Impact of the current ECJ jurisdiction on Art. 82 GDPR on Cyber insurance

In three recent judgments (C-687/21, C-340/21 and C-456/22), the ECJ has clarified its jurisdiction on the data protection responsibility of companies for their own IT and data security, as well as on the conditions for recognising non-material damage under Article 82 of the GDPR. The Court thus provides further clarity on when data subjects can claim compensation for non-material damage against companies in the event of data loss. This continues the trend of the ECJ to expand the liability of companies, thereby increasing the likelihood of sues in the future. This will also have an impact on Cyber insurance, as situations where companies are sued by customers for compensation under Article 82 of the GDPR will generally be covered by Cyber policies. This article briefly summarizes the ECJ rulings C-687/21, C-340/21 and C-456/22, explains the provisions for a claim for compensation under Article 82 of the GDPR and concludes with a look at the insurability of such claims under Cyber insurance.

ECJ, judgment of 15.01.2024, Case No. C-687/21 – No compensation without third-party knowledge

A consumer bought a household appliance from an electronics retailer. However, at the point of sale, the appliance, along with the purchase and credit agreement documents, was mistakenly given to another customer who was cutting in line. The documents gave the queue-jumper the buyer's address, employer and income. An employee of the electronics retailer noticed the mistake, and shortly afterwards the appliance and documents were returned to the correct buyer. The customer then claimed compensation for the non-material damage he experienced as a result of the employee's error and the resulting risk of losing control over his personal data.

The ECJ rejected the claim for compensation under Article 82 of the GDPR. According to the ECJ, non-material damage does not arise merely because a person whose personal data have been disclosed to an unauthorized third party, who has not actually accessed them, nevertheless fears that the data have been copied and could be disclosed or even misused in the future. Thus, a mere feeling of unease about one's data does not justify a claim for non-material damages, especially if the data has not been accessed by an unauthorized party.

ECJ, judgment of 14.12.2023, Case No. C-340/21 – Compensation for fear of data misuse

The situation was different in a case where a Bulgarian authority was the victim of a hacking attack in which the tax and social security data of more than 6 million people were exfiltrated and published on the Internet. One of the individuals sued the authority for compensation for non-material damage, fearing that her data would be misused by third parties.

In this case, the ECJ affirmed a liability for damages. According to the ECJ, a reasonable fear of future misuse of data alone is sufficient to give rise to a claim for compensation. The authority failed to take appropriate technical and organizational measures to ensure adequate security in the processing of personal data. However, there is no automatic assumption that protective measures are inadequate or insufficient if there has been successful unauthorized access. The authority could have exonerated itself only if it had proved that the measures taken to prevent hacking were effective and that it was in no way responsible for the damage.

ECJ, judgment of 14.12.2023, Case No. C-456/22 – No de minimis threshold for compensation

It is also worth mentioning a judgment of the ECJ based on a case in which the names of two individuals were published by a city in Baden-Württemberg. Without any legal basis, the city published on its website the agenda of a council meeting containing the names of the plaintiffs, as well as an administrative court decision containing the names and addresses of the plaintiffs. Although the entry was deleted shortly afterwards, the individuals concerned claimed compensation under Article 82 of the GDPR for the unauthorized publication of their personal data.

The ECJ upheld a claim under Article 82 of the GDPR. Although it was a less significant matter, the publication of personal data on the internet and the resulting temporary loss of control over the data could have caused non-material damage to the affected individuals within the meaning of Article 82 of the GDPR. The data subjects only need to prove that they have in fact suffered such damage, however minor it may be.

According to the ECJ, there is thus no de minimis threshold for damage under Article 82 of the GDPR, and the judgment strengthens the rights of data subjects to compensation for non-material damage.

Conditions for a claim for compensation under Article 82 of the GDPR

A common feature of the CJEU's judgments is that they have always revolved around the question whether data subjects have a claim under Article 82 of the GDPR. Article 82 of the GDPR provides an independent, directly applicable tort basis that aims to provide compensation for material and non-material damage suffered as a result of breaches of data protection laws, and to sanction data protection breaches in order to prevent further breaches.

