing cargo within terminal, quay, or yard facilities operated, controlled, or contracted by the Employer.
- **Worker-Generated Data:** Any data, metadata, feedback, or digital trace produced by workers in the course of their duties, including operation logs, sensor interactions, task inputs, override actions, and contextual information that contributes to the design, training, or performance of automated or AI systems.
- **Tacit Knowledge:** Non-codified, experience-based understanding or intuition demonstrated by workers through their decisions, adjustments, and interactions with digital or physical systems, often extracted indirectly via data traces or feedback loops and used to improve AI performance.
- **High-Risk System:** Any AI or automated system that has the potential to significantly impact employment status, task assignment, performance evaluation, safety, or worker autonomy, as determined by the Joint Technology Review Committee (JTRC).
- **Prohibited Technology:** Any system or tool that infringes on fundamental rights to privacy, dignity, or nondiscrimination, including but not limited to emotion recognition, covert surveillance, and biometric tracking technologies, is designated as unacceptable under this Agreement and applicable laws.
- **Joint Technology Review Committee (JTRC):** A joint oversight body composed of equal representatives from the Union and the Employer, responsible for evaluating technological proposals, monitoring implementation, and ensuring compliance with risk classification, data governance, and compensation provisions under this Agreement.

3. Mandatory Consultation

3.1 Advance Notice and Scope

The Employer shall provide written notice to the Union, the Works Council (if applicable), and the Joint Technology Review Committee (JTRC) at least forty-five (45) calendar days before initiating the procurement, testing, deployment, or substantial modification of any Artificial Intelligence (AI), automated technology, or data-driven system.

3.2 Required Impact Assessment

The notice shall include a comprehensive **Technology Impact Assessment**, written in clear, accessible language and covering at least the following:

a) The strategic goals and intended functions of the proposed technology.
b) The specific tasks, departments, or work processes impacted.
c) Anticipated effects on employment levels, working conditions, job autonomy, and required skill profiles;
d) A list of all types of data to be collected, including personal and worker-generated data, with intended processing methods;
e) Legal grounds for data processing (e.g., consent, legitimate interest, compliance obligations);
f) When applicable, proposed governance measures, fallback protocols, and worker rights to contest automated decisions.

3.3 Union Review and External Expertise

Upon receipt of the Impact Assessment:

a) The Union may engage independent technical, legal, or ethical experts to review the proposed technology.
b) The Employer shall grant timely access to relevant technical documents, vendors, test results, and personnel.
c) All reasonable expenses related to the independent review shall be covered by the Employer.
d) The Union and the JTRC shall have fifteen (15) calendar days to complete their review and submit written feedback.
e) No implementation, testing, or pilot may proceed until the union has reviewed the proposal and issued a written recommendation.

4. Joint Technology Review Committee (JTRC)

4.1 Establishment and Structure

The Employer and Union shall jointly establish a standing Joint Technology Review Committee (JTRC) as the primary governance and oversight body for the planning, deployment, and operation of Artificial Intelligence (AI), automated technologies, and data-driven systems in cargo-handling operations. The JTRC shall:

I. Be composed of an equal number of representatives from the Union and the Employer;
II. Include at least one member from each side with relevant technical, legal, or ethical expertise;
III. Be granted access to independent advisors as needed, whose costs shall be borne by the Employer.

4.2 Mandate and Core Functions
The JTRC shall ensure that technological transitions proceed in a manner that is transparent, participatory, rights-respecting, and consistent with the provisions of this Agreement. Its responsibilities include:

a. Pre-Deployment Evaluation

I. Review all Technology Impact Assessments submitted under Section 3;
II. Classify proposed technologies under the risk framework (Prohibited, High-Risk, Acceptable with Safeguards);
III. Identify likely impacts on employment, autonomy, safety, and skill requirements;
IV. Issue binding recommendations regarding implementation conditions or prohibitions.

b. Oversight of Data Use and Worker Contributions

I. Review all proposed uses of worker-generated data for AI training or system optimization;
II. Approve or deny data-sharing agreements with vendors or third parties (per Section 7);
III. Recommend fair compensation measures for worker data contributions and any job restructuring, as outlined in Section 8.

c. Implementation and Safeguards

I. Define necessary oversight mechanisms (e.g., human-in-the-loop protocols, audits, fallback procedures);
II. Coordinate with relevant departments on reskilling and redeployment plans;
III. Ensure that High-Risk systems include enforceable safeguards before launch.

