Beware of the geolocation of company cars

The geolocation of company cars, which is increasingly used by companies, enables employers to keep track of the movements of their employees in time and space. These devices raise certain **questions in terms of data protection**, however. They actually entail a risk of infringing on the privacy of employees who are then tracked in real time by their employer outside working hours.

In order to limit these risks, the use of a geolocation system must comply without fail **with certain rules and principles**, which derive in particular from the applicable legislation on the protection of personal data.

For the first time, on 8 April of this year, the National Commission for Data Protection ("NCDP") imposed an administrative fine on an employer whose geolocation system was operated in violation of the General Data Protection Regulation ("GDPR").

Following this decision, various lessons can be drawn on the precautions to be taken by any employer using geolocation:

Set an appropriate retention period

The retention period of the data must in fact correspond to the time **strictly necessary** to achieve the desired purpose. In addition, if geolocation has multiple objectives, a retention period must be defined for each purpose.

In addition, geolocation data may be retained beyond two months only if the geolocation has other purposes than simply tracking the location of the equipment, which justify a longer retention period (e.g., tracking and protection of transported goods).

Beyond these limits, the data must be anonymized or deleted. Failure to do so will result in retention being deemed excessive and contrary to the GDPR.

Document the content of information provided to employees

Under the principle of "responsibility," the employer must document the content of the information relating to the geolocation system that it communicates to its employees.

A simple oral communication is possible, but the proof of such communication must be documented in writing.

It is therefore advisable to communicate to employees the most important information concerning the geolocation system first, namely: the identity of the data controller, the details of the purposes pursued, the information relating to their rights as well as any information having a significant impact on the processing.

Individualize accounts and identifiers and configure access for authorized persons

Each person authorized to access the personal data processed must have an individual account, identifiers and authentication method.

Implement corrective measures without delay and cooperate during the investigation

The decision shows that the pro-activity and seriousness of the audited company in complying with the regulatory provisions largely contributed to mitigating the penalty imposed on it. Thus, the initial fine of €4000 proposed to the NCDP by the head of the investigation was finally reduced to €2,800.