Datatilsynet

Argon Medical Devices, Inc.
2600 Dallas Parkway, Suite 440
Frisco, TX 75034 USA

| Your reference | Our reference | Date |
|---|---|---|
| | 21/03126-13 | 08.03.2023 |

## Administrative Fine — Argon Medical Devices, Inc.

### 1. Introduction and Summary

The Norwegian Data Protection Authority ("Datatilsynet", "we", "us", "our") is the independent supervisory authority responsible for monitoring the application of the General Data Protection Regulation ("GDPR")[1] with respect to Norway.

On 24 September 2021, Argon Medical Devices, Inc. ("Argon", "you", "your", the "company") submitted a personal data breach notification to Datatilsynet pursuant to Article 33(1) GDPR. Such notification concerned a cyber security incident that Argon experienced between 21 May and 14 June 2021, which affected the personal data of all of Argon's European employees, including one employee in Norway.

Further to an inquiry into this matter, Datatilsynet found that Argon became aware of the personal data breach in question at least on 19 July 2021, and that it notified the breach to Datatilsynet 67 calendar days after that date, thus well beyond the statutory deadline imposed by Article 33(1) GDPR for personal data breach notifications.

In light of the above and for the reasons outlined below, Datatilsynet issues an administrative fine of NOK 2 500 000 (two million and five hundred thousand) against Argon for having infringed Article 33(1) GDPR.

### 2. Decision

Pursuant to Articles 58(2)(i) and 83(4)(a) GDPR, we impose an administrative fine of NOK 2 500 000 (two million and five hundred thousand) against Argon Medical Devices, Inc. for:

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ [2018] L 119/1.

- having infringed Article 33(1) GDPR by failing to notify a personal data breach without undue delay.

Our inquiry has only focused on Argon's compliance with Article 33(1) GDPR. Thus, the present decision is without prejudice to the possibility of opening future inquiries into Argon's compliance with other provisions of the GDPR, including with the security requirements imposed by Articles 5(1)(f) and 32 GDPR and the data protection officer requirements laid down in Articles 37-39 GDPR.

## 3. Factual Background

On 24 September 2021, the law firm Ræder AS wrote to Datatilsynet to inform us—on behalf of Argon—that between 21 May and 14 June 2021 Argon had experienced a cyber security incident, which affected the personal data of all of Argon's employees in Europe, including one employee in Norway.[2] Argon sent an analogous personal data breach notification to several other European supervisory authorities.[3]

The incident at hand concerned an unauthorized access to the mailbox account of Argon's US Senior Vice President of Human Resources.[4] Most notably, the threat actor had accessed a spreadsheet containing personal data such as salary and benefits of all of Argon's European employees,[5] including a Norwegian employee,[6] which was contained in the [redacted] connected to that mailbox account.[7]

Argon has indicated that the personal data affected by the incident include the following kinds of data:

*(a) Name*

*(b) Job Title*

*(c) Location (which only includes the City and Country of the respective employee)*

*(d) Employee Hire date*

*(e) Statutory holiday entitlement*

*(f) Total salary 2020*

[2] See Notification of Personal Data Breach - Argon Medical Devices, lnc. (ref: 129172) (hereinafter "Argon's Notification"). Argon's Notification was wrongly dated 24 September 2020, but it was submitted to Datatilsynet on 24 September 2021.
[3] Ibid., para. 2.7.
[4] Ibid., paras. 1.1-1.7.
[5] Ibid., paras. 1.4 and 2.2-2.6.
[6] It should be noted that, although Argon's notification generally refers to "Argon's employees within the EU and UK" or "EU/UK employees", such references are to be understood as encompassing also EEA employees, as Argon's Notification makes express reference to Norway (see e.g. para. 2.5).
[7] Argon's Notification, para. 1.4.

*(g) Bonus*

*(h) Employer paid social charges*

*(i) Employer paid pension & Insurance*

*0) Additional employer paid benefits*

*(k) Company car/Car allowance/Mileage.*[8]

In its notification to Datatilsynet, "Argon recognises that the Involved Data, being salary and benefits information, is subject to a greater degree of sensitivity on the part of the employees."[9] However, Argon considered that the steps it took after it discovered the incident mitigated the risks to the individuals concerned.[10]

The timeline of the incident, and the steps taken by Argon in response to it, may be summarized as follows:

- On 14 June 2021 at 20:24 UTC, Argon's IT security team was alerted by the company's US Senior Vice President of Human Resources of an oddity in his day-to-day activity, namely that he appeared to be missing emails within his mailbox.[11]

- Upon further investigation, Argon determined that it had been subject to a business email compromise, perpetrated through its [redacted] platform by an unauthorized third party, most likely through a phishing email. Argon also determined that such a third party may have logged in to the relevant mailbox account on 21 May 2021 at 18:06 UTC, and that the third party commenced substantive activity on that account on 25 May 2021.[12]

- Upon discovery of the incident, Argon's Director of Global IT Security put in place several cyber security measures, which appear to have contained the incident on 14 June 2021.[13]

- Thereafter, on 15 June 2021, Argon reported the incident to the local FBI Cybercrime Unit in the United States.[14]

[8] Argon's Notification, para. 2.4.
[9] Ibid., para. 2.6.
[10] Ibid., para. 3.1.
[11] Ibid., para. 1.1.
[12] Ibid., paras. 1.1-1.2.
[13] Ibid.
[14] Ibid., para. 4.4.

- Following containment of the incident, Argon commenced an internal investigation to determine the extent and nature of the incident.[15] This led to the discovery—on 19 July 2021—that the personal data of Argon's European employees had been affected by the incident. In this regard, Argon's notification to Datatilsynet states:

> *further investigation* […] *completed by Argon and its cyber forensic expert on l9 July 2021, revealed that two files within the* [redacted] *connected to the Mailbox Account (the "Share Files") were accessed by the Threat Actor, as detailed in the* [redacted] *logs. These Share Files included* […] *a spreadsheet containing the salary and benefits personal data of all 20 of Argon's European employees (including 16 employee located in EU/UK jurisdictions* […]*).*[16]

The notification further states:

> *Argon only became fixed with knowledge of the Share File relating to the personal data of the l6 EU/UK employees (and additional 4 Swiss employees) on 19 July 2021.*[17]

- After having realized that the incident had affected the personal data of individuals in several EU/EEA countries, Argon undertook an assessment of whether the incident was reportable under Article 33(1) GDPR. This assessment revealed that the incident was reportable, as Argon concluded that:

> *(i) a qualifying personal data breach, (ii) involving personal data, (iii) connected to 16 UK (and EU) individuals including 1 Norwegian individual, (iv) that was not unlikely to result in a risk to the rights and freedoms of said individuals, had occurred.*[18]

- Therefore, Argon submitted a personal data breach notification to Datatilsynet and several other European supervisory authorities on 24 September 2021.

In essence, 67 calendar days elapsed from the moment in which Argon become "fixed with knowledge"[19] that the incident had affected the personal data of individuals in the EU/EEA on 19 July 2021 until it notified Datatilsynet on 24 September 2021. Argon's notification to Datatilsynet explained this temporal gap as follows:

> *Argon only became aware with a reasonable degree of certainty that, in all the circumstances of the Incident and the personal data involved* […]*, the Incident may be reportable on 21 September 2021, upon receipt of related advice from its legal advisers,*

[15] Ibid., para. 1.2.
[16] Ibid., para. 1.4 (emphasis added).
[17] Ibid., para. 1.7 (emphasis added).
[18] Ibid., page 1.
[19] Ibid., para. 1.7.

*and coordination of legal counsel across the EU and UK jurisdictions in scope for the Incident.*[20]

Upon receipt of Argon's notification, Datatilsynet sent Argon a request for further information on 4 October 2021.[21] In particular, Datatilsynet asked Argon to describe the activities it undertook between l9 July and 21 September 2021 in relation to the incident, and asked the company to clarify why it claimed that it became aware that the incident was reportable only on 21 September 2021.

On 28 October 2021, Argon answered Datatilsynet's questions.[22] In its letter to Datatilsynet, Argon reiterated its view that the company acted "without undue delay, to notify the supervisory authorities within 72 hours […] by 24 September 2021".[23] It also described the steps it took in relation to the incident in the period from 19 July to 21 September 202l, and provided further updates and clarifications on the incident and related notifications it filed in Europe. It also informed Datatilsynet that, on 20 October 2021, Argon proceeded to notify all of the data subjects affected by the incident. [24]

On 31 January 2022, Datatilsynet sent Argon an advance notification of its intention to issue an administrative fine of NOK 2 500 000 (two million and five hundred thousand) against Argon for having violated Article 33(1) GDPR.[25]

On 22 February and 11 March 2022, Argon submitted written representations to Datatilsynet regarding the contested violation and envisaged administrative fine.[26] In its written representations, Argon essentially confirmed the factual elements it provided in the personal data breach notification it sent to Datatilsynet in September 2021, but added that "Argon's third-party forensic expert undertook a comprehensive forensic investigation from 1 July 2021 to 29 July 2021, when Argon received the full findings and conclusions of the investigation".[27] However, as Argon never mentioned the date of 29 July 2021 in its personal data breach notification (or in the response it sent us on 28 October 2021), Datatilsynet asked Argon to confirm the correctness of such a date, and whether the reference to the date of 19 July 2021 in the notification was correct. In its response, Argon confirmed the correctness of the information provided in the personal data breach notification, but noted that "Argon considers that both dates form part of the chronology, each forming part of the continuum of the full and comprehensive forensic investigation Argon undertook with the assistance of a third-party expert."[28] In essence, Argon confirmed the correctness of the information provided in the personal data breach notification, which constitutes the primary evidence to be taken into account for the purpose of the present case.

---

[20] Ibid., para. 1.7.
[21] See Datatilsynet's letter to Argon dated 4 October 2021 (ref: 21/03126-3).
[22] See Argon's letter to Datatilsynet dated 28 October 2021 (ref: 729172/129172) (hereinafter "Argon's Response to Datatilsynet").
[23] Ibid., para. 3.3.
[24] Ibid. para. 7.1.
[25] See Datatilsynet's letter to Argon dated 31 January 2022 (ref: 21/03126-6).
[26] See Argon's letters to Datatilsynet dated 22 February and 11 March 2022.
[27] See Argon's letter to Datatilsynet dated 22 February 2022, p. 9.
[28] See Argon's letter to Datatilsynet dated 11 March 2022, p. 4.

The present decision takes account of Argon's written representations. However, in our view, Argon's submissions do not warrant any significant changes in our assessment of the present case, as outlined in further detail below.

## 4. Legal Background

### 4.1. Scope of Application of the GDPR

Under Article 2(1) GDPR, the Regulation:

> […] *applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.*

Moreover, Article 3(1) GDPR provides that the Regulation:

> […] *applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.*

### 4.2. Definitions

The GDPR lays down the following definitions, which are relevant in the present case:

Pursuant to Article 4(1) GDPR:

> "*personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*

Pursuant to Article 4(2) GDPR:

> *"processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.*

Pursuant to Article 4(7) GDPR:

> *"controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing*

*of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.*

Pursuant to Article 4(12) GDPR:

*"personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.*

### 4.3. Notification of a Personal Data Breach to the Competent Supervisory Authority

Article 33 GDPR sets out personal data breach notification requirements. In particular, Article 33(1) provides that:

*In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.*

Further, Article 33(4) reads:

*Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.*

### 4.4. Competence, Tasks and Powers of Supervisory Authorities under the GDPR

Pursuant to Article 55(1) GDPR:

*Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State.*

Further, Article 56(1) GDPR reads as follows:

*Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.*

The term "main establishment" is defined in Article 4(16) GDPR as follows:

*"main establishment" means:*

*(a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;* […].