4.3 Decision-Making and Authority

a. The Employer shall not deploy any AI or automated system without written review from the JTRC;
b. The JTRC's decisions are binding on all matters involving Prohibited technologies and minimum safeguards for High-Risk systems;
c. In case of disagreement, either party may invoke the grievance resolution process outlined in this Agreement.

4.4 Monitoring and Accountability

a. The JTRC shall meet at least quarterly, and more frequently as required, to:
I. Review operational data from active AI systems;
II. Monitor for adverse impacts on workers or deviations from agreed implementation terms;
III. Assess compliance with transparency, safety, and data governance provisions.
b. The Committee shall prepare an annual Technology Impact Report to be shared with all stakeholders, summarizing the status, risks, and outcomes of all monitored technologies.

4.5 Resources and Support

a. The Employer shall provide the JTRC with timely access to relevant technical documentation, system logs, test results, vendor contracts, and personnel as needed to carry out its duties.

b. Reasonable costs associated with JTRC operations—including external expertise, independent audits, or legal consultation—shall be borne by the Employer.

---

5. Risk Classification

5.1. Existing and future technologies can be classified by the JTRC as follows:

a. **Prohibited**: Technologies that fundamentally undermine dignity, safety, privacy, or labor rights, such as emotion recognition, invasive biometric tracking, or AI used for covert behavioral surveillance.
b. **High-Risk**: Systems that directly influence employment status, task assignment, or performance evaluation, including algorithmic scheduling, productivity scoring, or predictive absenteeism tools.
c. **Acceptable with Safeguards**: Technologies that support efficiency or safety but require oversight, transparency, and human-in-the-loop design.

5.2. Technologies classified as "Prohibited" shall not be introduced under any circumstances.

5.3. High-Risk systems may be implemented only with Union agreement and after documented safeguards are put in place.

---

6. Transparency and Oversight of AI Systems

6.1 Disclosure and Explainability Requirements
The Employer shall disclose to the Union, affected workers, and the Joint Technology Review Committee (JTRC), in clear and non-technical language, the logic, purpose, and potential effects of any AI or automated system deployed in the workplace. This disclosure shall be provided:

- As part of the Technology Impact Assessment (Section 3.2);
- Before deployment, and in advance of any major system modification;
- For all systems classified as High-Risk or Acceptable with Safeguards (Section 5).

Each disclosure shall include:

a. A description of how the system works, including:

i. The types of data it uses (e.g., performance metrics, behavioral indicators);

ii. The decision logic by which it processes this data to generate outputs (e.g., task allocation, risk scores);

iii. The intended operational function of the system (e.g., shift planning, safety alerts);

iv. When applicable, visual or numerical explanations generated by recognized interpretability tools such as LIME (Local Interpretable Model-agnostic Explanations) or SHAP (SHapley Additive exPlanations),

to clarify how key features influence specific predictions.

b. The legal basis for data processing under applicable laws (e.g., GDPR, AI Act), including worker rights to explanation, access, and rectification.

c. A full list of internal and external parties with access to the system or its outputs, including vendors, consultants, or integrated third-party tools.

6.2 Worker Rights to Audit, Challenge, and Explanation
Where systems influence employment conditions—such as job assignments, evaluations, or terminations—the following safeguards apply:

a. **No decision shall be based solely on automated outputs**. Meaningful human review is mandatory.

b. Workers shall have the right to:
- Request a full explanation of any decision made or influenced by an AI system;
- Contest the decision and present counter-evidence;
- Be represented by the Union during any challenge or appeal process.

6.3 Oversight of Worker-Generated Data and Vendor Use
If an AI or automated system uses data generated by workers—including but not limited to sensor data, override inputs, or interaction logs—the Employer must:

a. Obtain prior review and approval by the JTRC before such data is used for AI development or optimization;

b. Secure a Data Stewardship Agreement**,** approved by the JTRC, before granting third-party access. This agreement must specify:
- Purpose and scope of data use;
- Ownership and access rights;
- Terms of worker compensation (per Section 8);
- Security and retention measures;
- Audit rights and penalties for misuse.

