California Management Review

INSIGHT

Business Ethics

To Be or Not to Be Transparent? How Scania and Volvo Deal with Data Transparency Paradox and Manage Compliance

Charlotte A. Shahlaei, Nicholas Berente, Annette Hultaker, Alev Yeter, and Anders Friis

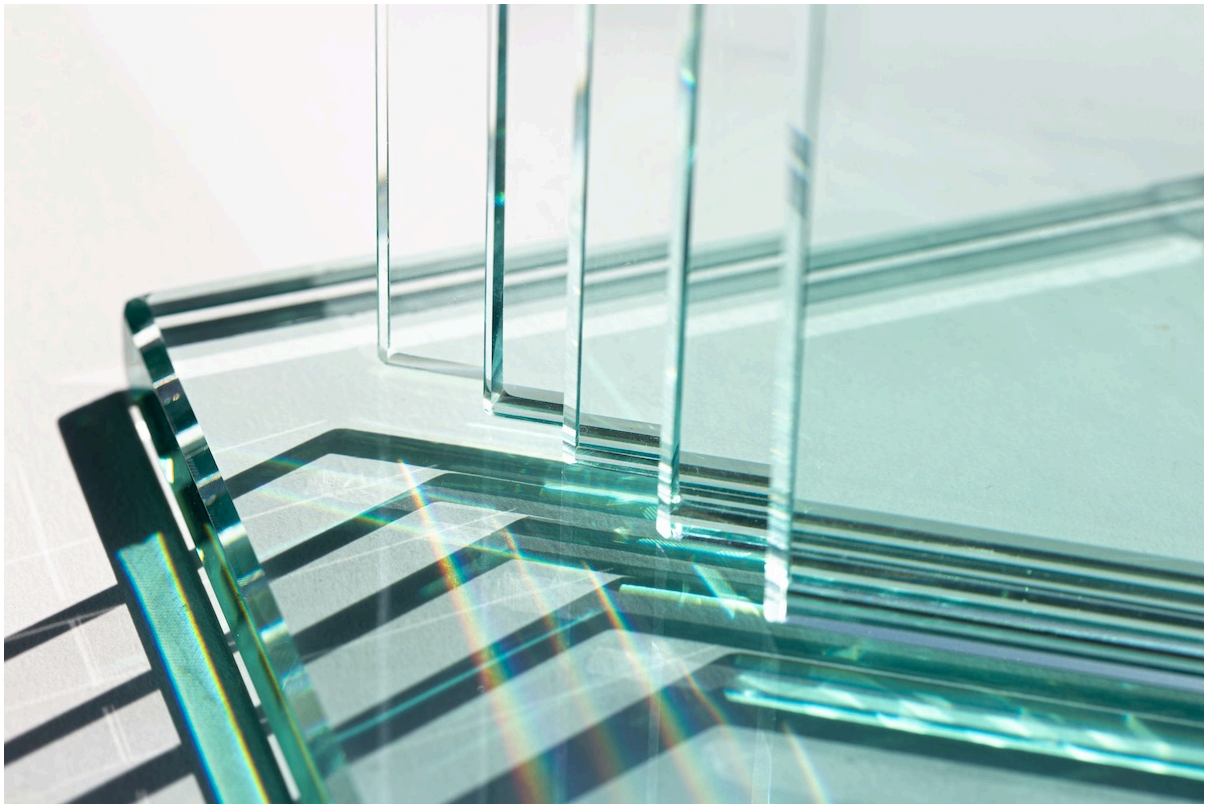


Image Credit | noprati

Navigating the data transparency paradox is a strategic imperative for IoT solution providers

Firms across all industries are amassing vast data to improve products, gain user insights, train AI models, and even for direct monetization. These practices, however, introduce significant potential liability. This is particularly true for Internet of Things (IoT) manufacturers. These firms all face what we call the “data transparency paradox”; a dilemma where the potential for legal liability escalates from both disclosing unnecessary information about data governance and failing to disclose what is essential about it, at the same time.

RELATED ARTICLES

Roy Suddaby and Rajat Panwar. “**On the Complexity of Managing Transparency.**” California Management Review Insights, November 1, 2022.

Cory Searcy, Pavel Castka, Jakki Mohr, and Sönke Fischer . “**Transformational Transparency in Supply Chains: Leveraging Technology to Drive Radical Change**.” California Management Review Insights, November 1, 2022.