Pursuant to Article 58(2) GDPR:

*Each supervisory authority shall have all of the following corrective powers:*

*(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;*

*(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;*

*(c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;*

*(d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;*

*(e) to order the controller to communicate a personal data breach to the data subject;*

*(f) to impose a temporary or definitive limitation including a ban on processing;*

*(g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;*

*(h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;*

*(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;*

*(j) to order the suspension of data flows to a recipient in a third country or to an international organisation.*

### 4.5. General Conditions for Imposing Administrative Fines

The general conditions for imposing administrative fines are laid down in Article 83 GDPR. In particular, Article 83(1) provides that:

> *Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.*

Further, Article 83(2) states:

> *Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:*
>
> *(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;*
>
> *(b) the intentional or negligent character of the infringement;*
>
> *(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;*
>
> *(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;*
>
> *(e) any relevant previous infringements by the controller or processor;*
>
> *(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;*
>
> *(g) the categories of personal data affected by the infringement;*
>
> *(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;*
>
> *(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;*

*(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and*

*(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.*

Moreover, Article 83(4)(a) reads:

*Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:*

*(a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43.*

### 4.6. EEA and Norwegian Law

The GDPR has been incorporated into Annex XI to the European Economic Area ("EEA") Agreement by means of Decision of the EEA Joint Committee No 154/2018 ("EEA Joint Committee Decision").[29]

Article 1(b) of the EEA Joint Committee Decision provides that:

[…] *the terms "Member State(s)" and "supervisory authorities" shall be understood to include, in addition to their meaning in the Regulation, the EFTA States and their supervisory authorities, respectively.*

Further, Article 1(c) of the EEA Joint Committee Decision reads as follows:

*References to Union law or Union data protection provisions shall be understood as referring to the EEA Agreement or data protection provisions contained therein, respectively.*

The Norwegian Personal Data Act incorporated the GDPR into Norwegian law.[30] The Personal Data Act and the GDPR entered into force in Norway on 20 July 2018.[31]

[29] Decision of the EEA Joint Committee No 154/2018 of 6 July 2018 amending Annex XI (Electronic communication, audiovisual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement OJ [2018] L 183/23.
[30] Act No 38 of 15 June 2018 relating to the processing of personal data ("personopplysningsloven").
[31] Ibid., § 32.

## 5. Datatilsynet's Competence

In its notification to Datatilsynet, Argon stated:

> *Argon has a global presence, with customer service, direct sales and manufacturing facilities in multiple jurisdictions, including but not limited to, Singapore, the US and Europe (France, Denmark, Norway, and others).*[32]

Thus, Argon has several establishments in the EU/EEA, including in Norway, and in the context of the activities of these establishments it processes personal data, including personal data of its European employees. Therefore, the GDPR applies to such data processing activities in accordance with Article 3(1) GDPR. In this regard, Argon acknowledged that "Argon in the US [i.e., Argon Medical Devices, Inc.] is the data controller with respect to the personal data connected to this Incident".[33]

Argon has also indicated that:

> *Argon's European head office resides in Switzerland, and only its Swiss establishment enjoys a power of direction and control over its other EU/EEA establishments. Therefore, Argon does not have a main establishment in the EU/EEA for the purposes of Article 4(16) of the GDPR.*[34]

Consequently, the cooperation mechanism and procedure set out in Articles 56(1) and 60 GDPR do not apply in this case, as the existence of a "main establishment" in the EU/EEA is one of the key conditions for the application of the so-called One-Stop-Shop mechanism.[35] Therefore, pursuant to Article 55(1) GDPR, we are competent to perform the tasks assigned to us and exercise the powers conferred on us by the GDPR in relation to the personal data breach notification that Argon submitted to Datatilsynet. This was not disputed by Argon in its written representations.[36]

It should be made clear that our competence is limited to safeguarding the data protection rights of Norwegian data subjects and to ensuring compliance with the GDPR with respect to Norway. Therefore, it is without prejudice to the competence of supervisory authorities in other countries. Further, Datatilsynet is not bound by any decisions that other European supervisory authorities may take regarding the personal data breach notifications that Argon submitted to such authorities. Therefore, for the purposes of the present case, it is immaterial that the UK Information Commissioner's Office ("ICO") decided to issue a closure letter after having received essentially the same notification that was sent to Datatilsynet,[37] or that other EU supervisory authorities have—at least thus far—decided to take no further action after having

[32] Argon's Notification, page 1 (emphasis added).
[33] Ibid.
[34] Argon's Response to Datatilsynet, para. 1.1.
[35] See Kuner et al, *The EU General Data Protection Regulation (GDPR): A Commentary* (OUP 2020), pp. 961-962.
[36] Cf. Argon's letter to Datatilsynet dated 22 February 2022.
[37] See Argon's Response to Datatilsynet, paras. 5.1-5.4.

received Argon's notification.[38] Incidentally, however, it should be noted that a closure letter is not *per se* evidence of compliance, as it is not issued further to a full investigation and may simply reflect the enforcement priorities of a given authority. Moreover, the letter that the ICO sent to Argon appears to refer only to Article 5(1)(f) UK GDPR, but does not seem to make any reference to or comments on Article 33(1) UK GDPR, which is the equivalent provision of Article 33(1) GDPR (i.e., the statutory provision at issue in the present case).[39] Similarly, none of the EU supervisory authorities that decided to take no further action after having received Argon's data breach notification has expressly stated that Argon has complied with the deadline set out in Article 33(1) GDPR.[40]

## 6. Datatilsynet's Assessment

### 6.1. Findings of an Infringement of Article 33(1) GDPR

#### 6.1.1. Introduction

As noted above in the Legal Background, Article 33 GDPR imposes personal data breach notification obligations on controllers. Under Article 33(1), a controller that experiences a personal data breach (within the meaning of Article 4(12) GDPR) must:

> *notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.*

Concerning the timeframe of the notification, Article 33(1) GDPR stipulates that the controller must notify the personal data breach:

> *without undue delay and, where feasible, not later than 72 hours after having become aware of it.*

The rationale behind such notification requirements is that, on the one hand, breach disclosure requirements enable supervisory authorities to provide guidance on whether the affected individuals should be notified of the breach and to adopt any other measures they may deem appropriate to safeguard their rights and, on the other hand, they provide additional incentives to operators to ensure adequate levels of security of their information systems.[41]

The European Data Protection Board ("EDPB") has emphasized this by stating that:

> […] *breach notification should be seen as a tool enhancing compliance in relation to the protection of personal data.* […]

[38] See Argon's letter to Datatilsynet dated 22 February 2022, para. 7.4.
[39] See Argon's Response to Datatilsynet, paras. 5.1-5.4.
[40] Cf. Argon's letter to Datatilsynet dated 22 February 2022, para. 7.4.
[41] Kuner et al, *The EU General Data Protection Regulation (GDPR): A Commentary* (OUP 2020), p. 190.

> *Notifying the supervisory authority within the first 72 hours can allow the controller to make sure that decisions about notifying or not notifying individuals are correct.*
>
> *However, the purpose of notifying the supervisory authority is not solely to obtain guidance on whether to notify the affected individuals.*[42]

In this respect, Recital 85 GDPR notes that:

> *A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority* […]

Further, Recital 87 GDPR emphasizes that:

> […] *Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation.*

In essence, as noted by the EDPB, "compliance with Articles 33(1) […] GDPR [is] central to the overall functioning of the supervision and enforcement regime" under the GDPR.[43]

Hence, the following assessment of Argon's compliance with Article 33(1) GDPR should be read and understood in light of the aforementioned key role that Article 33(1) plays within the GDPR's regulatory regime.

#### 6.1.2. Argon's Reportable Personal Data Breach

In the present case, it is uncontested that Argon experienced a personal data breach within the meaning of Article 4(12) GDPR and that such breach was reportable to Datatilsynet in accordance with Article 33(1). Indeed, Argon decided to notify Datatilsynet, as it concluded that:

> *the Incident involved (i) a qualifying personal breach, (ii) involving personal data, (iii) connected to 16 UK (and EU) individuals including 1 Norwegian individual, (iv) that*

[42] Article 29 Data Protection Working Party (WP29), Guidelines on Personal Data Breach Notification under Regulation 2016/679 (WP250rev.01, as revised and adopted on 6 February 2018) (hereinafter "Personal Data Breach Notification Guidelines"), p. 12. These guidelines have been endorsed by the EDPB. See EDPB, Endorsement 1/2018 (adopted on 25 May 2018).

[43] EDPB, Decision 01/2020 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Twitter International Company under Article 65(1)(a) GDPR (adopted on 09 November 2020) (hereinafter "EDPB Decision 01/2020"), para. 193.

*was not unlikely to result in a risk to the rights and freedoms of said individuals had occurred*.[44]

However, for the sake of completeness, Datatilsynet considers that the cyber security incident experienced by Argon between May and July 2021 falls within the definition of "personal data breach" in Article 4(12), as it consists in "a breach of security leading to the […] unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed" by Argon.[45] In fact, as mentioned above in the Factual Background, the incident concerned an unauthorized access to a spreadsheet containing personal data (e.g., salary and benefits of employees) through the mailbox account of Argon's US Senior Vice President of Human Resources, most likely through a phishing email.

As acknowledged by Argon itself,[46] the personal data breach at hand is not unlikely to result in a risk to the affected individuals' rights and freedoms. This is also because it is not unlikely that—as a result of the breach—Argon's employees could suffer significant detriment due to the disclosure of information about them, such as their salary and benefits, to unintended recipients (e.g., identity theft or fraud), a disclosure that does not necessarily require the exfiltration of the data.[47] At any rate, even if Argon claims that the measures it took after the breach significantly mitigate such risk,[48] Argon was not able to exclude this risk promptly after having become aware of the breach.

Consequently, the personal data breach at hand was reportable for the purposes of Article 33(1).

