SIGNATURE



European rulings provide new clarity over data controllers' liability in cases of GDPR infringements

Five years after the entry into force of the General Data Protection Act (GDPR), the Court of Justice of the European Union (CJEU) just started to tackle a long list of questions referred to it by national courts regarding the interpretation of Article 82 GDPR on the right to compensation and liability.

In particular, the CJEU is expected to clarify the nature of the data controller's liability in case of breach of the GDPR and the kind of damages that could be compensated should the liability be established.

Whether this will trigger a wave of group actions on the basis of a GDPR-breach remains to be seen.

When GDPR was enacted, it was clear that Article 82 would raise questions and require interpretation. Indeed, Article 82 was seen as potentially becoming an important basis for data subjects to obtain redress in case of data breaches or GDPR infringements. However, national courts have been awaiting these clarifications for some time, meaning that the CJEU's 4th May ruling is an important step forward (case C-300/21).

Nature of the liability regime in case of GDPR breach

This recent ruling by the CJEU determined that Article 82 of the GDPR does not entitle an individual to compensation merely because the infringement occurred. Instead, the CJEU found that compensation is only due in cases where (i) an infringement has occurred, (ii) damage was caused to the claimant, and (iii) there was a causal link between the infringement and the damage caused.

The ruling followed swiftly after Advocate General Giovanni Pitruzzella issued an equally significant opinion on 27th April regarding a separate case dealing with the issue of compensation following a GDPR breach (case C-340/21). AG Pitruzzella determined that unlawful access to personal data by third parties does lead to liability for presumed fault on the part of the data controller and may give rise to non-material damage for which compensation can be awarded.

AG Pitruzzella's opinion was issued in relation to a case involving an unauthorised access to personal data and the moral damages allegedly suffered by one data subject following a cyberattack (case C-340/21). According to Pitruzzella, the illegal disclosure of personal data should not, in itself, constitute a breach of the GDPR from the data controller. In other words, the unlawful access to personal data by third parties in the context of a cyberattack is not sufficient to conclude that the technical and organisational measures – that must be implemented by a data controller or processor in accordance with Article 32 GDPR – were not appropriate.

As such – and in line with the CJEU's ruling shortly after – there is no automatic liability, and the data subject must demonstrate (i) a breach of GDPR, (ii) the damage suffered because of that breach, and (iii) a causal link between both. To be exempted from liability, the data controller must demonstrate that it was not responsible for the harmful event, by showing that the organisational and technical measures implemented to ensure the security of the data were appropriate, and that it is in no way responsible for the breach which gave rise to the damage suffered by the data subject. Advocate General Pitruzella also specified that the data controller cannot be exempted from liability by the mere fact that the data breach resulted from a cyberattack (i.e., a third-party).

Therefore, the level of proof required from the data controller is high.

Recoverable damages in case of a GDPR's infringement

The Advocate General considered that the data subject must suffer an "actual and certain" emotional damage as a result of the GDPR's infringement. The assessment of such damages will of course be made on a case-by-case basis in each national court where such cases are brought, but the opinion provides a valuable basis on which to consider such claims.

According to Pitruzzella, a potential misuse of personal data may constitute recoverable non-material damage under the GDPR, if proved by the data subject. However, the data subject must prove they have objectively suffered sufficiently real and certain emotional harm to meet the threshold for compensation to be





LONDON PARIS GIBRALTAR

considered. Pitruzzella noted that courts could weigh up whether such harm had occurred when hearing each case, "*provided that the principles of equivalence and effectiveness of EU law are complied with*".

The CJEU's subsequent ruling a few days later, in the case C-300/21, concurred with the conclusions reached by Pitruzzella in relation to all three conditions needing to be met in order for the right to compensation to apply. However, the CJEU also specified that a moral damage does not need to reach a specific level of seriousness, and that the EU Regulation favours a "*broad conception of 'damage'*". This may be contrary to, or difficult to align with, Pitruzzella's opinion which seems to require a "test of seriousness". As a result, the CJEU's stance could still give rise to data controllers' liability for non-serious infringements of GDPR which did not result in real and certain harm to the data subject.

Despite the rulings' impact on data subjects' ability to claim compensation in the event of GDPR breaches, national courts will still be the ultimate arbiters of each case brought before them, in terms of the size of any damages awarded. The rulings have certainly provided some much-needed clarity on the interpretation of the threshold for GDPR-related claims, but until test cases reveal courts' attitude to how much compensation is due in such cases, there is unlikely to be a sudden wave of claims and redress requests brought across the EU and UK in the meantime.

Further clarifications are expected in the near future. Indeed, the CJEU has received several preliminary ruling requests about Article 82 – see, for instance, cases C-687/21, C-741/21, C-590/22 and C-456/22.

Impact of the group action reform

The EU Directive 2020/1828 of 25 November 2020 on representative actions for the protection of the collective interests of consumers should have been transposed within national laws since 25 December 2022. French lawmakers are still working on a bill that will substantially reform the actual group action regime, even though the opt-in principle should remain.

To bring a class action in France today, the data subjects need to turn to a government-approved consumer protection group, a trade union, or a non-profit group which has existed for at least five years with a relevant statutory purpose. If the group agrees to take the case, it will represent the class in court and would distribute damages if they were granted. Data subjects may seek both injunctive relief and monetary damages not only for data security violations but also for all potential claims under the GDPR and France's Data Protection Act.

Despite the existing regime, data protection class actions have never taken off in France. Of the 32 French group actions registered by the end of 2022, only two of them related to data protection issues and never succeeded.

It therefore remains to be seen whether the upcoming reform, which aim is to simplify group actions, provide better compensation for victims and reduce the time taken to bring cases to trial, combined with the favourable interpretation of Article 82 GDPR, will trigger a rise of data protection group actions in France.



Mathilde Gérot
COUNSEL

mathilde.gerot@signaturelitigation.com