Heather Domin, Francesca Rossi, Brian Goehring, Marianna Ganapini, Nicholas Berente, and Marialena Bevilacqua. “**On the ROI of AI Ethics and Governance Investments: From Loss Aversion to Value Generation**.” California Management Review Insights, July 29, 2024.

Samuel Tang and Colin Higgins. “Do Not Forget the ‘How’ along with the ‘**What’: Improving the Transparency of Sustainability Reports**.” California Management Review Insights, November 1, 2022.

Paul McGrath, Lucy McCarthy, Donna Marshall, and Jakob Rehme. “**Tools and Technologies of Transparency in Sustainable Global Supply Chains.**” California Management Review Insights, November 10, 2021.

RELATED TOPICS

Inclusivity & Transparency
Regulatory Compliance
Security & Privacy
Data Management

How should firms navigate this paradox? We draw lessons from a multi-year study with Scania AB (Scania) and Volvo Group Trucks Technology (Volvo) to explore how they deal with the data transparency paradox. These two are exemplar firms that span old and new economies as both industrial leaders and major players in data-driven connected digital technologies. With cars and trucks being major IoT data producers, these firms must resolve the transparency paradox on multiple fronts not just to avoid liability, but also to position themselves as first-mover, market shaping IoT solution providers.

Scania and Volvo follow various tactics for dealing with the transparency paradox including “strategic transparency” and “proactive diligence”. Strategic transparency is a curated approach that avoids exhaustive disclosure of information, instead focusing on clearly communicating the most essential information to users. Proactive diligence involves distributing governance among employees across the firm and empowering them with the right tools to continuously monitor evolving data demands and regulatory issues.

In this article, we describe the transparency paradox and ensuing issues for firms engaged with the IoT and connected devices. We point out how these firms face two challenges distinct from traditional approaches to handling data: data is not encapsulated by a single firm, yet firms seek to maximize their data across their platform ecosystems. The result is that firms have access to more data but without necessarily maintaining exclusive control of it. We then provide examples for how Scania and Volvo deal with the paradox through strategic transparency and proactive diligence.

Liability and The Data Transparency Paradox

The data transparency paradox can be explained from both a user perspective and a legal perspective. From a user perspective, recent European Union regulations require firms to obtain users’ approval for processing their IoT data through reasonably detailed,

transparent explanations. This need for detail, however, directly conflicts with the key feature of IoT services - that data and systems should be designed to connect and work together in the background without concerning users with intricate details. Thus, a user-oriented data governance calls for transparency and non-transparency simultaneously.

This paradox also manifests in a legal form. To prove compliance, firms must reveal enough details about their IoT data handling practices. However, an equal need for strategic opacity exists for firms to avoid the risk of creating rigid limitations. Such terms can subject them to unpredictable liability windows or force them to constantly revise contracts. Thus, compliance with IoT data regulations paradoxically calls for both transparency and opacity.

Traditionally, the boundaries of liability for a firm would be defined by the combination of regulatory compliance and contractual terms with users. “Turn-key” contracts, for instance, would assign comprehensive liability to a firm for everything within a specific domain, and none beyond that. However, IoT contexts make such turn-key contracts less tractable. IoT data is not encapsulated in the boundaries of a single firm, but is generated through an extended information system of networks, devices, platforms, as well as the organizations that provide them.[1] As a result, the role of actors and their degree of involvement can be ambiguous in IoT environments.

Further, many IoT firms pursue a strategy of “data maximalism”,[2] believing all data holds potential future value, even if its direct value is not obvious today. This leads them to favor large-scale data collection and sharing over exclusive control.[3] The direct result is a highly unpredictable future, where it’s unclear how different systems, organizations, and data will eventually be linked.

Thus, firms must navigate the transparency paradox within complex IoT ecosystems where no single entity has full control,[4] yet all are driven to maximize and share data. To address this, Scania and Volvo balance several approaches. Below, we describe strategic transparency which focuses on setting contractual terms in a strategic way, and proactive diligence which goes beyond contractual terms to demonstrate a commitment to robust

and continuous governance to stakeholders. Respectively, these methods help firms achieve transparency both in terms of explainability as well as communicating confidence in their internal governance capabilities.

