To act or not to act: are supervisory authorities obliged to take corrective action when personal data has been breached?

On 26 September, the CJEU ruled in Land Hessen (C-768/21) that supervisory authorities are not required to automatically exercise corrective powers, such as imposing fines, in the event of a personal data breach.

29 October 2024

The Court of Justice of the European Union (**CJEU**) issued a judgement in Land Hessen (C-768/21) on 26 September, confirming that in the event of a personal data breach, supervisory authorities are not obliged to exercise their corrective powers, (such as imposing an administrative fine) as a matter of course. It will depend on the specific circumstances of the case and whether the authority considers the exercise of such powers is appropriate and proportionate to address the relevant infringement and ensure that the GDPR is fully enforced.

Background

In 2019, a German savings bank detected that one of its employees had unlawfully accessed a customer's personal data, on several occasions. The bank investigated the issue and took disciplinary action against the relevant employee. In accordance with Article 33 of the GDPR, it notified the Land Hessen's Data Protection Commissioner (the **Commissioner**) of the data breach.

However, the bank did not notify the relevant customer of the breach (under Article 34 of the GDPR), as the bank's data protection officer was satisfied it did not pose a high risk to the relevant customer's rights and freedoms. Even though the employee had consulted the personal data, there was no evidence that the employee had disclosed them to third parties or had used them to the customer's disadvantage.

The customer became aware of the breach incidentally and lodged a complaint with the Commissioner. The customer alleged that the breach of his personal data should have been communicated to him directly and the failure to do so was in breach of Article 34 GDPR. He also criticised the period for which the bank's access logs were retained, (set for a three month retention period), and the fact that savings bank employees seemed to have extensive access rights to customer data.

Having assessed the complaint, the Commissioner found that the bank had not infringed Article 34 GDPR, since the bank's assessment that the personal data breach committed was unlikely to result in a high risk to the customers rights and freedoms, was not manifestly incorrect. As regards the issue of access by employees to personal data, the Commissioner rejected the customer's claim, observing that extensive access rights may, in principle, be granted where it is certain that each user is informed of the conditions under which employees may access the data. Finally, the Commissioner stated that it had

requested the bank to keep its access logs for a longer period than three months. Importantly the Commissioner did not deem it appropriate to issue a fine to the bank for an infringement of the GDPR.

The relevant customer subsequently challenged the Commissioner's decision before the German Courts, requesting that the Commissioner be ordered to take action against the bank.

The customer claimed that the Commissioner should have imposed a fine on the bank in view of the latter's various infringements of the provisions of the GDPR, in particular Article 5, Article 12(3), Article 15(1)(c), Article 33(1) and Article 33(3). According to the customer, where a breach of the GDPR is established, the principle of expediency does not apply, so that the Commissioner did not have discretion to decide whether or not to act but that, at most, its discretion extended to which measures to adopt.

Question referred

Following consideration of the customer's claim, the German court referred the matter to the CJEU. The referring court essentially asked, where a breach of the GDPR's provisions relating to the protection of personal data is established, should the GDPR be interpreted as meaning that the supervisory authority is *required* to exercise corrective powers under Article 58(2), (such as the power to impose an administrative fine).

CJEU's approach

In considering the query referred to it, the CJEU noted at the outset that it must always be borne in mind that "*the interpretation of a provision of EU law requires that account be taken not only of its wording, but also of its context and the objectives and purpose pursued by the act of which it forms*".[1]

The CJEU stated that the objective pursued by Article 83 GDPR, as informed by Recital 148, is to strengthen the enforcement of the rules of that regulation. However, recital 148 also states that, in a case of a minor infringement or if the administrative fine likely to be imposed would constitute a disproportionate burden to a natural person, supervisory authorities may refrain from imposing an administrative fine and instead issue a reprimand.[2]

The CJEU stated that the objective of Article 58(2) GDPR is to ensure that the processing of personal data complies with the GDPR and to remedy situations where there has been an infringement. The CJEU also noted that Article 58(2) confers on supervisory authorities the power to adopt various corrective measures. It follows from this that the GDPR intends to provide those authorities with a degree of discretion as to the manner in which it will remedy any shortcoming it finds.[3]

The CJEU referenced the ruling in *Facebook Ireland and Schrems*, C-311/18, which confirmed that a supervisory authority must determine which action is "a*ppropriate and necessary*", and must do so "*taking into consideration all the circumstances of the specific case*" and "*executing its responsibility for ensuring that the GDPR is fully enforced with all due diligence*".[4]

The Court emphasised that the system of sanctions provided for by the EU legislature allows supervisory authorities to impose the most appropriate penalties depending on the circumstances of each case. As a result, it cannot be inferred either from Article 58(2) or from Article 83 GDPR that the supervisory authority is under an obligation to exercise a corrective power, in particular the power to impose an

administrative fine, in all cases where it finds a breach of personal data. Its obligation in such circumstances is to react appropriately in order to remedy the shortcoming found.

The Court stated that, in exceptional cases, the exercise of corrective powers might not be necessary if the specific circumstances of the case indicate that:

- the relevant GDPR violation has been fully rectified
- any ongoing processing by the controller is in compliance with the GDPR and
- the supervisory authority's decision not to exercise its power does not compromise the robust enforcement of GDPR requirements[5]

Access to the full judgement is available here.

For further infromation in relation to this topic, please contact Chris Bollard, Shannon Owens or any member of A&L Goodbody's Technology team.

Date published: 29 October 2024

[1] *Land Hessen* (C-768/21) at [30]

[2] *Land Hessen* (C-768/21) at [47]

[3] *Land Hessen* (C-768/21) at [37], and[45] - [46]

[4] *Facebook Ireland and Schrems*, (C-311/18) at [112]

[5] *Land Hessen* (C-768/21) at [46]