This is further supported by the EDPB's Guidelines on Examples regarding Data Breach Notification, which describe as reportable—both to the competent supervisory authority and to the affected data subjects—an incident in which an attacker gained access to information on the salary of several employees of a company by exfiltrating emails from that company's mailbox accounts.[49] The latter scenario is not identical but is highly comparable to the present case. The main difference is that in the present case employees' personal data were accessed—but do not appear to be exfiltrated—by the unauthorized third party. This difference is, however, irrelevant for present purposes, as the definition of "personal data breach" in Article 4(12) GDPR also covers "unauthorised […] access to, personal data". Instead, the example provided in the Guidelines presents numerous significant similarities to the present case: in both cases, the attacker altered the rules within the mailbox account of a company; the attacker was probably

[44] Argon's Response to Datatilsynet, para. 3.2(e). See also Argon's letter to Datatilsynet dated 22 February 2022, para. 4.13.
[45] Cf. Art. 4(12) GDPR.
[46] Argon's Response to Datatilsynet, para. 3.2(e) (stating that Argon concluded in September 2021 that the breach "was not unlikely to result in a risk to the rights and freedoms of said individuals had occurred").
[47] Contrary to what Argon seems to suggest. See Argon's letter to Datatilsynet dated 22 February 2022, p. 14-15.
[48] Ibid.
[49] EDPB, Guidelines 01/2021 on Examples regarding Data Breach Notification of the European Data Protection Board (Adopted on 14 December 2021, Version 2.0) (hereinafter "EDPB Guidelines on Examples regarding Data Breach Notification"), page 32. It should be noted that a first version of these guidelines was adopted and published in January 2021(hence, before the Argon's personal data breach), and that such first version of the guidelines included the same example cited above. See EDPB, Guidelines 01/2021 on Examples regarding Data Breach Notification, Adopted on 14 January 2021, Version 1.0, page 31.

not aiming at collecting personal data, but created a forged invoice, by way of social engineering, in order to facilitate a misdirected payment; the attacker gained access to employees' personal data, such as name and salary.[50]

### 6.1.3. Moment at Which Argon Became Aware of the Personal Data Breach

Under Article 33(1) GDPR, a controller must report a personal data breach "without undue delay and, where feasible, not later than 72 hours after having become aware of it" (emphasis added).

Thus, to assess whether a controller has complied with its reporting obligations under Article 33(1), it must first be assessed whether and when the controller has "become aware" of a "personal data breach", as this is the moment when the statutory 72 hours deadline starts to run.

Contrary to what Argon seems to suggest,[51] the timeframe for notification under Article 33(1) commences from when the controller "become[s] aware" that a "personal data personal breach" has taken place, and not from when the controller has a reasonable certainty that the breach is *not unlikely to result in a risk to the rights and freedoms of natural persons*. In other words, the deadline starts to run when the controller becomes aware of a "personal data breach", and not when the controller becomes aware that the personal data breach in question is *notifiable* in accordance with Article 33(1) GDPR. As noted by the EDPB, the likely risks for individuals should be determined during the 72 hours *after* the controller has "became aware" of the personal data breach:

> *Once the controller has become aware, a notifiable breach must be notified without undue delay, and where feasible, not later than 72 hours. During this period, the controller should assess the likely risk to individuals in order to determine whether the requirement for notification has been triggered, as well as the action(s) needed to address the breach.*[52] (emphasis added)

This clearly emerges also from the wording of Article 33(1): "not later than 72 hours after having become aware of it" (emphasis added), "it" being the "personal data breach" mentioned in the opening sentence of Article 33(1) and defined in Article 4(12) GDPR.

In essence, the statutory 72 hours deadline starts to run when the controller has a reasonable degree of certainty that an incident falling within the definition of "personal data breach" in

---

[50] Ibid. Cf. Argon's Notification, pp. 2 and 3.

[51] See Argon's Response to Datatilsynet, para. 3.2(e) (stating: "This investigative process and outcomes based response strategy concluded on 21 September 2021, allowing Argon to conclude, in light of forensic findings and legal analyses, that the Incident involved (i) a qualifying personal breach, (ii) involving personal data, (iii) connected to 16 UK (and EU) individuals including 1 Norwegian individual, (iv) that was not unlikely to result in a risk to the rights and freedoms of said individuals had occurred. Prior to this date, Argon did not consider that it did not possess the requisite degree of reasonable certainty in relation to the Incident" (emphasis added)). See also Argon's letter to Datatilsynet dated 22 February 2022 (stating: "Argon remains of the view that it only became fixed with knowledge that the Incident affected UK/EU individuals that were subject to the GDPR satisfying the threshold for notification under Article 33 on 21 September 2021"(emphasis added)).

[52] Personal Data Breach Notification Guidelines, p. 11.

Article 4(12) GDPR has taken place. This knowledge materializes when the controller becomes aware of the existence of a breach that meets *all of the constituent elements* of the definition in Article 4(12) GDPR.[53] In other words, the 72 hours deadline starts to run when the controller becomes aware that:

- A "breach of security" has taken place;
- Such a breach of security has led to the "unauthorised disclosure of, or access to" data transmitted, stored or otherwise processed (or one of the other kinds of security breaches mentioned in Article 4(12)); and
- Such a breach of security has affected "personal data".

This is further supported by the EDPB's Guidelines on Personal Data Breach Notification, which state that:

> *a controller should be regarded as having become 'aware' when that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised*.[54] (emphasis added)

Argon became aware of all of these elements at least on 19 July 2021. This is because, according to the notification it submitted to Datatilsynet on 24 September 2021:

- "On 14 June 2021 […] Argon determined it had been subject to a business email compromise, perpetrated through its [redacted] platform by an unauthorised third party" (emphasis added).[55] Thus, on 14 June 2021, Argon had specific knowledge that a "breach of security" had taken place, even though at the time it did not know the exact implications of that breach.
- "further investigation […] completed by Argon and its cyber forensic expert on 19 July 2021, revealed that two files within the [redacted] connected to the Mailbox Account (the 'Share Files') were accessed by the Threat Actor" (emphasis added).[56] Therefore, on 19 July 2021, Argon had specific knowledge that the identified security incident had led to the "unauthorised disclosure of, or access to" data transmitted, stored or otherwise processed by the company. This qualifies the breach as a "confidentiality breach".[57]
- On the same date (i.e., on 19 July 2021), Argon became aware that the above "Share Files included (i) a spreadsheet containing the salary and benefits personal data of all

[53] To be covered by the Article 4(12) definition, a breach must have three key attributes: (1) it must concern a violation of "security measures" (2) leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, data (3) which qualify as "personal data". See Kuner et al, *The EU General Data Protection Regulation (GDPR): A Comme*ntary (OUP 2020), p. 191.
[54] Personal Data Breach Notification Guidelines, pp. 10-11.
[55] Argon's Notification, para. 1.1.
[56] Ibid., para. 1.4.
[57] Personal Data Breach Notification Guidelines, p. 7.

> 20 of Argon's European employees" (emphasis added).[58] Thus, on 19 July 2021, Argon had specific knowledge that the breach had affected "personal data" of individuals in Europe, including in Norway. Indeed, Argon expressly stated in its personal data breach notification that Argon "became fixed with knowledge of the Share File relating to the personal data of the l6 EU/UK employees (and additional 4 Swiss employees) on 19 July 2021".[59]

In light of the above, the deadline for Argon's notification to Datatilsynet under Article 33(1) GDPR started to run at least from 19 July 2021.

It bears emphasizing that the issue of controller "awareness", and its role in terms of defining the timeframe within which notification is required to take place, must be understood in the context of the broader obligation on a controller to ensure that it has appropriate measures in place to facilitate such "awareness". This requirement is reflected in Recital 87 GDPR, which states that:

> *It should be ascertained whether all appropriate technical and organizational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject* […] (emphasis added)

This is underlined also in the EDPB's Guidelines on Personal Data Breach Notification, which state that:

> *the GDPR requires the controller to implement all appropriate technical protection and organisational measures to establish immediately whether a breach has taken place and to inform promptly the supervisory authority and the data subjects. It also states that the fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the breach and its consequences and adverse effects for the data subject. This puts an obligation on the controller to ensure that they will be 'aware' of any breaches in a timely manner so that they can take appropriate action*.[60] (emphasis added)

The Guidelines further state that:

> *After first being informed of a potential breach* […] *or when it has itself detected a security incident, the controller may undertake a short period of investigation in order to establish whether or not a breach has in fact occurred. During this period of investigation the controller may not be regarded as being "aware". However, it is expected that the initial investigation should begin as soon as possible and establish with a reasonable degree of certainty whether a breach has taken place; a more detailed investigation can then follow*.[61] (emphasis added)

---

[58] Argon's Notification, para. 1.4.
[59] Ibid., para. 1.7.
[60] Personal Data Breach Notification Guidelines, p. 11.
[61] Ibid.

The EDPB placed particular emphasis on the fact that the initial investigation must be "short" in its Decision 01/2020 where it stated:

> *the GDPR puts an obligation on the controller to ensure that they will be "aware" of any breaches in a timely manner so that they can take appropriate action" and explain that "the controller may undertake a short period of investigation in order to establish whether or not a breach has in fact occurred. During this period of investigation the controller may not be regarded as being "aware"".*[62] (emphasis in the original)

Having regard to the above, it is clear that the controller's notification obligation in Article 33(1) GDPR must be understood within the context of its broader obligations under the GDPR, and specifically, the controller's overarching responsibility to ensure that there is compliance with the principles of data protection, as encompassed in the accountability obligation under Article 5(2) GDPR.

In this respect, it should be underlined that it took Argon over a month to "become aware" (within the meaning of Article 33(1) GDPR) of the personal data breach at issue. This is because it took the company over a month—i.e., from 14 June 2021 to 19 July 2021—to determine whether personal data had been affected by the security incident at issue. This may not be regarded as a "short period of investigation", and is indicative of the fact that Argon did not have or followed appropriate technical and organizational measures to *establish immediately* whether a personal data breach had taken place, as required by the GDPR.

A fortiori, even if one would accept Argon's arguments regarding its awareness of the reportable breach on 21 September 2021, the period of investigation of *over three months*, between 14 June and 21 September 2021, may not be regarded as a "short period of investigation" that the EDPB Guidelines consider to be physiological, and during which the controller may not be regarded as being "aware".[63]

In short, Argon ought to have been "aware" of the personal data breach at hand even before 19 July 2021, which worsens the nature and seriousness of any subsequent delays. This is not to say that the measures that Argon took to contain the incident and to limit its impact are to be criticized; the only matter that the present decision addresses and that is reproached to Argon in this case is its lack of sufficient responsiveness to ensure its prompt compliance with its notification obligations under the GDPR.

In its written representations, Argon insisted that in July 2021 it was not "aware" of the personal data breach at issue, due to the fact that at that time its internal findings were still being verified by its external forensic and legal advisors and a full organizational and legal review of the incident was still ongoing.[64] According to Argon, it only become "aware" of the personal data breach on 21 September 2021, upon receipt of a legal advice on the relevant incident from its

[62] EDPB Decision 01/2020, para. 190.
[63] Personal Data Breach Notification Guidelines, p. 11.
[64] See Argon's letter to Datatilsynet dated 22 February 2022, pp. 7-12.

external legal advisers.[65] This argument should be rejected. As noted above, for a controller to be considered "aware" of a personal data breach under Article 33(1) GDPR, it is sufficient that the controller has a reasonable degree of certainty that a security incident has occurred and that the latter has led to personal data being compromised; the controller neither needs to be aware of the full extent or consequences of the incident nor of its legal implications. In this regard it is worth noting that ignorance of the applicable notification duties is no excuse.[66] Thus, Argon's argument that in July 2021 "it was not aware of the context of the document and the applicability of the GDPR to the particular processing activities engaged by the Incident"[67] should be rejected too. Indeed, it is part of the controller's accountability obligations to know whether a processing is covered by the GDPR, also in light of the requirements set out in Article 30 GDPR. GDPR applicability is not something to be explored only after the occurrence of a data breach. To determine whether and when Argon became aware of the personal data breach at issue in the present case, it is sufficient to determine whether and when the company become aware of all of the factual elements listed in the definition of "personal data breach" in Article 4(12) GDPR. Whether at the time the company was aware of these factual elements the company was *also* aware of its legal obligations under the GDPR, as well as of the possible risks that may result from the incident, is irrelevant to determine whether the company was "aware" of the personal data breach within the meaning of Article 33(1) GDPR.

