Use Case: AI-Powered Non-Compliance Monitoring for Remote Workforce

Client

A renowned Business Process Outsourcing (BPO) company with a global presence, catering to diverse industries including BFSI, Direct-to-Consumer (D2C), Healthcare, and Automotive. With a workforce of over 15,000 employees across various locations, they provide comprehensive voice and non-voice business process support to their end clients.

Business Problem

During the unprecedented challenges of the Covid-19 pandemic in 2020, the client encountered a critical dilemma. Their voice processes demanded stringent compliance, even to the extent that customer executives were prohibited from having items as basic as pens on the work floor. As remote work became the norm, ensuring data security and compliance became more complex. The risk of non-compliant activities, like unauthorized object usage and unauthorized persons in proximity, escalated due to the shift to remote work.

Solution

To address the intricate compliance concerns amidst remote work, we proposed and implemented an innovative AI-Powered Compliance Monitoring platform. The solution hinged on Computer Vision, Face Recognition, Object Recognition, and Gesture Detection technologies:

- Scenario Identification: Collaborating closely with the client, we identified scenarios necessitating alerts. These included unauthorized usage of pens, paper, mobile phones, taking pictures of laptop screens, and the presence of unapproved individuals near customer executives.

- Face Recognition Model: A custom Face Recognition model was trained with authorized customer executive faces. This lightweight model operated in real-time through laptop cameras, promptly detecting unauthorized individuals and alerting supervisors.

- Gesture Detection Model: A tailored gesture detection model was developed to recognize activities like writing, mobile phone usage, and laptop screen photography. This model, also operating in real-time, triggered alerts for such non-compliant actions.

- Object Recognition: An object recognition model was customized to identify items like pens, mobile phones, and cameras. This further fortified the platform's capability to detect non-compliance activities.

- Alert and Evidence Capture: The models immediately alerted supervisors to suspicious activities while capturing evidence in the form of pictures of customer executives engaged in non-compliant actions.

Outcome

The implementation of the AI-Powered Non-Compliance Monitoring platform delivered significant outcomes for the client:

- Enhanced Compliance: The platform allowed the client to monitor and deter 80-90% of non-compliant activities, even during the remote work scenario.

- Data Security Assurance: The solution empowered the client to uphold their stringent data safety and security commitments to end clients, fostering trust and compliance adherence.

- Risk Mitigation: By effectively preventing major data leaks or security breaches during the work-from-home setup, the client avoided potential penalties and business disruptions.

Conclusion

The AI-Powered Non-Compliance Monitoring platform exemplifies the fusion of technology and proactive strategy. Through real-time detection of non-compliant activities, the client managed to maintain compliance integrity even during a challenging remote work landscape. This successful implementation showcases the power of AI in safeguarding sensitive data, securing business processes, and ensuring compliance in an ever-evolving business environment.