A requirement for a claim under Article 82 of the GDPR is, firstly, that there has been a breach of a provision of the GDPR. In addition, the data controller must have negligently or intentionally caused the data protection violation. Fault is generally presumed. In order to exculpate itself, the data controller must therefore prove that it was not responsible for the event causing the damage by taking appropriate technical and organizational measures to ensure adequate security in the processing of personal data. For example, if a company affected by a data breach or exfiltration can prove that it took all reasonable steps to prevent the loss of data, exculpation may be possible.

According to consistent case law, the essential core of a justified claim for damages under Article 82 of the GDPR is the occurrence of causal damage. This can be both material damage, which can be quantified in concrete financial terms (e.g. financial loss due to the use of the payment data of the data subject), as well as non-material damage. In order to establish a claim for non-material damage, it is generally considered that the data subject must have suffered a tangible disadvantage resulting from an objectively comprehensible impairment of personal interests.

Insurability in Cyber insurance

"It is reassuring that in cases where companies are sued by customers for damages under Article 82 of the GDPR, there is usually coverage under Cyber insurance policies. The scope of Cyber insurance is usually opened because there is a so-called "coverage triggering event" in the form of a breach of data protection regulations," reassures Dr Marcel Straub, Head of Legal at Finlex. "Physical documents or non-electronic data are also considered as data in many wordings, so that even in the case of the electronics retailer (Case No. C-687/21), where purchase and credit contract documents were inadvertently passed on to another customer, a coverage-triggering event would be assumed,"

adds the in-house lawyer.

If a coverage-triggering event exists, the liability portion of the policy is activated. The first step is for the insurer to assess the liability. On the basis of this assessment, the insurer then provides cover for the judicial and out-of-court defense costs of unsubstantiated claims or indemnifies the insured company against substantiated claims.

"This means that in all three ECJ cases, an insurer would have had to cover the reasonable defense costs incurred. In addition, insurance coverage would generally also extend to an insurer having to pay the compensation that the company owes to customers. In cases C-340/21 and C-456/22, insurance coverage would therefore exist both for the costs of unsuccessfully defending against the claims brought and for the compensation claims to be paid under Article 82 of the GDPR," Dr. Straub concludes.

Outlook

The judgments extend the existing case law on Article 82 of the GDPR and clarify the already recognizable line of the ECJ. By emphasizing the need for a concrete and individual assessment of security measures, as well as the responsibility of data processors and the rejection of a de minimis threshold for non-material damage, the ECJ further strengthens the rights of data subjects in the event of data protection breaches.

Dr. Straub: "Of the more than 200 Cyber claims that we have dealt with over the last two years at Finlex's claims department, very few claims have so far been made against companies for compensation under Article 82 of the GDPR. However, recent case law suggests that the number of such claims is likely to increase in the future. Therefore, companies are well advised to take out a Cyber policy – also with regard to the cost risk of claims under Article 82 of the GDPR. Even if a potential claim under Article 82 of the GDPR for an individual data subject usually only amounts to a three- or four-figure sum, in a case involving a large number of affected persons, the damage could run into millions. For example, if a medium-sized company has 10,000 customers' data stolen and each affected individual is entitled to compensation of €500, the total amount of potential compensation claims, excluding legal and court costs, would already amount to €5 million. It is therefore imperative that companies protect their IT and customer data. In addition, risk management should be strengthened, and reliable documentation of the measures taken should be established in view of the burden of proof. In addition, every company should seriously consider taking out Cyber insurance to minimize the cost risk and to have a specialist at their side in case of need."

The following images are released for reprinting subject to editorial, non-commercial use.

Dr. Marcel Straub | (Press photo)

Photo credit: Finlex GmbH

Finlex

Press contact

Finlex GmbH

Denise Jetzki | Head of Marketing & Communication
E-Mail: marketing@finlex.de
Phone: +49 (0) 69 / 8700 142-00

finlex.io