As explained above, Argon's data breach notification to Datatilsynet states that an investigation "completed by Argon and its cyber forensic expert on l9 July 2021, revealed that two files […] (the 'Share Files') were accessed by the Threat Actor" and that Argon "became fixed with knowledge of the Share File relating to the personal data of the l6 EU/UK employees (and additional 4 Swiss employees) on 19 July 2021".[68] This is sufficient to conclude that Argon was "aware" of the personal data breach at least on 19 July 2021; the fact that at that time the company had yet to receive a legal advice on the incident and its obligations under the GDPR from its external legal advisers is irrelevant to determine whether Argon could be regarded as being "aware" of the breach at that time. In this respect, it should be restated that the statutory deadline for reporting a breach is triggered under Article 33(1) when a controller "becomes aware" of a *personal data breach*, and not when the controller concludes—after a legal and risk assessment—that the breach at hand is *notifiable* under the GDPR. The 72 hours timeframe set out in Article 33(1) is specifically envisaged to allow the controller to make such an assessment. Consequently, Argon's following argument should be rejected:

> [in July 2021] *Argon did not have the requisite awareness of a personal data breach as it did not have a reasonable degree of certainty that "Argon's employees could suffer significant detriment due to the disclosure of information about them, such as their salary and benefits, to unintended recipients (e.g., identity theft or fraud)".*[69]

---

[65] Ibid., paras. 5.1 and 5.3.

[66] The fact that a controller failed to submit a personal data breach notification in a timely manner under the GDPR gives rise per se to an infringement of Article 33(1) GDPR, whether or not the controller was aware of the obligation imposed by that provision or that the GDPR applied to its processing activities (*ignorantia legis non excusat*). See by analogy Opinion of Advocate General Tizzano in Case C-551/03 P, *General Motors BV (formerly General Motors Nederland BV) and Opel Nederland BV v Commission of the European Communities*, para. 77.

[67] Argon's letter to Datatilsynet dated 22 February 2022, p. 9.

[68] Argon's Notification, paras. 1.4. and 1.7 (emphasis added).

[69] Argon's letter to Datatilsynet dated 22 February 2022, pp. 14-15.

For completeness purposes, it should be noted that the interpretation of Article 33(1) GDPR that Argon seems to embrace—according to which the deadline for a notification under Article 33(1) would be triggered only once the controller has had time to *fully* investigate the nature and extent of a security incident—is at odds with the objectives of Article 33(1)—as outlined above (see section 6.1.1)—and negates the very purpose of data breach notifications. This is because the interpretation proposed by Argon would transform such notifications into a mere formal exercise and would render them essentially meaningless. Indeed, this interpretation would basically leave the controller free to decide the timeframe for investigating and reporting the breach. In practice, if one would follow this approach, the timeframe for reporting (and potentially even the obligation to report at all) would depend on whether the controller decides to undertake a full investigation and on the pace with which such investigation is conducted. Moreover, a notification received by a supervisory authority several months after an incident was first detected would hinder any timely and meaningful intervention from its part to safeguard the rights of data subjects.

#### 6.1.4. Argon's Late Notification to Datatilsynet

Having established that Argon became aware of the personal data breach at least on 19 July 2021, it must be determined whether Argon's notification has taken place within the timeframe set out in Article 33(1), which requires that a notification be submitted "without undue delay and, where feasible, not later than 72 hours after having become aware of it".

In the context of Datatilsynet's inquiry, Argon expressed the following views on its alleged compliance with the timeframe set out in Article 33(1):

> […] *In light of the role of the SVP of HR, Argon was focused on ensuring its investigation was full and accurate in order to identify all personal data connected to EU and UK individuals that may have been in scope for the Incident. As such Argon worked with its third-party cyber forensic expert to investigate the Incident and establish the extent to which any personal data was involved. This investigation also involved undertaking additional technical analysis and internal risk identification to ensure that all possibilities were explored by both Argon and its third-party cyber forensic expert, to ensure a methodical and full risk assessment process was completed. This investigation was completed on 21 September 2021.*
>
> *While Argon's investigation was able to confirm that the Share Files (containing EU and UK employee personal data) were accessed, it was unable to confirm the extent to which the broader emails within the Mailbox Account were, in fact, accessed. Therefore, out of an abundance of caution, Argon conducted an organisational and legal review of the Mailbox Account to understand the full scope of the personal data involved so that regulators and individuals were notified fully of their involvement in the Incident, as required. Once this was completed, Argon worked with legal counsel and its cyber forensic experts to properly understand the nature of the impact to the subset of personal data so Argon could determine the appropriate next steps and enable full and accurate notifications to be prepared and effected. This necessarily took some time.*

> *The processes* […] *involved multiple rounds of interviews, discussions and collaborative sessions at each stage to determine the personal data categories in scope, the context in which the US SVP of HR was processing the personal data (including whether this was in fact connected to the EU/UK establishments) and the likely degree of sensitivity attaching to each category. This diligent and comprehensive process was designed to ensure Argon could answer all queries from regulators and employees following notification and, in particular, so as not to cause undue concern to the individuals impacted by the Incident.*
>
> *This investigative process and outcomes based response strategy concluded on 21 September 2021, allowing Argon to conclude, in light of forensic findings and legal analyses, that the Incident involved (i) a qualifying personal breach, (ii) involving personal data, (iii) connected to 16 UK (and EU) individuals including 1 Norwegian individual, (iv) that was not unlikely to result in a risk to the rights and freedoms of said individuals had occurred. Prior to this date, Argon did not consider that it did not possess the requisite degree of reasonable certainty in relation to the Incident.*
>
> *Therefore, Argon acted proportionately and without undue delay, to notify the supervisory authorities within 72 hours of this confirmation, by 24 September 2021, pursuant to Article 33 of the GDPR.*[70]

While it is appropriate for controllers to conduct an extensive investigation after any data breach, the notification requirement in Article 33(1) is intended to ensure that supervisory authorities are informed of the breach *shortly after* an initial assessment of the breach, and not after a very lengthy and extensive investigation, like the one conducted by Argon.

Recital 85 GDPR expresses this in the following terms:

> *as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority* […] (emphasis added)

Recital 87 GDPR further emphasizes this, as it states that controllers are required:

> *to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory.* (emphasis added)

In this respect, the EDPB not only stressed that:

> *After first being informed of a potential breach* […] *or when it has itself detected a security incident, the controller may undertake a short period of investigation in order*

[70] Argon's Response to Datatilsynet, para. 3.2.

> *to establish whether or not a breach has in fact occurred.* […] *a more detailed investigation can then follow*.[71] (emphasis added)

It also opined that:

> *The breach should be notified when the controller is of the opinion that it is likely to result in a risk to the rights and freedoms of the data subject. Controllers should make this assessment at the time they become aware of the breach. The controller should not wait for a detailed forensic examination and (early) mitigation steps before assessing whether or not the data breach is likely to result in a risk and thus should be notified.*
>
> […]
>
> *Gathering exact information on the unauthorized access is key for determining the risk level and preventing a new or continued attack.* […] *When uncertain about the specifics of the illegitimate access, the worse scenario should be considered and the risk should be assessed accordingly*.[72] (emphasis added)

In essence, as noted by the EDPB:

> *It should* […] *be clear that after making an initial notification, a controller could update the supervisory authority if a follow-up investigation uncovers evidence that the security incident was contained and no breach actually occurred*.[73]

This is expressly envisaged by Article 33(4) GDPR, which provides that:

> *Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.*

The wording and normative structure of Article 33 itself indicate that as a *general rule* a controller must notify *all* personal data breaches it becomes aware of "without undue delay" and "not later than 72 hours". However, the second part of the Article introduces an exception to this general rule ("*unless* the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons"). Thus, if the controller is unable to confirm within the 72 hours timeframe that such an exception applies (and hence that a notification is not necessary), it must proceed with the notification, without prejudice to the possibility of submitting a follow-up notification to inform the authority—after a more thorough analysis—that no risks for data subjects have been identified or no personal data breach actually occurred. In the words of the EDPB:

---

[71] Personal Data Breach Notification Guidelines, p. 11.

[72] EDPB Guidelines on Examples regarding Data Breach Notification, paras. 9 and 30. The same statements were also included in the version of the guidelines adopted and published in January 2021 (i.e., before Argon's breach). See Guidelines 01/2021 on Examples regarding Data Breach Notification, Adopted on 14 January 2021, Version 1.0, paras. 9 and 30.

[73] Personal Data Breach Notification Guidelines, p. 16.

> *Once the controller has become aware, a notifiable breach must be notified without undue delay, and where feasible, not later than 72 hours. During this period, the controller should assess the likely risk to individuals in order to determine whether the requirement for notification has been triggered.*
>
> […]
>
> *after making an initial notification, a controller could update the supervisory authority if a follow-up investigation uncovers evidence that the security incident was contained and no breach actually occurred*.[74]

In light of the above, given that on 19 July 2021 Argon had sufficient elements to conclude, with a reasonable degree of certainty, that a personal data breach (within the meaning of Article 4(12)) had taken place, Argon could and should have submitted an initial notification "without undue delay" from that date. Such an initial notification would have been without prejudice to the possibility of submitting a follow-up notification at a later stage (potentially and theoretically even to inform Datatilsynet that, after a further extensive investigation, Argon determined that no personal data had been affected by the breach). In this respect, it should be noted that—as Argon rightly pointed out[75]—the EDPB recommends that controllers try to identify "the root cause of the issue".[76] However, it also stresses that "the notification does not need to be postponed until the risk and impact surrounding the breach has been fully assessed, since the full risk assessment can happen in parallel to notification, and the information thus gained may be provided to the SA in phases without undue further delay".[77]

It should also be stressed that—given that the GDPR envisages and allows notification in phases—a controller does not need to provide "full … notifications"[78] and be able to "answer all queries from regulators"[79] immediately after having detected a breach. In other words, contrary to what Argon suggests, the obligation to notify a personal data breach under the GDPR is not triggered only after the controller has had time to "to fully investigate the Incident and apply the applicable GDPR risk analysis [to determine] that a personal data breach was reportable in all the circumstances".[80] Moreover, as noted above, one of the purposes of the notification process is specifically to enable supervisory authorities to advise controllers on whether and how to communicate with the individuals affected by the breach. Thus, the key considerations that appear to have led Argon to delay the notification were misplaced. As noted above, Argon stated that the extensive process it designed and implemented after the breach:

---

[74] Personal Data Breach Notification Guidelines, pp. 11 and 16.
[75] See Argon's letter to Datatilsynet dated 22 February 2022, pp. 16-17.
[76] EDPB Guidelines on Examples regarding Data Breach Notification, para. 8.
[77] Ibid.
[78] Cf. Argon's Response to Datatilsynet, para. 3.2(c).
[79] Ibid. cf. para. 3.2(d).
[80] See Argon's letter to Datatilsynet dated 22 February 2022, p. 12.

