American company fined 2.5 million NOK for failure to notify the Data Protection Authority within 72 hours

Petter Bjerke
Partner, Location Head IPT

William Myhr
Associate

The duty to notify data breaches (personal data security) and affected parties of data breaches is a one of many key obligations under the GDPR. Failure to notify the data protection authorities of such data breaches may have severe consequences.

The Norwegian Data Protection Authority issued last week one of its first administrative fines for failure to notify the Data Protection Authority within the required 72 hours.

Medical device supplier Argon Medical Devices, Inc. reported a data breach 67 days after becoming aware of a data breach. The GDPR requires businesses to notify supervisory authorities within 72 hours of the business becoming aware of the data breach. The Norwegian Data Protection Authority believed that Argon Medical Devices, Inc. notified too late and issued the company an administrative fine of 2.5 million Norwegian Kroners (NOK).

Facts of the case

On 24 September 2021, Argon Medical Devices, Inc. filed a data breach notification to the Norwegian Data Protection Authority, stating that in the period 21 May 2021 to 14 June 2021, the company had been exposed to a cyber-attack. The incident resulted in the attacker gaining unauthorized access to the personal data of all employees in Europe, including a Norwegian employee.

The security incident was first discovered on June 14, 2021, which led to the launch of an internal investigation of the incident. At the beginning of the internal investigation, the main focus was on the company's operations in the USA. However, on 19 July 2021, the company became aware that the breach also involved European employees.

Argon Medical Devices, Inc. therefore carried out an assessment of whether the data breach was notifiable under the GDPR and concluded that the breach had to be notified. However, the notification was first filed on 24 September 2021.

The Norwegian Data Protection Authority's assessment

When the Norwegian Data Protection Authority received the notification of the data breach, the Norwegian Data Protection Authority requested more information about what measures the company took between 19 July 2021 and until the Norwegian Data Protection Authority received the notification of the data breach on 21 September 2021. To this, Argon Medical Devices, Inc. replied that during this period they conducted an internal investigation. Argon Medical Devices, Inc. stated that they first had sufficient information regarding the data breach when they notified the data breach to the Norwegian Data Protection Authority in September and that they had therefore notified within the 72-hour deadline that applies to notifiable data breaches.

The Norwegian Data Protection Authority disagreed and concluded that the 72-hour period commences when a company becomes aware that a data breach has occurred, and not when the business has a full overview of the breach.

The Norwegian Data Protection Authority therefore considered that the company had breached the 72-hour deadline and issued an administrative fine of NOK 2.5 million. As an aggravating factor, the Norwegian Data Protection Authority emphasized that the company had not provided precise enough information in its correspondence with the Norwegian Data Protection Authority and that it was only a careful examination of the notification by the Norwegian Data Protection Authority that revealed that the 72-hour deadline had been breached. Furthermore, the Data Protection Authority emphasized that the personal information that had been exposed, such as salary and benefit information, was of a sensitive nature.

For more information, please see the decision here.

What can businesses learn from the decision?

The decision from the Norwegian Data Protection Authority shows the importance of handling data breaches appropriately.

Firstly, companies must have appropriate routines for detecting data breaches and how data breaches are to be notified. In Argon Medical Devices, Inc.'s routines, it was stipulated that data breaches should only be

notified when the company had a full overview of the data breach. According to the GDPR and the Norwegian Data Protection Authority's assessment, this was not correct.

Secondly, the decision is an important reminder that data breaches must be notified no later than 72 hours after a company becomes aware of the data breach. If the company does not have the full overview within the deadline, it must be notified successively, as the business receives more information.

Thirdly, the decision shows that businesses established outside the EEA must be diligent of whether EU citizens are also affected by a data breach. If the business' focus is limited in scope, for example limited to American laws and regulations, there is a risk that 72-hour deadline may be exceeded.

Services	Immaterialrett og teknologi