Strategic Transparency at Scania

As emerging EU laws disrupt IoT data governance requirements,[5] and escalate the tensions resulting from the transparency paradox, firms operating in Europe must decide on the right level of transparency for their terms and conditions. This decision is complex, influenced not just by the paradox itself but also by a competitive landscape. Competitors in a domain all respond to regulatory requirements with their own innovative transparency approaches which can sometimes strengthen competitive positions.[6]

This creates a strategic dilemma.[7] For instance, a granular list of all the data a commercial vehicle manufacturer and solution provider is willing to process and share with users can be very attractive to its business users. But, leading firms such as Scania and Volvo are also aware that this exhaustive list can overburden users, or even restrict the firm from processing or sharing unlisted data necessitating more frequent contract revisions. Conversely, while over-generalized terms avoid these disadvantages, but they can create liability due to lack of transparency and may be less appealing to users.

In response, Scania is developing two interrelated practices that guide its judgement on determining the right level of transparency. The first is integrating minimum requirements and corner requirements, which involves identifying corner cases and indispensable transparency requirements. The second is developing agile governance for sensitive data- which involves mapping different categories of sensitive data to various user base preferences.

A) Integrating Minimum and Corner Case Data Requirements

The first step to crafting strategic transparency terms is to identify what information is indispensable and must be explicitly communicated in transparency terms. Scania achieves this by identifying both bare minimum and corner cases in IoT data handling.

These cases fall outside the scope of typical transparency terms and cannot be identified by relying on industry best practices, or historical or majority user preferences. Bare minimum cases refer to the baseline requirements where data must be processed irrespective of user preferences. This includes processing IoT data for safety and security reasons, vehicle functionality and maintenance, or for compliance with certain environmental regulations mandating manufacturers to provide information about vehicle battery performance and fuel consumption to national and European authorities.

Corner cases entail complex IoT scenarios that defy a user's normal expectations about the manufacturer's data handling processes. For example, consider a scenario where to ensure cargo safety, Scania must process data from smart trailer cabins made by another supplier. This requires the user's approval to share data among multiple firms. This is while the fleet owner who has purchased Scania trucks likely expects Scania as the complete product provider, to have control over all the truck data. Scania employs several mechanisms to manage these complex situations.

First, Scania recently implemented a sophisticated digital user agreement system. This system directly solicits end-user approval for the collection and processing of various categories of IoT data under Scania's control, and it also directs users to grant approval to other data controllers connected to a Scania product or service.

Second, this digital agreement system is integrated with an internal filtering mechanism called the "Scania Read Flag". The Read Flag filters data based on a comprehensive set of user agreements before it populates Scania's various data lakes. The Read Flag specifically scrutinizes data against the bare minimum case requirements to ensure they are prioritized over user preferences. As Scania's Data Strategy and Compliance Project Manager explained, "the Read Flag mechanism existed since the GDPR days to handle personal data, it is now evolving to handle IoT data as well." Additionally, the goal is no longer just to be clear on what data can be collected and processed, but also to define "what data can or must be shared, and with whom". This advanced system is also becoming more visible to all employees who handle the data, allowing them to see "the details of user agreements" for collecting, processing and sharing data. This level of granularity and system connection is unprecedented.

Once the indispensable information is identified and integrated into agreement filtering systems, firms like Scania could opt to be more opaque about the rest of the data categories to avoid overwhelming users with lengthy transparency explanations. However, Scania is compensating for such opaque terms by developing agile approval-control tools which empower users to manage their approval dynamically based on data categories or time frame. This approach offers users greater control over their IoT data and naturally shifts partial responsibility to them. Setting up these rather agile mechanisms can, however, be challenging and it requires that firms have a keen understanding of data categories that users potentially deem sensitive in different circumstances.

B) Agile Sensitive Data Governance

With over 700,000 connected products across 100 nations,[8] Scania faces complex IoT data governance challenges, particularly concerning sensitive IoT data categories and diverse nation-specific laws and preferences. Most firms currently lack the agility required to lead the frontier of user-oriented data governance. However, Scania's strategists are incrementally exploring viable solutions by anticipating most acute datasets, contextual conditions, and periods of heightened data sensitivity. Sensitive datasets may include geo-positioning data, driver key performance indicators (KPIs), tachometer data, or information pertaining to cargo content. The combination of these datasets can progressively amplify their sensitivity. This occurs, for instance, when cargo and geo-positioning data are linked, or when driver performance data is associated with vehicle health status.

Two crucial steps are currently under negotiation for future implementation. First, Scania is analyzing the preferences of its largest fleet owners, which can yield valuable insights into common categories of sensitive datasets and contextual conditions, as their needs often reflect those of smaller user bases. To build the required agility, Scania's initial step is to analyze and categorize that data.