> *was designed to ensure Argon could answer all queries from regulators and employees following notification and, in particular, so as not to cause undue concern to the individuals impacted by the lncident.*[81]

As mentioned above, the standard statutory timeframe for notification under Article 33(1) is "where feasible, not later than 72 hours" after becoming aware of the personal data breach. Datatilsynet sees no practical reasons or evidence why a notification within 72 hours was not "feasible" in the present case, as confirmed by the fact that Argon notified the local FBI Cybercrime Unit in the US already on 15 June 2021—only one day after it first detected the incident—even though we understand that such a notification is voluntary under U.S. law. Moreover, Argon's notification to Datatilsynet was not accompanied by reasons for the delay as Article 33(1) requires for notifications that are submitted after the 72 hours deadline.

Consequently, Argon's notification should have taken place "not later than 72 hours" after 19 July 2021. Hence, it should have taken place not later than Thursday 22 July 2021,[82] in particular as Argon could not confirm within that date that the breach was unlikely to result in a risk to the rights and freedoms of natural persons. Instead, Argon notified Datatilsynet on 24 September 2021, over two months outside the 72 hours timeframe set out in Article 33(1).

For completeness purposes, it should be noted that, in the present case, notifying more than two months after becoming aware of the personal data breach would be an undue delay also in light of the features of the breach experienced by Argon. In this regard, Recital 87 states that:

> *The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject.*

The personal data breach at hand affected personal data that could be used to commit actions leading to both material (e.g. financial loss) and non-material damage (e.g. identity theft or fraud), or could be used to facilitate other attacks (e.g. phishing).[83] Thus, potentially, it could have serious consequences and adverse effects for data subjects, although no such effects appear to have materialized to date. In any event, the assessment of the timeliness of the notification should be made taking into account the information that was available to the controller at the time when it became aware of the personal data breach, and in the course of the initial investigation that took place in the first few days after the controller became aware of the breach. Therefore, Argon's argument that it did not violate Article 33(1) because in hindsight and to date "the timing of its Initial Notification has not led to any detriment to the data subjects"[84] should be rejected. However, this element should be taken into account when deciding whether to impose an administrative fine and when deciding on the amount of the administrative fine for Argon's violation of Article 33(1) (see section 7.1.1 below).

---

[81] Argon's Response to Datatilsynet, para. 3.2(d).
[82] See Regulation of the Council of 3 June 1971 determining the rules applicable to periods, dates and time limits OJ [1971] L 124/1.
[83] See by analogy EDPB Guidelines on Examples regarding Data Breach Notification, page 32.
[84] See Argon's letter to Datatilsynet dated 22 February 2022, p. 12.

Argon's argument that it did not violate Article 33(1) GDPR because "Datatilsynet's ability to provide guidance and protect the interests of data subjects has not been impaired through the actions of Argon in submitting its Initial Notification"[85] should be rejected as well. First, as Datatilsynet was not promptly informed of the breach upon its discovery (contrary to the FBI in the US), it was objectively impossible for Datatilsynet to provide any guidance in the first critical days after the breach. Secondly, whether Datatilsynet took any measures—or could have taken any measure—in relation to the breach after it received Argon's notification is immaterial to the assessment of whether Argon submitted the notification "without undue delay".

A 64-day delay is a very considerable delay, which is hardly justifiable under any circumstances. It is especially unjustifiable in the circumstances of the present case where the controller did not notify the breach promptly, despite the fact that it was aware—at least as of 19 July 2021—that the attacker had "accessed"[86] personal data "subject to a greater degree of sensitivity"[87] such as salary and benefits personal data, and that at that point Argon was unable to confirm the extent to which the broader emails within the affected mailbox account had in fact been accessed. Thus, at that point in time, the worse scenario should have been considered and the risks should have be assessed accordingly,[88] including in terms of notification measures.

Argon's delay is further aggravated by the fact that it took the company over one month to confirm that personal data had been affected by the breach. As a consequence, over three months have elapsed from the time the security incident was first detected by Argon in June 2021 to the moment when Argon submitted its notification to Datatilsynet in September 2021.

Having regard to the above, Datatilsynet has concluded that Argon notified the personal data breach with a very considerable and unjustified delay, and thus failed to notify the personal data breach to Datatilsynet "without undue delay", as stipulated by Article 33(1) GDPR.

Significantly, such a long delay is also indicative of the fact that, at the time of the incident, Argon had not implemented or followed adequate technical and organizational measures to establish immediately whether a personal data breach had taken place and to inform promptly the competent supervisory authorities, as required by the GDPR (see further section 7.1.4. below). This is not to say that Argon had no cybersecurity measures in place; the present decision and case focus exclusively on the lack of measures to ensure that personal data breaches (within the meaning of Article 4(12) GDPR) are promptly identified and notified in accordance with the GDPR.

In its written representations, Argon argued that Datatilsynet failed to assess Argon's notification "against the WP250 Guidelines, in conjunction with the Notification Guidelines [i.e., EDPB Guidelines 01/2021]",[89] and that "[t]he interpretation of Article 33(1) of the GDPR, as applied by Datatilsynet […] was not foreseen by Argon with reference to the available

[85] Ibid.
[86] Argon's Notification, para. 1.4.
[87] Argon's Notification, para. 2.6.
[88] EDPB Guidelines on Examples regarding Data Breach Notification, para. 30.
[89] Argon's letter to Datatilsynet dated 22 February 2022, pp. 17-19.

guidance, and seems country specific for Norway".[90] We take note of these arguments, but find them untenable. Throughout the present decision, Datatilsynet has made extensive reference to EDPB and WP29 guidance. Therefore, Datatilsynet's interpretation of Article 33(1) reflects the interpretation of that provision at European level, and is not specific for Norway. In this respect, it should be recalled once again that it was the EDPB that stated in its guidance that "[o]nce the controller has become aware, a notifiable breach must be notified without undue delay, and where feasible, not later than 72 hours. During this period, the controller should assess the likely risk to individuals in order to determine whether the requirement for notification has been triggered. […] after making an initial notification, a controller could update the supervisory authority if a follow-up investigation uncovers evidence that the security incident was contained and no breach actually occurred."[91]

Thus, Argon's view that, until it received external legal advice in September 2021, it was not required to notify the breach to Datatilsynet as it was not "aware of with a reasonable degree of certainty that the Incident was reportable based on the available guidance" is clearly at odds with EDPB guidance. To the avoidance of doubts, it should be re-emphasized that the relevant EDPB guidelines state that "a controller should be regarded as having become "aware" when that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised"[92], and not—as Argon would seem to suggest—when the controller has concluded that the level of risk makes the breach reportable under Article 33(1) GDPR. The EDPB has made clear that it is within the 72 hours after such an awareness that "the controller should assess the likely risk to individuals in order to determine whether the requirement for notification has been triggered".[93] If after this short timeframe, the controller is still "uncertain about the specifics of the illegitimate access, the worse scenario should be considered and the risk should be assessed accordingly",[94] hence in these circumstances an initial notification must be promptly submitted to the competent supervisory authority, without prejudice to the possibility of updating "the supervisory authority if a follow-up investigation uncovers evidence that the security incident was contained and no breach actually occurred."[95] In short, Datatilsynet's interpretation of Article 33(1) GDPR is fully in line with the position on the notifications requirements under the GDPR that the EDPB/WP29 expressed in guidance documents published before Argon's security incident.

[90] Ibid., p. 24.
[91] Personal Data Breach Notification Guidelines, pp. 11 and 16.
[92] Ibid, pp. 10-11.
[93] Ibid., p. 11.
[94] EDPB Guidelines on Examples regarding Data Breach Notification, para. 30. The same statements was also included in the version of the guidelines adopted and published in January 2021 (i.e., before Argon's breach). See Guidelines 01/2021 on Examples regarding Data Breach Notification, Adopted on 14 January 2021, Version 1.0, para. 30.
[95] Personal Data Breach Notification Guidelines, p. 16.

## 7. Administrative Fine

### 7.1. Consideration of the Criteria in Article 83(2) in Deciding Whether to Impose an Administrative Fine and the Amount of the Fine

Under Article 58(2) GDPR, Datatilsynet has several corrective powers, including the power to impose administrative fines for violations of the GDPR.

When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine, due regard must be given to the factors listed in Article 83(2)(a) to (k) GDPR. The following sub-sections outline how Datatilsynet has given "due regard" to these factors in the present case.

#### 7.1.1. Nature, Duration and Gravity of the Infringement (Art. 83(2)(a))

With respect to the nature of Argon's infringement, it should be noted that the infringement at hand concerns a requirement that is "central to the overall functioning of the supervision and enforcement regime" under the GDPR.[96] Therefore, we consider that, overall, the infringement may be deemed to be moderately serious in nature in the present circumstances.

In respect of the duration of the infringement, the latter has had a considerable duration, as the infringement consists in having notified Datatilsynet 64 days outside the 72 hours timeframe set out in Article 33(1) GDPR, which is no trivial delay. Such a prolonged delay is also one of the key elements to take into consideration in the analysis of the gravity of the infringement.

The gravity of the infringement should be assessed bearing in mind that the infringement in question does not relate to the substantive matter or the causes of the personal data breach itself; it only concerns a key procedural safeguard (*i.e*., the notification) that should be deployed in case of a personal data breach. Nonetheless, the infringement should be seen against the backdrop of the relevant personal data breach and underlying processing carried out by Argon.

Insofar as the breach suffered by Argon is concerned, the level of *potential* impact for the affected individuals is significant. Even though the attacker was probably not specifically aiming at collecting personal data, the attack was likely financially motivated (as it led to a fraudulent payment),[97] and the data accessed by the attacker could be used to commit actions leading to both material (e.g., financial loss) and non-material damage (e.g., identity theft or fraud), or could be used to facilitate other attacks (e.g., phishing).[98] However, whilst it cannot be ruled out that no data subjects will eventually be damaged as a result of the breach or delayed notification, equally, there is currently no direct evidence of damage to them from the breach itself or delayed notification,[99] and Argon has taken several mitigating measures to limit the risks that damages to data subjects will materialize in the future as a result of the breach (see further section 7.1.3 below).

[96] EDPB Decision 01/2020, para. 193.
[97] Argon's Notification, para. 1.5.
[98] See by analogy EDPB Guidelines on Examples regarding Data Breach Notification, page 32.
[99] Argon's Notification, para. 3.4.

In respect of the number of affected data subjects, the personal data breach affected a small cohort of people, as all in all it affected 20 individuals in Europe, and only one individual in Norway.[100] The same number of individuals was equally affected by the delayed notification.

While the last two elements attenuate to a certain extent the gravity of the infringement, a central element of the analysis of the gravity of the infringement should be whether the nature and scope of the infringement are indicative of broader compliance issues. In this regard, Datatilsynet considers that a multinational company operating in the healthcare sector, like Argon, should have sufficient procedures and routines in place to enable the company to comply with the duty of notification under Article 33(1) GDPR. A delay of the magnitude mentioned above, which was not due to an occasional oversight—as Argon claims that its internal "guidelines were followed to the best of Argon's ability in relation to this Incident"[101]—is indicative of a failure to put in place adequate procedures and routines to ensure compliance with the notification requirements under the GDPR, which is a significant compliance issue that enhances the gravity of the infringement (see further section 7.1.4. below). In this regard, it should be emphasized once again that what is reproached to Argon in this case is only the lack of adequate procedures and routines to ensure a timely notification of a personal data breach under the GDPR, and not the failure to put in place other kinds of cybersecurity measures.

