



Context

In a recent decision, the Belgian Data Protection Authority (DPA) reviewed an employer's use of geolocation system company vehicles. An employee challenged the practice, arguing that he had neither given consent nor had the ability to deactivate the device outside working hours, during holidays and sick leave.

The DPA examined key aspects of this issue, particularly the legitimacy of data collection and compliance with the principles of transparency and purpose limitation.



Key principles

- **Legitimate interest, but clear purpose:** The DPA confirmed that employers may justify the use of geolocation systems based on legitimate interest, such as tracking working hours, optimizing travel, and reducing costs. However, the employer should have explicitly defined the system's purpose – in this case, tracking working hours.
- **Data Minimization and Proportionality:** The DPA found that the continuous recording of location data, including outside working hours, was disproportionate. Employers should implement solutions that allow employees to deactivate tracking outside working hours.
- **Enhanced transparency obligations:** The DPA criticized the employer's geolocation policy for being vague and ambiguous. To ensure compliance, employers must provide clear and precise information on how geolocation data is collected, stored, and used, eliminating any room for interpretation.
- **Balancing employer needs with employee rights:** While the DPA acknowledged that restricting access to geolocation data during working hours limited the impact on employees' privacy, it emphasized the need for a system that better respects individual freedoms.



Recommendations for Employers

To ensure compliance with GDPR and best practices in geolocation tracking, employers should:

- **Clarify the purpose of geolocation:** Clearly define the systems' objectives (e.g., tracking working hours) and ensure they align with a legitimate interest.
- **Enhance transparency:** Provide employees with detailed documentation on data collection, processing and usage.
- **Limit data collection:** Enable employees to deactivate geolocation tracking outside working hours or implement a technical mechanism to restrict continuous tracking.
- **Conduct a data protection impact assessment:** Assess potential risks for employees before deploying a geolocation system and implement necessary safeguards.

- **Ensure compliance with internal policies:** Regularly review and update the geolocation policy to align with evolving data protection requirements.

Our Employment & Benefits Practice is closely monitoring these developments. If you have questions or wish to discuss this topic in further, please contact our team.



Stefanie Tack



Aylin Ozturk