



MA NEWS

LIABILITY OF THE CONTROLLER OF PERSONAL DATA IN THE EVENT OF A CYBER-ATTACK UNDER THE GDPR

*Judgment of the Court of Justice of the European Union of 14 December 2023
Case C-340/21*

Following media reports of a cyber-attack on a Bulgarian national authority, which is said to have affected more than six million Bulgarian and foreign citizens, multiple legal actions have been brought against this authority.

In one of these actions, the Court of Justice of the European Union was asked to rule on the liability of the data controller in the event of unauthorised access to personal data under the General Data Protection Regulation (GDPR).

By decision of 14 December 2023, in case C-340/21, the Court of Justice ruled, on the questions referred to it for a preliminary ruling, that:

- In the event of unauthorised disclosure of or access to personal data or unauthorised access to those data, national courts cannot infer from this fact alone that the protective measures implemented by the controller were not appropriate. Judges must examine the appropriateness of these measures in a concrete manner;
- It is up to the controller to prove that the protection measures implemented were appropriate;
- In the event that the unauthorised disclosure of or unauthorised access to personal data has been committed by "third parties" (such as cybercriminals), the controller may have to compensate the data subjects who have suffered damages, unless he proves that the damage is in no way attributable to him; and that
- The fear that a person may have experienced about a potential misuse of their personal data by a third party, following a breach of the GDPR, is in itself likely to constitute "non-material damage".



MELO ALVES

This decision follows the judgment of the Court of Justice of 4 May 2023 in Case C-300/21, which ruled that the GDPR must be interpreted as follows:

- the mere breach of the provisions of the GDPR is not sufficient to confer a right to compensation;
- it precludes a national rule or practice which makes compensation for non-material damage conditional on the damage suffered by the data subject reaching a certain degree of seriousness; and that
- for the purposes of establishing the amount of compensation due under the right to compensation, national courts must apply the internal rules of each Member State relating to the scope of pecuniary compensation, provided that the principles of equivalence and effectiveness of European Union law are respected.

Paulo Lação

Senior Consultant