Having considered the above, and taking into account all of the aforementioned aggravating and mitigating elements in their complexity, Datatilsynet considers the infringement to be moderately grave. This factor should be weighed accordingly in the present case.

In its written representations, Argon argued that greater regard should be had under the criterion at Article 83(2)(a) to "the number of data subjects affected and the level of damaged suffered by them".[102] Argon also claimed that only if adverse effects "do materialize […] should corrective responses or sanctions be employed by the supervisory authority".[103] We take note of these arguments. However, we note that both of the factors that Argon pointed to were taken into account by Datatilsynet, and that this was done to a sufficient extent. Indeed, the fine imposed by Datatilsynet in the present case is only 2.5 % of the maximum applicable fine also in light of these factors (see section 7.3 below). Moreover, we note that the damage suffered by data subjects is only one of the factors to be assessed when deciding whether to impose an administrative fine under Article 83 GDPR. Thus, it is not the case that the mere fact that a violation of the GDPR has not resulted in a material or non-material damage for data subjects entails in itself that no administrative fine may be issued. In this respect, it should be noted that fines for violations of Article 33(1) GDPR have been issued even in cases scrutinized by the EDPB where "there was no direct evidence of damage to [data subjects] arising from the delayed notification".[104]

---

[100] Ibid., paras. 1.4, 2.4 and 2.5.
[101] Argon's Response to Datatilsynet, para. 4.1.
[102] See Argon's letter to Datatilsynet dated 22 February 2022, p. 22.
[103] Ibid., p. 20.
[104] EDPB, Decision 01/2020 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Twitter International Company under Article 65(1)(a) GDPR, Adopted on 09 November 2020, paras. 150 and 186.

#### 7.1.2. Intentional or Negligent Character of the Infringement (Art. 83(2)(b))

In respect of the criterion at Article 83(2)(b), the EDPB found that:

> *In general, "intent" includes both knowledge and wilfulness in relation to the characteristics of an offence, whereas "unintentional" means that there was no intention to cause the infringement although the controller/processor breached the duty of care which is required in the law.*[105]

Further to our inquiry, we see no evidence of an intentional infringement on Argon's part. However, in our view, the infringement arose due to negligence on the part of Argon, insofar as the company failed to implement and follow appropriate technical and organizational measures to establish immediately whether a personal data breach has taken place and to inform promptly the competent supervisory authorities, thus disregarding its duty of care (see section 7.1.4. below).

It bears emphasizing that—since June 2021—several of the top executives of Argon, including its US Senior Vice President of Human Resources and Director of Global IT Security,[106] have been involved in the management of the breach. Therefore, it may be concluded that the company's failure to notify the breach on time may also be attributed to the fact that these executives acted negligently in connection with the breach, as they disregarded their duty of care to ensuring compliance with a legal obligation under the GDPR.[107]

Overall, this factor should be weighed moderately against Argon in the present case.

In its written representations, Argon argued that neither the company nor its top executives acted negligently.[108] In this respect, Argon noted that it "does not consider that taking the time to comprehensively investigate and assess the nature and scope of the Incident, before concluding that Article 33 and 34 GDPR notifications were required, automatically constitutes negligence on the part of Argon as a business or with respect to the top executives. Argon's management promptly sought advice from US and UK/EU counsel as the investigation developed, and did not disregard their duty at any time".[109] Moreover, Argon argued that "negligence must be proved with clear preponderance of probability".[110] Datatilsynet takes note of these arguments, but we maintain our view that the infringement arose due to negligence on the part of Argon. This is because Article 33(1) GDPR imposed a duty on Argon—and as a result on its top executives too—to ensure that the personal data breach at issue in the present

---

[105] WP29, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP 253, Adopted on 3 October 2017) (hereinafter "Guidelines on Administrative Fines", p. 12. These guidelines have been endorsed by the EDPB. See EDPB, Endorsement 1/2018 (adopted on 25 May 2018).
[106] See Argon's Notification, paras. 1.1-1.2.
[107] See Section 46 of the Public Administration Act ('forvaltningsloven'). It should be noted that, under the Public Administration Act, the negligence requirement can be met by both anonymous and cumulative errors. See Prop. 81 L (2021–2022).
[108] See Argon's letter to Datatilsynet dated 22 February 2022, pp. 23-25.
[109] Ibid., p. 24.
[110] Ibid.

case was notified *without undue delay and, where feasible, not later than 72 hours after having become aware of it*. This duty was clearly breached in this case, as despite the fact that the company and some of its top executives were aware of the breach at least as of June 2021 (a fact acknowledged by Argon itself),[111] the breach was notified to Datatilsynet only in September 2021, and this was not due to an occasional oversight, given that Argon claims that its internal "guidelines were followed to the best of Argon's ability in relation to this Incident".[112] Seeking legal advice from external counsel is not sufficient to respect such a duty, and whether or not the company or its top executives were aware of the obligation imposed by Article 33(1) GDPR at the time they became aware of the breach, or that that obligation applied to the breach at hand, is irrelevant in this respect (*ignorantia legis non excusat*).[113] Moreover, it should be noted that legal advice given by a lawyer cannot, in any event, form the basis of a legitimate expectation on the part of an undertaking that its conduct does not infringe Article 33 GDPR or will not give rise to the imposition of a fine.[114] Therefore, an undertaking which has infringed that provision may not escape imposition of a fine where the infringement has resulted from that undertaking erring as to the lawfulness of its conduct on account of the terms of legal advice given by a lawyer.[115]

#### 7.1.3. Action Taken by the Controller to Mitigate the Damage Suffered by Data Subjects (Art. 83(2)(c))

Argon has taken several specific remedial actions in order to mitigate risks of damage to the data subjects affected by the breach. For example, after the incident, Argon [redacted].[116] Argon has also notified the individuals affected by the breach on 20 October 2021, and offered them 12 months of complimentary credit (and/or identity) monitoring services,[117] although it did it only in October 2021, after the opening of Datatilsynet's inquiry. However, Argon claims that preparations for notifications to data subjects were already in progress whilst the notifications to the European supervisory authorities were being drafted and submitted.[118] Further, Argon offered a session to the involved individuals and gave them the opportunity to ask questions about the incident.[119] All in all, this goes to the credit of Argon and should be weighed in favor of the company in the present case.

[111] See Argon's Notification, paras. 1.1-1.2.
[112] Argon's Response to Datatilsynet, para. 4.1.
[113] See by analogy Opinion of Advocate General Tizzano in Case C-551/03 P, *General Motors BV (formerly General Motors Nederland BV) and Opel Nederland BV v Commission of the European Communities*, para. 77.
[114] See by analogy judgment in Case C-681/11, *Schenker and Others*, para. 41.
[115] Ibid, para. 43.
[116] See Argon's Notification, para. 4.2.
[117] Argon's Response to Datatilsynet, para. 7.1.
[118] See Argon's letter to Datatilsynet dated 22 February 2022, p. 25.
[119] Argon's Response to Datatilsynet, para. 7.3.

#### 7.1.4. Degree of Responsibility of the Controller Taking Into Account the Technical and Organizational Measures Implemented Pursuant to the GDPR (Art. 83(2)(d))

As noted above, the GDPR imposes a requirement on controllers to have appropriate technical and organizational measures to establish immediately whether a personal data breach has taken place and to inform promptly the competent supervisory authorities.

In the context of Datatilsynet's inquiry, Argon claimed that:

> *Argon implemented a global information security programme in the fourth quarter of the 2020 financial year, which was designed to provide an overall risk-based approach to cyber security, to align with global security frameworks and ensure compliance with the GDPR. This includes the lnformation Security Policy, enacted on 12 January 2021. Section 13 of this policy outlines the relevant guidelines to Argon staff regarding information security incident management.*[120]

Argon did not produce such Information Security Policy to Datatilsynet. However, it stated that Argon's internal "guidelines were followed to the best of Argon's ability in relation to this lncident."[121] This is in itself indicative of the fact that Argon's internal policies were not adequate to enable the company to comply with its obligations under Article 33(1), if following the internal policies led to a considerable delay in the notification to Datatilsynet. Again, it should be emphasized that what is reproached to Argon in this case is only the lack of adequate procedures and routines to ensure a timely notification of a personal data breach under the GDPR, and not the failure to put in place other kinds of cybersecurity measures. Thus, any other measures that Argon may have taken pursuant to Article 25 and 32 GDPR are essentially immaterial for the purposes of the present case.[122]

The company's account of how it handled the breach at hand and how it would handle breaches generally reveals some of the possible root causes of the inadequacy of Argon's measures. For instance, the company seems to rely systematically and extensively on external consultants to determine whether a personal data breach should be reported in Europe, as it states that:

> *Once any potential personal data is identified, Argon engages and seeks advice from legal counsel in all potentially affected jurisdictions to understand whether the incident is likely to meet respective thresholds and to ensure legal and regulatory compliance for the purposes of any potential notification.*[123]

While companies are entitled to seek legal advice as they see fit, this compliance model would generally slow down the reporting process, in particular if it is not accompanied by clear instructions to the external advisors on the timeframe for their assessment, which should necessarily be shorter than 72 hours to enable Argon to meet the Article 33(1) deadline. In any

[120] Ibid., para. 4.1.
[121] Ibid.
[122] Cf. See Argon's letter to Datatilsynet dated 22 February 2022, pp. 3-11.
[123] Argon's Response to Datatilsynet, para. 4.4.

event, the controller bears the burden of ensuring and demonstrating the adequacy of its technical and organizational measures to meet its obligations under the GDPR,[124] and is ultimately responsible for any non-compliance or delays caused by the external consultants it uses.

Moreover, the Data Protection Officer ("DPO) that Argon involved in the management of the breach and the related notification process does not appear to have the necessary functional independence to carry out that role, as he simultaneously acted as Argon's Director of Global IT Security.[125] In this regard, it should be noted that that the tasks and duties of a Director of IT Security are generally incompatible with those of a DPO under Article 38(6) GDPR,[126] as a Director of IT Security would normally be significantly involved in "determining the objectives and methods of processing personal data" with respect to the development and deployment of cybersecurity measures[127] and would thus not have the sufficient "functional independence" to carry out "the review of those objectives and methods […] independently".[128] While Argon's compliance with Articles 37-39 GDPR falls outside the scope of the present case, these elements further confirm Argon's failure to ensure that all of the necessary organizational measures were in place in order to properly handle the personal data breach notification at issue in the present case.[129]

Accordingly, we consider that Argon carries a moderate to high level of responsibility in this context.

#### 7.1.5. Relevant Previous Infringements by the Controller (Art. 83(2)(e))

The criterion at Article 83(2)(i) is not applicable in the present case, as Argon has not been sanctioned for similar or otherwise "relevant" infringements in the past.

#### 7.1.6. Degree of Cooperation with the Supervisory Authority (Art. 83(2)(f))

---

[124] See Articles 5(2) and 24 GDPR.

[125] See Argon's letter to Datatilsynet dated 22 February 2022, p. 26.

[126] WP29, Guidelines on Data Protection Officers ('DPOs') (WP 243 rev.01, adopted on 13 December 2016, as last Revised and Adopted on 5 April 2017) (hereinafter "DPO Guidelines"), p. 16.