6.4 Audit Authority and Corrective Measures
The Union and the JTRC shall have the right to initiate audits of any deployed AI system under the following circumstances:

a. Routine review**,** to be conducted annually;

b. Triggered review**,** upon credible concern of:
- Privacy violations;
- Discriminatory outcomes;
- Misuse of worker data or deviation from agreed safeguards.

The Employer shall fully cooperate, including:

- Providing access to documentation, decision logs, and communications;
- Requiring third-party vendors to comply with audit protocols.

If violations are found, the Employer must:

- Immediately suspend use of the system;

- Collaborate with the JTRC on remediation (e.g., altering data use, reclassification, or full withdrawal).

---

7. Benefit-Sharing and Job Protections in Technological Transitions

7.1 Recognition of Worker-Generated Data as Added Value

a. The Employer and the Union recognize that data generated by workers through the performance of their duties constitutes a form of labor-derived value. As such, this data plays a critical role in the design, training, and improvement of AI and automated systems.

b. This data includes, but is not limited to:

i. Operation logs, equipment usage data, interaction patterns, sensor annotations, performance metrics, and video/audio recordings;
ii. Tacit knowledge reflected through interactions with digital systems, such as override patterns, feedback inputs, and metadata capturing decision-making or task execution processes.

c. When such data is used—directly or indirectly—to develop, train, or enhance AI or automated systems, it shall trigger obligations related to consent, governance, and compensation.

7.2 Fair Compensation for Woker-Generated Data

a. In recognition of the economic and operational value of worker-generated data and the potential job restructuring linked to automation, the Employer shall negotiate with the Union to implement one or more of the following benefit-sharing mechanisms:

i. **Wage premiums** for roles that generate continuous, high-value data used to train or calibrate automated systems;
ii. **Annual AI dividends** or one-time bonuses where data use or automation leads to measurable cost savings or productivity gains;
iii. **Royalties or revenue-sharing** when data contributions are monetized directly or indirectly (e.g., through commercial licensing or vendor partnerships);
iv. **Reduced working hours or job reclassification** without loss of pay, when automation alters job content;
v. Access to a **jointly governed AI Transition Fund**, administered by the JTRC, for training, reskilling, or early retirement.

b. All compensation mechanisms shall be reviewed annually by the Joint Technology Review Committee (JTRC) and documented in an addendum to this Agreement.

7.3 Job Security Guarantees

a. No full-time employee shall experience involuntary job loss, demotion, or income reduction as a direct result of AI, digitalization, or automation deployment.

b. Where automation modifies job tasks or staffing needs, the Employer shall:

i. Offer equivalent or enhanced roles in oversight, system operation, or maintenance;
ii. Provide fully funded training programs designed and monitored by the JTRC;
iii. Guarantee redeployment pathways (i.e., job reassignments or reallocations) that maintain existing wages, benefits, and seniority.

c. In cases involving large-scale workforce changes (e.g., role eliminations, site closures), the Employer and Union shall co-develop a Social Transition Plan, under JTRC supervision, which may include:

i. Voluntary transfers or buyouts;
ii. Early retirement schemes;
iii. Collective workload redistribution;
iv. Training and job-seek support for impacted workers.

---

8. Revisions and Regulatory Compliance

8.1 Review and Renegotiation Procedure

a. This Article—including all provisions related to AI, automation, worker-generated data, and technology transitions—shall be subject to a comprehensive review every twelve (12) months, or earlier at the written request of either party.

b. All proposed changes shall be negotiated in good faith and implemented only by mutual agreement, unless otherwise mandated by applicable law.

c. The Joint Technology Review Committee (JTRC) shall serve as the designated forum for initiating, evaluating, and coordinating revisions to this Article, especially in response to:

i. Emergent technologies not previously covered;

ii. New use cases or data applications;

iii. Evolving industry standards or worker complaints;

iv. Regulatory updates (see Section 8.3).