For instance, South Korea, the second largest market for Scania's engines with a focus on advanced fuel efficiency, is governed by national IoT data laws with specific requirements. As Scania's head of data compliance explains, this includes local legislation concerning

geo-positioning data. Under these laws, not only must these users first approve geo-positioning data monitoring, but they also "should have the ability to 'temporarily' switch that approval off", a requirement he notes is "right now, a hassle".

This is an advanced and challenging pursuit. Switching off the collection and processing of certain datasets can affect data quality and related services. But initiating this prediction process helps Scania to create conceptual parsimony[9] and incrementally build a portfolio of cases where users value agile controls. This is where Scania's second step, developing internal anonymizer keys, is useful. When data cannot be switched off (e.g., due to bare minimum scenarios), Scania can assign priority to anonymizing and aggregating the already identified sensitive datasets.

Leading the frontier of data governance, however, is more than just strategically crafted transparency terms. It requires firms to establish trust by showing that they are invested in governance beyond contractual terms. To this end, Volvo and Scania are engaging a large array of organizational actors and domains to build a proactive governance culture.

Proactive Diligence at Volvo

Despite being industrial firms who gain market share through product quality rather than governance policies,[10] Scania and Volvo understand that investments in their governance strategies is not only a matter of liability deterrence but also a reputational concern.[11] They understand data protection and trust not in terms of written lines of a formal policy, but in terms of a social contract[12] - rooted in the assumption that these firms are also invested in maintaining stakeholder trust.

Transparency in the sense of providing accurate information about the output of data and AI-driven operations is by no means the only antecedent to building trust. In fact, excessive details risks information overload and false alarms, potentially eroding user trust more than occasional oversight.[13] Instead, users might prefer firms to communicate confidence in their data and model handling rather than overwhelming them by

exhaustive explanations.[11, 14]Volvo employs two overarching mechanisms to communicate this confidence and calibrate trust: a distributed internal governance, and continuous monitoring.

A) Democratized Internal Governance

One way for firms to communicate confidence in their own internal governance is to show that they are striving to actively reduce the psychological distance resulting from indirect and unpredictable associations.[15] Volvo does this through a decentralized governance strategy. Rather than confining responsibility to a central legal unit, Volvo engages experts from across the organization to improve clarity and oversight about data and AI solutions. These individuals do not simply follow legal guidelines, but they are educated and empowered to co-create guidelines and policies with the legal unit. This makes the approach not just distributed but also democratized, relying on distributed moral agency.[16]

Since 2020, Volvo has been enhancing its governance agility in meeting the evolving EU regulatory landscape. The key to this effort was reframing the regulations not as a mere compliance task, but as an opportunity to solve longstanding data management issues. Key actions to achieve governance agility at Volvo include, a) training a significant number of engineer representatives across all technology streams on legal requirements, and enabling them to co-develop tools and policies with legal counsel, b) fundamentally improving structural and semantic interoperability of engineering data by reviewing, refining and mapping data point descriptions and sources, and c) designing and creating checkpoints in the existing engineering systems to tag data points according to multiple interacting legal requirements.

The changes, according to Volvo's Senior Data and AI Compliance Lead, are based on the lessons drawn from new regulations like the EU AI Act which hold "even intermediary actors like importers and distributors" accountable. The firm is applying this principle internally. "It is not just the procurement, purchasing or legal, but engineers and everyone else. They cannot say they are just engineers. But responsibility has to come with empowerment, so we train them to steadily become active stewards of our principles". The goal is to let users know that Volvo on-boards "anyone who is directly or indirectly related".

It is not only the ambiguous roles of IoT actors, but also the unpredictability of future cases that concern users. Building trust then requires not only engaging diverse domain expertise but also continuous monitoring. Once a wide range of organizational actors such as engineers are trained and included in governance, ongoing monitoring of data and AI systems can turn into a long-term feasible option. Therefore, democratization and distribution of governance is an infrastructural step for continuous monitoring.