[127] In the present case, it should be noted that Argon's Director of IT Security was in "charge to design, develop and deploy an Information Security and Compliance Programme at Argon" and that "Argon's Director of IT Security formed part of [a] key leadership team and ensured that all information was made available to the investigating teams, whilst continuing to progress Argon's global information security and compliance programme". See Argon's letter to Datatilsynet dated 22 February 2022, pp. 6 and 8. Therefore, due to their role within the company, Argon's Director of IT Security was inevitably involved in determining the objectives and methods of processing personal data in the context of developing and deploying Argon's information security and compliance programme.

[128] CJEU, Case C-453/21, *X-FAB Dresden GmbH & Co. KG v FC*, paras. 44 and 45.

[129] In this regard, it should be noted that "the DPO should play an key role in assisting the prevention of or preparation for a breach by providing advice and monitoring compliance, as well as during a breach (i.e. when notifying the supervisory authority), and during any subsequent investigation by the supervisory authority. In this light, WP29 recommends that the DPO is promptly informed about the existence of a breach and is involved throughout the breach management and notification process". See DPO Guidelines, p. 28. These guidelines have been endorsed by the EDPB. See EDPB, Endorsement 1/2018 (adopted on 25 May 2018).

Argon has provided a timely response to Datatilsynet's request for further information.[130] However, Argon's cooperation did not go beyond what was required by law. Thus, in our view, this factor should be weighed neither in favor nor against Argon. As noted by the EDPB with respect to Article 83(2)(f): "it would not be appropriate to give additional regard to cooperation that is already required by law".[131]

In its written representations, Argon argued that its cooperation with Datatilsynet should be considered a mitigating factor and not a neutral element. We take note of this argument, but find it unconvincing. As noted by the EDPB, "it must be reiterated that a general obligation to cooperate is incumbent on the controller […] pursuant to Article 31 GDPR, and that lack of cooperation may lead to the application of the fine provided for in Article 83(4)(a) GDPR. It should therefore be considered that the ordinary duty of cooperation is mandatory and should therefore be considered neutral (and not a mitigating factor)".[132]

#### 7.1.7. Categories of Personal Data Affected by the Infringement (Art. 83(2)(g))

The breach at issue in the present case did not affect any special categories of personal data (within the meaning of Article 9 GDPR). However, it did affect data such as salary and benefit information which are—as acknowledged by Argon itself—"subject to a greater degree of sensitivity"[133] on the part of the individuals affected. Even if the attacker was probably not aiming at collecting personal data, the data accessed by the attacker could potentially be used to commit actions leading to both material (e.g., financial loss) and non-material damage (e.g., identity theft or fraud), or could be used to facilitate other attacks (e.g. phishing).[134] Hence, the categories of data affected warranted a prompt response from Argon, not only in terms of remedial actions but also in terms of data breach notifications. This element should be weighed against Argon in the present case.

With respect to the data affected by the incident, "Argon recognises [in its written representations that] there may attach a greater degree of sensitivity if disclosed to colleagues" but it "did not consider that this information places the involved individuals at a high risk of identity theft and fraud, or phishing" also in light of the mitigating measures the company put in place.[135] We take note of this statement, but find it immaterial for the purposes of assessing the criterion at Article 83(2)(g), as the latter provision only demands that due regard should be given to the "the categories of personal data affected by the infringement"—which in the present case and according to Argon itself concern data "subject to a greater degree of

[130] See the Factual Background above.
[131] Guidelines on Administrative Fines, p. 14.
[132] EDPB, Guidelines 04/2022 on the calculation of administrative fines under the GDPR, Version 1.0, Adopted on 12 May 2022 Para. 96.
[133] Argon's Notification, para. 2.6.
[134] EDPB Guidelines on Examples regarding Data Breach Notification, page 32.
[135] See Argon's letter to Datatilsynet dated 22 February 2022, p. 26.

sensitivity"[136]—and not the level of risk for data subjects (which was assessed under Article 83(2)(a) in section 7.1.1 above). In any event, for completeness purposes, we note that to establish an infringement of Article 33(1) GDPR, the relevant level of risk is the one perceived or perceivable when the notification was due, and that Argon notified Datatilsynet because it concluded that the incident "was not unlikely to result in a risk to the rights and freedoms of [the affected] individuals".[137]

#### 7.1.8. Manner in Which the Infringement Became Known to the Supervisory Authority (Art. 83(2)(h))

The infringement contested in the present case—which concerns a failure to notify on time, and not a failure to notify as such—became known to Datatilsynet after a careful scrutiny of Argon's very lengthy and detailed notification. Such a notification did not inform Datatilsynet of the delay. On the contrary, its introductory statement was misleading in that it said that "Argon only became aware [of a personal data breach within the meaning of the GDPR] on 21 September 2021",[138] and thus a superficial reading of the notification could have led the authority to believe that the notification was submitted on time three days later, on 24 September 2021. Therefore, the infringement became known to Datatilsynet only after and due to a careful assessment of the notification and the inquiry that followed it. This factor should be weighed against Argon.

While the infringement contested in this case is not a failure to notify as such or a violation of the broader security requirements set out by the GDPR, for completeness purposes, it should be made clear that, as indicated by the EDPB:

> *The controller has an obligation according to the Regulation to notify the supervisory authority about personal data breaches. Where the controller merely fulfils this obligation, compliance with the obligation cannot be interpreted as an attenuating/ mitigating factor.*[139]

In its written representations, Argon argued that the manner in which Datatilsynet became aware of the infringement should not be weighed against Argon, as its notification was not intended to deceive supervisory authorities and simply reflected its understanding of the timeline of the breach at the time of the notification.[140] We take note of this argument, but find it unconvincing. In the present case, there is no evidence of an intentional infringement on Argon's part (see section 7.1.2 above), and Datatilsynet has no ground to conclude that the notification was intentionally misleading. However, the negligent conduct of the controller that ultimately triggered the opening of an inquiry "may also be considered by the supervisory authority to merit a more serious penalty", including where the controller "acted carelessly without […] notifying all of the details of the infringement due to a failure to adequately assess

[136] Argon's Notification, para. 2.6.
[137] Argon's Notification, page 1.
[138] Ibid.
[139] Guidelines on Administrative Fines, p. 15.
[140] See Argon's letter to Datatilsynet dated 22 February 2022, p. 27.

the extent of the infringement".[141] This is the factor that Datatilsynet considers to be relevant under Article 83(2)(h) in the present case, as Argon acted carelessly by providing inaccurate and misleading details on the personal data breach at issue in the present case in its notification to Datatilsynet, namely the fact that "Argon only became aware [of a personal data breach within the meaning of the GDPR] on 21 September 2021".[142]

In its written representations, Argon also claimed that Datatilsynet's approach with respect to the criterion at Article 83(2)(h) in the present case would be at odds with the approach that Datatilsynet followed in a prior case where – according to Argon – Datatilsynet did not treat as an aggravating factor the fact that "the Oslo Municipality admitted that their breach notifications were misleading".[143] This claim is simply inaccurate, as Datatilsynet expressly stated that that fact played a role in its assessment of whether a fine had to be imposed on the Oslo Municipality (which eventually occurred in that case).[144]

#### 7.1.9. Compliance with Corrective Measures Previously Ordered Against the Controller with Regard to the Same Subject-Matter (Art. 83(2)(i))

The criterion at Article 83(2)(i) is not applicable in this case, as no measures referred to in Article 58(2) GDPR have previously been ordered against Argon by Datatilsynet.

#### 7.1.10. Adherence to Approved Codes of Conduct or Certification Mechanisms (Art. 83(2)(j))

The criterion at Article 83(2)(j) is not applicable in this case, as Argon does not appear to adhere to any approved codes of conduct pursuant to Article 40 GDPR or approved certification mechanisms pursuant to Article 42 GDPR.

#### 7.1.11. Any Other Aggravating or Mitigating Factor (Art. 83(2)(k))

Another aggravating factor is the fact that—as outlined above—Argon not only notified the breach to Datatilsynet with a considerable delay from the moment when it became aware of the personal data breach (i.e., at least on 19 July 2021); it also took Argon over a month to find out that personal data had been compromised after it first detected the security incident. This factor should be weighed against Argon in the present case.

In its written representations, Argon argued that "the timeline for the forensic investigation should not be considered an aggravating factor in the circumstances".[145] We take note of this argument, but we find it unconvincing. Although the GDPR required Argon to implement all

[141] Guidelines on Administrative Fines, p. 15.
[142] Argon's Notification, page 1.
[143] See Argon's letter to Datatilsynet dated 22 February 2022, p. 28.
[144] See Vedtak om overtredelsesgebyr (ref: 18/02579-13/KBK), p. 10 (stating in Norwegian: "Oslo kommune innrømmer da også at avviksmeldingene var misvisende. Dette vil ha betydning i vår vurdering om overtredelsesgebyr skal ilegges" (emphasis added)).
[145] See Argon's letter to Datatilsynet dated 22 February 2022, p. 29.

appropriate technical protection and organisational measures to "establish *immediately*"[146] whether a breach has taken place and to inform promptly the supervisory authority and the data subjects, Argon took measures to assess whether personal data were affected by the incident only in July 2021,[147] even though it was aware of the incident since 14 June 2021.[148]

Argon also submitted that the fact that Argon gained no financial benefits due to the violation of Article 33(1) "should in itself be seen as a mitigating factor".[149] This argument should be rejected. In this regard, it suffices to note that, under EU/EEA law, it is well established that the benefits obtained from an infringement are among the factors that *may* be taken into account in order to determine the amount of the fine, but there is no obligation to ensure that the fine is directly proportional to the benefits achieved by that undertaking or that it does not exceed those benefits.[150] Therefore, the absence of financial benefits may be regarded as a neutral factor, as the aim of Article 83(2)(k) is to ensure that the sanction applied is effective, proportionate and dissuasive in each individual case.[151]

### 7.2. Conclusion with Regard to Whether to Impose an Administrative Fine

Having had due regard to the factors under Article 83(2), in our view, the infringement that has been identified warrant the imposition of an administrative fine in the circumstances of this case.

Despite the limited number of individuals affected by the data breach at issue and the measures taken by Argon to contain the consequences of the breach, the considerable duration of the delay and Argon's approach towards the interpretation of its data breach notification obligations under the GDPR are indicative of broader compliance flaws within the company, which—if not remedied—could result in serious consequences in the event of future breaches. In Datatilsynet's view, the imposition of an administrative fine is therefore warranted to produce a genuine deterrent effect, and dissuade Argon—as well as companies in general—from committing similar infringements in the future. Indeed, enforcement efforts must generate sufficient pressure to make non-compliance economically unattractive in practice.[152] This is particularly salient with regard to data breach notification obligations, as companies appear to have often a tendency not to report data breaches to regulators, or to be otherwise opaque about the breaches they experience.[153]

---

[146] See Recital 87 GDPR (emphasis added).
[147] See Argon's Notification, para. 1.4.
[148] Ibid., para. 1.1.
[149] See Argon's letter to Datatilsynet dated 22 February 2022, p. 29.
[150] See judgment in Case T-406/09, *Donau Chemie AG v European Commission*, para. 258; EDPB, Binding Decision 2/2022 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Meta Platforms Ireland Limited (Instagram) under Article 65(1)(a) GDPR, para. 219.
[151] See EDPB, Binding Decision 2/2022 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Meta Platforms Ireland Limited (Instagram) under Article 65(1)(a) GDPR, para. 216.
[152] See Opinion of Advocate General Geelhoed in Case C-304/02, *Commission v. France*, delivered on 29 April 2004, para. 39.
[153] For example, a survey conducted among 597 companies in 33 European countries revealed that only 23% of breaches are reported to European regulators. See Catch-22: Digital Transformation And Its Impact On Cybersecurity – RSM (2019).