8.2 Grievance and Enforcement Mechanism

a. Any alleged violations of this Article—including unauthorized technology deployment, failure to consult, misuse of worker data, or non-implementation of agreed safeguards—shall be subject to the expedited grievance process outlined in Article [X] of the Collective Bargaining Agreement.

b. The JTRC is authorized to initiate fact-finding reviews, independent audits, or third-party consultations as part of the grievance resolution process.

c. Confirmed violations shall entitle affected workers and the Union to:
- Immediate suspension of the offending system;
- Backpay or compensatory measures for denied benefits or adverse outcomes;
- Binding arbitration if resolution is not reached within 30 calendar days.

8.3 Regulatory Alignment and Legal Compliance

a. The Employer shall ensure that all AI systems, data-driven tools, and automated technologies deployed in cargo-handling operations comply with relevant international, regional, and national legal frameworks, including but not limited to:

i. **General Data Protection Regulation (GDPR):** Ensuring lawful, fair, and transparent processing of personal data, including rights to access, rectification, and explanation.
ii. **EU Artificial Intelligence Act (AI Act):** Including outright prohibitions (e.g., emotion recognition), mandatory risk classification, human oversight, transparency, and conformity assessments for high-risk systems in employment.
iii. **National Labor and Collective Bargaining Laws:** Enforcing rights to consultation, co-determination, equal treatment, and protection against algorithmic discrimination.
iv. **Occupational Health and Safety Directives (OSH):** Guaranteeing that automation does not compromise physical or mental health, workplace safety, or the right to rest.

8.4 Non-Derogation Clause

Nothing in this Article shall be interpreted in a way that limits or waives any legal rights held by workers under applicable law or international labor conventions. This section shall be interpreted to enhance, not diminish, protections otherwise afforded to workers.

Appendix A: Annual Review and Compliance Checklist

Joint Technology Review Committee (JTRC) – Operational Tool

This checklist shall be used by the JTRC during its mandated annual review or any triggered audit to ensure that all AI, automated, and data-driven technologies deployed in cargo-handling operations are compliant with the terms of this Agreement.

---

1. System Inventory and Classification

- List of all AI and automated systems currently in use.
- Confirmed risk classification for each system (Prohibited, High-Risk, Acceptable with Safeguards).
- Date of last Technology Impact Assessment for each system.
- Documentation of any reclassification decisions made in the past 12 months.

---

2. Consultation and Deployment Compliance

- Was written notice provided at least 45 days before deployment or modification?
- Was a Technology Impact Assessment submitted and reviewed?
- Did the Union and/or JTRC submit formal objections or requests for clarification?
- Was deployment suspended in any case pending resolution?

---

3. Data Governance and Use of Worker-Generated Data

- List of systems using worker-generated data.
- Is there a JTRC-approved Data Stewardship Agreement for each use?
- Is there clear documentation of consent, purpose limitation, and data minimization?
- Were any third-party vendors granted data access? If yes:
  [ ] JTRC approval documented
  [ ] Security and retention safeguards in place
  [ ] Revenue-sharing or compensation mechanisms recorded

---

4. Transparency and Worker Rights

- Are explainability tools used for High-Risk systems (e.g., SHAP, LIME)?
- Have workers received clear notices about the system's logic, purpose, and effects?
- Have there been any worker challenges to algorithmic decisions?
  [ ] If yes, was human review conducted?
  [ ] Was the decision overturned or adjusted?

---

5. Compensation and Benefit-Sharing

- List of all compensation mechanisms implemented:
  • Wage premiums
  • AI dividends or bonuses
  • Royalties/revenue-sharing
  • Reduced working hours with no pay loss
  • Access to AI Transition Fund
- Have affected workers received compensation linked to data use or job changes?
- Has the JTRC reviewed and updated benefit-sharing terms in the last 12 months?

---

6. Training and Role Transition

- Were retraining or reskilling programs implemented for affected workers?
- Was redeployment offered for all displaced or reclassified roles?
- Were training outcomes evaluated by the JTRC?

---

7. Grievances and Compliance Breaches

- Number of grievances related to AI/automation filed in the last year.
- Number of investigations or audits initiated by the JTRC.
- Summary of corrective actions taken and systems suspended or modified.
- Any pending compliance issues requiring further negotiation or legal remedy?

---

8. Legal and Regulatory Updates

- Have there been any relevant changes to:
  • GDPR or data protection regulations
  • EU AI Act
  • National labor laws or OSH directives
- Has the Employer notified the Union and JTRC of compliance updates?
- Have systems been updated or withdrawn in response to legal changes?