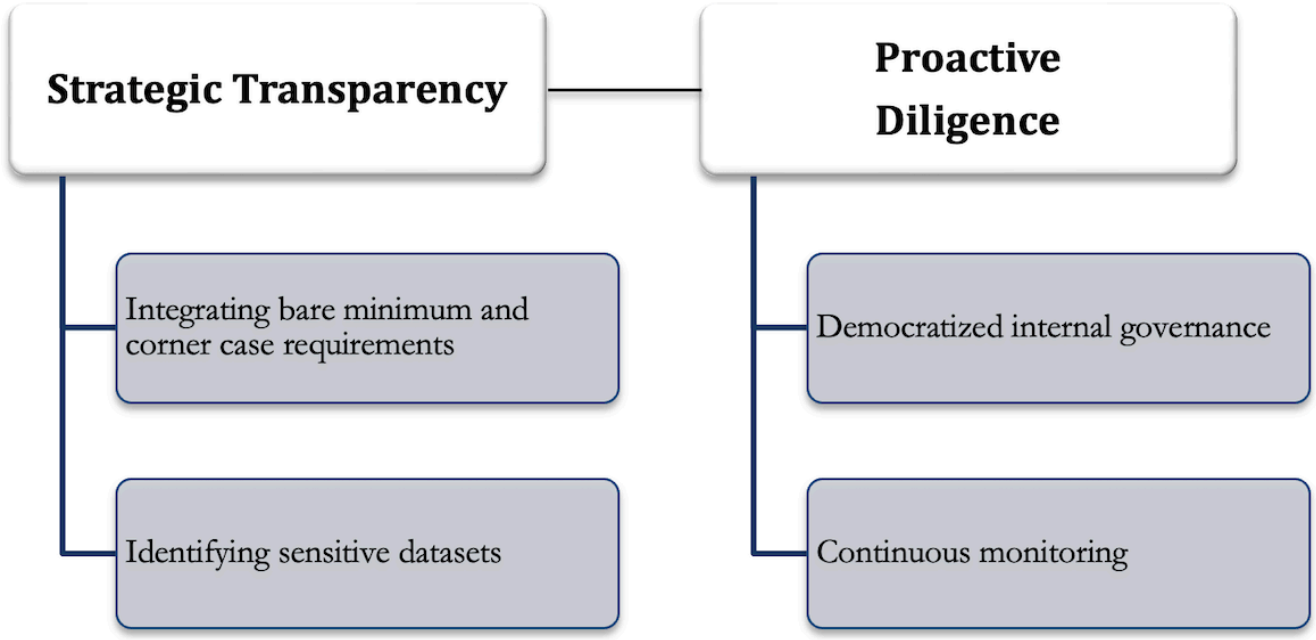
B) Continuous Monitoring

To instill trust, the temporal aspect of monitoring is as important as its scope. Confidence can be communicated in terms of distribution of problems over time or intervals of problems. Continuous monitoring signals a high level of confidence and grows trust. But it is particularly challenging for vehicle manufacturers because they traditionally designed and certified vehicles under Type Approval regulations. Under this model, once a product was tested and confirmed to be on the market, it was legally approved forever. The complexity around vehicle data and services, however, is extreme and does not fit with the assumptions in a Type Approval scheme turning it into an outdated concept. Data that can be trusted as reliable according to a specific set of criteria at one point in time can prove to be unreliable in another context, and even well-tested systems can produce unforeseen results in new applications.

As Volvo's Technical Advisory for the Implementation of Data Compliance explains, "when an engineer looks at the data, they are capable of imagining scenarios and connections that people from, e.g., legal are not, and these cases come up only when the systems and data are put into different use cases". This means that "you can't do a one-off auditing and be done with it". As Volvo's Senior Data and AI Compliance Lead emphasizes, the firm will "send the same message to suppliers and partners too". If there are two suppliers with the same solutions and one is clear about their data lineage and provenance and continues checking it, and the other is delivering a seemingly efficient but black boxed solution, Volvo "will have a preference for the first supplier".

To actualize continuous monitoring, Volvo's most important steps include, a) setting up mechanisms to continuously denoise datasets such as defining criteria against the redundant collection of vehicle data, b) linking systems that track physical components'

alterations with legal classification processes, and c) creating automated checkpoints in the existing engineering systems to prompt a review of legal classifications upon even minor changes in components collecting data or their analysis algorithms.



Conclusion

IoT environments operate based on unpredictable and ambiguous uses and connections. To meet legal transparency requirements in this environment, firms must make strategic choices about how to provide clarity without creating user confusion or contractual risks. Our examples from Scania and Volvo offer organizations an actionable framework (see figure) to think through the transparency paradox.