In its written representations, Argon claimed that the imposition of an administrative fine would be at odds with Datatilsynet's administrative practice in similar cases, and hence with the principle of administrative consistency and equal treatment.[154] In this respect, Argon referred to a prior case in which Datatilsynet imposed a reprimand—instead of an administrative fine—against a company that failed to comply with Article 33(1) GDPR.[155] The latter case (Case 20/02137, Telenor Norge AS, hereinafter "Telenor case") is, however, not comparable to the present one:

- In the Telenor case there was no evidence that a personal data breach had actually taken place (but it could not be excluded in the circumstances of that case),[156] whereas in the present case Argon's internal investigation revealed that employees' personal data "were accessed by the Threat Actor".[157]

- In the Telenor case there was no evidence of any specific data subject being affected by the breach and lack of notification, whereas the present case concerns the data of several identified employees, including an employee in Norway.

- In the Telenor case Datatilsynet identified a violation of Article 33(1) as a result of an own volition inquiry it opened, in light of press reports, shortly after the likely occurrence of a breach in November 2019 (i.e., within a matter of a few weeks from when the deadline for submitting a notification under Article 33(1) started to run), whereas in the present case Argon's notification was submitted and the violation of Article 33(1) was identified several months after the expiry of such deadline.

- In the Telenor case the violation of Article 33(1) was due to a failure to notify in circumstances where the controller had been unable to exclude that an authorized third party had access to personal data being processed by the controller, whereas in the present case Argon's failed to timely notify Datatilsynet even though its internal investigation revealed that certain personal data of its European employees "were accessed by the Threat Actor".[158]

- The Telenor case did not concern data "subject to a greater degree of sensitivity"[159] like the present case.

---

[154] See Argon's letter to Datatilsynet dated 22 February 2022, p. 23.
[155] Ibid. See too Argon's letter to Datatilsynet dated 11 March 2022.
[156] See Datatilsynet's Vedtak om irettesettelse - Informasjonssikkerhet knyttet til talepostkasse (Doc. No. 20/02137-2), p. 10 (stating (in Norwegian): "Datatilsynet mener derfor at det forelå en rimelig grad av sikkerhet for at det var skjedd et brudd da Telenor ble kjent med sårbarheten i november 2019, og brukerlogger for kun én måned var gjenstand for analyser. Datatilsynet mener altså at det forelå et meldepliktig brudd på personopplysningssikkerheten selv om det ikke kan konstateres med sikkerhet at sårbarheten faktisk ble utnyttet").
[157] Argon's Notification, paras. 1.4 and 1.7.
[158] Ibid.
[159] Ibid, para. 2.6.

- In the Telenor case the relevant company had already been fined NOK 1 500 000 (one million five hundred thousand) by a different authority (NKOM) in connection with the same incident prior to the completion of Datatilsynet's inquiry, and although such a fine was not issued for a violation of Article 33(1) GDPR, it was taken into account by Datatilsynet when assessing whether it was appropriate to issue another administrative fine or a reprimand.

It should be noted that other European supervisory authorities have imposed administrative fines to companies that failed to notify a personal data breach within the deadline imposed by Article 33(1), even in cases where the delays were significantly smaller than in the present case (e.g., a 22-day delay, and a 2-day delay in the context of the winter holidays).[160] It bears emphasizing that virtually all European supervisory authorities have been involved in such previous cases through the procedure set out in Article 60 GDPR. Thus, there was essentially unanimous agreement among European supervisory authorities that an administrative fine was warranted in such cases. Moreover, the multiple examples of cases in which European supervisory authorities have issued fines for violations of Article 33(1) given by Argon itself show that this kind of violations have frequently been deemed to warrant the imposition of an administrative fine.[161] Finally, it should be noted that Datatilsynet has already issued fines in circumstances where a violation of the GDPR affected a single data subject in Norway.[162]

### 7.3. Calculation of the Amount of the Administrative Fine

Having had due regard to the factors under Article 83(1) and (2), we find an administrative fine of NOK 2 500 000 (two million five hundred thousand) to be appropriate in the circumstances of this case. This is for the reasons outlined below.

In terms of the requirement under Article 83(1) to ensure that the imposition of the fine in the circumstances of this case is effective, proportionate and dissuasive, the financial position of Argon must be taken into account. The financial position of Argon is also relevant to determine the maximum fine applicable in the present case.

Argon's total annual turnover appeared to be in excess of $ 215 million (i.e., approximately NOK 1 900 000 000) in 2020,[163] and increased by approximately 20% in 2021.[164] Thus, the

---

[160] See Dutch Data Protection Authority, Decision Against Booking.com B.V of 10 December 2020 <https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit_boete_booking.pdf>; Irish Data Protection Commission ("DPC"), Decision Against Twitter International Company of 9 December 2020 (DPC Case Reference: IN-19-1-1) <https://edpb.europa.eu/sites/default/files/decisions/final_decision_-_in-19-1-1_9.12.2020.pdf>. The DPC's decision has been confirmed in the Dublin Circuit Court <https://www.dataprotection.ie/en/news-media/press-releases/confirmation-fine-twitter-international-company>.

[161] Cf. Argon's letter to Datatilsynet dated 22 February 2022, pp. 20-23.

[162] See e.g. Case 20/01874, Basaren Drift AS; Case 20/02220, Flisleggingsfirma AS; Case 20/02375, Ultra-Technology AS.

[163] This is according to the 2020 Annual Results of the Wego Group to which Argon belongs. See Wego, Investor Presentation: 2020 Annual Results (March 2021) <http://en.weigaogroup.com/upload/202103/30/202103301927500480.pdf> (stating: "In FY2020 Argon recorded total sales RMB1,370m").

[164] This is according to the 2021 Annual Results of the Wego Group to which Argon belongs. See Wego, Investor Presentation: 2020 Annual Results (March 2022)

maximum fine applicable in the present case is 10 000 000 EUR (i.e., around 100 000 000 NOK), as the latter amount is higher than 2% of the company's total annual turnover, and Article 83(4)(a) provides that infringements of Article 33 shall be subject to "administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher" (emphasis added).

Having considered the above, a fine of NOK 2 500 000 (two million five hundred thousand) seems appropriate, as it represents approximately 2.5% of the maximum applicable fine and sits within the lower end of the spectrum of possible fines. Therefore, such a fine is commensurate with the seriousness of the infringement for which it is imposed, taking into account all of the aggravating and mitigating factors outlined above (see sections 7.1.1 to 7.1.11).

Such a fine would represent approximately 0.1% of Argon's annual turnover for 2020 (or a smaller percentage if one considers the turnover for 2021). Therefore, it would have some significance to the company relative to its revenue—which is essential to ensure its dissuasive effect—without being disproportionate relative to the company's financial position and the infringement viewed as a whole.

In its written submissions, Argon claimed that the amount of the fine indicated above is disproportionately high and that it would not be in line with the existing administrative practice across the EU/EEA regarding administrative fines for violations of Article 33(1),[165] although the company did not provide the exact references of the specific cases that would support the latter claim.[166] In this regard, we reiterate that the setting of a fine is not an arithmetically precise exercise,[167] and supervisory authorities have a certain margin of discretion in this respect.[168] In any event, the examples given by Argon in its written submissions focus primarily on the numeric value of the fines imposed, but do not show how each of the amounts relate to the economic size of the recipient of the fine.[169] The size of the undertaking concerned is one of the key elements that should be taken into account in the calculation of the amount of the fine in order to ensure its dissuasive nature.[170] Taking into consideration the resources of the undertaking in question is indeed justified by the impact sought on the undertaking concerned, in order to ensure that the fine has sufficient deterrent effect, given that the fine must not be

<http://en.weigaogroup.com/upload/202208/22/202208221507029683.pdf> (stating: "Argon's revenue increased by 20.8% based on fixed exchange rate").

[165] See Argon' letter to Datatilsynet dated 22 February 2022, pp. 20-23.

[166] Argon referred to a number of fines issued for violations of Article 33(1) GDPR by various European supervisory authorities, but without providing any case number or reference.

[167] See, *inter alia,* Case T-425/18, *Altice Europe NV v Commission*, para. 362; Case T-11/06, *Romana Tabacchi v Commission*, para. 266. See too EDPB, Decision 01/2022 on the dispute arisen on the draft decision of the French Supervisory Authority regarding Accor SA under Article 65(1)(a) GDPR, adopted on 15 June 2022, para. 74.

[168] See, *inter alia*, Case T-192/06, *Caffaro Srl v Commission*, para. 38. See too EDPB, Decision 01/2022 on the dispute arisen on the draft decision of the French Supervisory Authority regarding Accor SA under Article 65(1)(a) GDPR, adopted on 15 June 2022, para. 74.

[169] Cf. Argon' letter to Datatilsynet dated 22 February 2022, pp. 20-23.

[170] EDPB, Decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR, paras. 405-412; EDPB, Decision 01/2022 on the dispute arisen on the draft decision of the French Supervisory Authority regarding Accor SA under Article 65(1)(a) GDPR, adopted on 15 June 2022, para. 76.

negligible in the light, particularly, of its financial capacity.[171] In this respect, it suffices to note that in a case concerning violations of the GDPR that the Norwegian Privacy Appeals Board (Personvernnemda) did not consider too serious, Personvernnemda deemed a fine equal to 0,9% of the annual turnover of the preceding financial year to be adequate.[172] Moreover, other European supervisory authorities have imposed fines for violations of Article 33(1) GDPR that are even higher—relative to the turnover of the relevant controller—than the one imposed in the present case. For instance, the Finnish supervisory authority imposed a fine of 145 600 EUR for an infringement of Article 33(1) GDPR, equal to approximately 1% of the annual turnover of the preceding financial year of the relevant controller.[173]

## 8. Right of Appeal

An appeal may be lodged against this decision by sending us a written complaint within three weeks after having received the present decision.[174] If we decide to uphold our decision after having received such a written complaint, we will transfer the case to Personvernnemnda, our appeal body.[175]

Kind regards

Jørgen Skorstad
Director, Legal Department

Luca Tosoni
Specialist Director

*This letter has electronic approval and is therefore not signed*

Copy to: ADVOKATFIRMAET RÆDER AS

[171] Case C-408/12 P, *YKK and Others v Commission*, para 85; Case C-413/08 P, *Lafarge v European Commission*, para. 104 and the case law cited therein. See too EDPB, Decision 01/2022 on the dispute arisen on the draft decision of the French Supervisory Authority regarding Accor SA under Article 65(1)(a) GDPR, adopted on 15 June 2022, para. 76.
[172] See PVN-2021-13.
[173] See Case 1150/161/2021.
[174] See Sections 28 and 29 of the Norwegian Public Administration Act.
[175] See Section 22 of the Norwegian Personal Data Act.