THE GREEK DATA PROTECTION AUTHORITY ISSUES A GDPR FINE AGAINST PWC FOR UNLAWFUL PROCESSING OF PERSONAL DATA OF ITS EMPLOYEES

On 30 July, the Greek Data Protection Authority (the "Greek DPA") issued a fine of € 150,000 against PwC as a result of breaching of the GDPR rules in processing personal data of its employees

The Greek DPA initiated an investigation regarding the processing of personal data by PwC following a complaint submitted against the company.

From the public information it appears that the investigation was limited to the processing of personal data of PwC's employees, with a focus on the legal basis used to legitimate the data processing operations.

Following the investigation, the Greek DPA gave PwC 3 months to comply with a series of corrective measures as to bring the processing operations of its employees' personal data to compliance with the provisions of the GDPR and also applied a EUR 150,000 fine as a sanctioning measure.

BACKGROUND

In its investigation, the Greek DPA concluded that PWC:

- had used an inappropriate legal basis for the processing of personal data of its employees. Thus, without making the proof of any internal documentation to support this approach, PwC chose consent as the legal basis for processing the data of its employees;
- this resulted in an unfair processing contrary to the provisions of the GDPR, since it moved the responsibility of the data processing on the employees, while in reality, the processing of their data was performed on other legal basis, such as performance of a contract, compliance with a legal obligation or legitimate interest, as the case;
- contrary to the GDPR requirements, the processing of employees data was also non-transparent since the employees had never in fact been informed on the actual legal grounds used to process their personal data for the various purposes pursued by their employer.

The Greek DPA concluded that by means of its practices, PwC breached the paramount principle of the GDPR, accountability. The controller was not able to demonstrate compliance with Article 5 (1) of the GDPR, and it violated the principle of accountability set out in Article 5 (2) of the GDPR.

Key issues

The Greek DPA concluded that PWC:

- had unlawfully processed the personal data of its employees contrary to the provisions of the GDPR since it used an inappropriate legal basis of the processing;
- had processed the personal data of its employees in an unfair and non-transparent manner, giving them the false impression that it was using their data under the legal basis of consent, while in reality, it was using the data under a different legal basis about which the employees had never been informed;
- although it was responsible in its capacity as controller, it was not able to demonstrate compliance with Article 5 (1) of the GDPR, and that it violated the principle of accountability set out in article 5 (2) of the GDPR.

The legal basis for processing employees' data

As repeatedly highlighted by the Article 29 Working Party (now the European Data Protection Board) in its Guidelines and Opinions, in the context of employment relations consent may only be used as a legal basis for processing data of employees in exceptional and very limited situations.

The employment relationship is seen as a dependency relationship, where the employee is not in fact free to express his/her will, for fear of suffering detrimental effects as a result of a refusal.

Consent as a legal basis for processing of personal data of employees may be used only when there may be no adverse consequences on a refusing employee, while the employer is the one to demonstrate the freedom of the employee consenting to the processing.

This will always mean that the employer should properly document in advance all situations when it intends to base any of its data processing operations regarding its employees on consent.

Data processing based on performance of contract may not be covered by relying on consent

While using consent as a legal basis whenever parties enter into a contractual relationship (since such a relationship also involves a consent as a pre-condition), especially when it comes to employment contracts, the difference between the two legal basis is of utmost importance.

Many controllers see it as a better protection to obtain and base the processing of data on the consent of their contracting party, however this may have side effects in what concerns compliance with the data protection requirements and the rights of the data subject.

Using consent as a legal basis for processing data necessary in the context of executing or performing a contract may seem more protective for the controller in what concerns the respective processing, but it may also give the data subject a feeling of more power over the processing than it actually has. This is very likely to result in an inappropriate regime applicable to the respective processing, for example in terms of safeguarding measures or in the manner of dealing data subjects' rights.

The data subject withdraws his consent

Where the legal basis for consent is properly applied, meaning that no other legal basis applies, failure to grant or revoke consent would amount to an absolute prohibition on the processing of personal data. If the data subject withdraws consent, the processing of personal data under another legal basis cannot be continued.

It is clear that this may not be the case in the context of data processing in employment relations (except for very limited situations when data processing may in fact occur based on consent.)

Takeaways

Each employer should carefully assess and document the legal basis used for the processing of the various categories of personal data of their employees for each purpose of processing.

Consent may be used as a legal basis for processing of personal data in the context of employment relationships only in exceptional and limited situations.

Whenever consent is identified as a legal basis of the processing, proper documentation supporting the assessment should be available to be presented in case of an investigation from the competent authorities.

The employer must always make sure that the employee is fully and thoroughly informed on all the details of the processing of their data, in full compliance with the GDPR. The employer must be able to properly demonstrate fulfilment of such information requirements.

CONTACTS

Nadia Badea
Partner

T +40 21 6666 102
E nadia.badea
@cliffordchance.com

Ecaterina Burlacu
Senior Associate

T +40 21 6666 144
M +40 741 041 605
E ecaterina.burlacu
@cliffordchance.com