References

1. Michele Colli et al., "**Translating Transparency into Value: An Approach to Design IoT Solutions**." Journal of Manufacturing Technology Management 32, no. 8 (2021): 1515–32.
2. Sandra Wachter, "**The GDPR and the Internet of Things: A Three-Step Transparency Model.**" Law, Innovation and Technology 10, no. 2 (2018): 266–94.

3. Robert Wayne Gregory et al., "**Data Network Effects: Key Conditions, Shared Data, and the Data Value Duality**." Academy of Management Review 47, no. 1 (2022): 189–92.
4. Susan Winter et al., "**Beyond the Organizational 'Container': Conceptualizing 21st Century Sociotechnical Work**." Information and Organization 24, no. 4 (2014): 250–69.
5. Charlotte A. Shahlaei and Nicholas Berente, "**An Analysis of European Data and AI Regulations for Automotive Organizations**." version 3, preprint, arXiv, 2024.
6. Nelson Granados and Alok Gupta, "Transparency Strategy: Competing with Information in a Digital World." MIS Quarterly 37, no. 2 (2013): 637–41, JSTOR.
7. Roy Suddaby and Rajat Panwar, "**On the Complexity of Managing Transparency**." California Management Review 65, no. 1 (2022): 5–18.
8. "[Facts and Figures 2024 Scania Group.](https://www.scania.com/group/en/home/about-scania/scania-in-brief/facts-and-figures.html)" Scania Corporate Website, accessed August 25, 2025.
9. Rita Gunther McGrath and Atul Nerkar, "**Real Options Reasoning and a New Look at the R&D Investment Strategies of Pharmaceutical Firms**." Strategic Management Journal 25, no. 1 (2004): 1–21.
10. Kristen Martin, "Platforms, Privacy & the Honeypot Problem," Harvard Journal of Law & Technology 37, no. 3 (2023): 1–25.
11. Heather Domin et al., "**On the ROI of AI Ethics and Governance Investments: From Loss Aversion to Value Generation**." California Management Review Insights, July 29, 2024.
12. Kristen Martin, "**Understanding Privacy Online: Development of a Social Contract Approach to Privacy**." Journal of Business Ethics 137, no. 3 (2016): 551–69.
13. John Zerilli et al., "**How Transparency Modulates Trust in Artificial Intelligence**." Patterns 3, no. 4 (2022): 100455.
14. Jasper Van Der Waa et al., "**Evaluating XAI: A Comparison of Rule-Based and Example-Based Explanations**." Artificial Intelligence 291 (February 2021): 103404.
15. Joseph Weizenbaum, Computer Power and Human Reason: From Judgment to Calculation. (San Francisco: W.H. Freeman & Co, 1976), 679.
16. Luciano Floridi, "Distributed Morality in an Information Society," in The Ethics of Information Technologies, ed. Keith Miller and Mariarosaria Taddeo (Routledge, 2017).

Charlotte A. Shahlaei

Charlotte Shahlaei is a Research Associate at the Notre Dame IBM Tech Ethics Lab and Assistant Professor at Halmstad University. She specializes in technology management with a focus on how evolving European data and AI regulations are compelling strategic change within the vehicle manufacturing industry.

Nicholas Berente Follow

Nicholas Berente is the James H. Sweeny III and Alicia Sweeny Collegiate Professor of IT, Analytics, and Operations and Senior Associate Dean of Academic Programs at the University of Notre Dame's Mendoza College of Business. He is Senior Editor at MIS Quarterly and at Information and Organization.

Annette Hultaker Follow

Annette Hultåker is Technical Manager for Data and Analytics within electrification development at Scania-TRATON. She holds a Ph.D. in Physics and a guest researcher position at the Integrated Transport Research Lab at Stockholm's Royal Institute of Technology. Her work centers on data-driven organizations and conditions preventing and enabling data sharing.

Alev Yeter Follow

Alev Yeter is a Senior Information Compliance Specialist at Volvo Group Trucks Technology. She has over 15 years of experience in compliance, regulatory frameworks and IT transformation across sectors including automotive, healthcare, banking and insurance. With a legal background, she bridges business, legal and technology needs in complex regulation-heavy environments.

Anders Friis Follow

Anders Friis is a senior Enterprise and Business Architect at Capgemini Insights & Data. He has over 30 years' experience at companies such as Saab Group and Volvo Cars R&D, leading complex technical initiatives, analytics-based digital transformation, and building DevOps and PetaByte environments for ADAS system verification.