---

9. Final Notes and Recommendations

- Summary of key findings
- Outstanding concerns or unresolved issues
- Proposed updates to the Agreement for the next review cycle

Date of Review:
Reviewed by (JTRC representatives):
Signatures: _____

Appendix B: Technology Impact Assessment (TIA) Template

To be submitted at least 45 calendar days prior to the planned deployment or modification of any AI, automated, or data-driven system.

---

1. Basic Information

- **Project Name:**
- **Date of Submission:**
- **Proposing Department/Division:**
- **Vendor(s) Involved (if any):**
- **Proposed Timeline (Testing, Deployment, Maintenance):**
- **Point of Contact:**

---

2. Purpose and Strategic Justification

- What is the intended function of the proposed system?
- What operational problem or goal is it designed to address?
- How does it align with the Employer's broader digital or automation strategy?

---

3. Scope of Application

- What terminal(s), location(s), or operational areas will the system affect?
- Which job functions, departments, or roles are expected to be impacted?
- Estimated number of workers affected directly and indirectly.

---

4. System Functionality Overview

- Brief technical description of the system (non-technical language preferred).
- Type of technology (check all that apply):
  [ ] AI or Machine Learning
  [ ] Robotics or Autonomous Equipment
  [ ] Predictive or Prescriptive Analytics
  [ ] Computer Vision
  [ ] Scheduling or Task Allocation System
  [ ] Monitoring or Surveillance System
  [ ] Other (please specify): _____
- Is the system capable of:
  [ ] Making or influencing employment decisions
  [ ] Allocating tasks or shifts
  [ ] Evaluating performance
  [ ] Monitoring behavior or location
  [ ] Improving safety or maintenance

---

5. Risk Classification (Initial Proposal)

- Proposed classification under Section 5:
  [ ] Prohibited
  [ ] High-Risk
  [ ] Acceptable with Safeguards
- Brief justification for this classification.

---

6. Anticipated Workforce Impacts

- Projected changes to:
  [ ] Job content or task structure
  [ ] Skill requirements
  [ ] Supervision models
  [ ] Worker autonomy or discretion
  [ ] Staffing levels or job security
- Describe any anticipated displacement, redeployment, or retraining needs.

---

7. Data Use and Governance

- Will the system use worker-generated data?
  [ ] Yes [ ] No
- If yes:
  - List types of data to be collected (e.g., logs, sensor data, video, override inputs).
  - State data retention period.
  - List internal and external data recipients.
  - Legal basis for data processing (e.g., consent, legitimate interest, compliance).
- Will the data be shared with third-party vendors or used for model training?
  [ ] Yes [ ] No
  If yes, a **Data Stewardship Agreement** must be attached.

---

8. Transparency and Oversight Mechanisms

- What tools will be used to ensure explainability (e.g., LIME, SHAP)?
- Will there be a human-in-the-loop or manual override mechanism?
- What fallback procedures are in place in the event of error or failure?
- How will workers be notified about system use, logic, and potential consequences?

---

9. Worker Participation and Safeguards

- Has the system been co-developed or tested with worker input?
- What measures will be in place to:
  - Contest decisions;

- Prevent retaliation;
- Enable opt-out (if applicable)?

- Attach any relevant ethical assessments or pilot reports.

---

10. Proposed Mitigation and Benefit-Sharing Measures

- What compensation mechanisms are proposed (if applicable)?
  [ ] Wage premium
  [ ] AI dividend or bonus
  [ ] Reduced work hours
  [ ] Access to Transition Fund
  [ ] Retraining/reskilling plan
- Has the Union been consulted in designing these mechanisms?
- Attach the proposed timeline and budget for implementation.

---

11. Required Attachments

- Technical documentation (whitepapers, manuals, diagrams)
- Risk classification rationale
- Draft Data Stewardship Agreement (if applicable)
- Worker communication plan
- Pilot results (if available)

Prepared by (Employer representative):
Name: _____ Signature: _____ Date: _____

Received by (Union representative):
Name: _____ Signature: _____ Date: _____

NO AI WITHOUT US!

A DOCKWORKER BARGAINING TOOLKIT ON AI

José Luis Gallegos
Jannes Ten Berge