Datatilsynet

ZALARIS ASA
Postboks 1053 Hoff

0218 OSLO

Your reference	Our reference	Date
	21/02873-22	10.05.2022

Compliance Order - Zalaris ASA

1. Introduction

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 18 March 2022, we notified Zalaris ASA ("Zalaris", "you", "your", "the company") of our intention to order Zalaris to comply in full with an access request it received on 28 September 2021 from a data subject residing in Germany. We also informed Zalaris that it could submit written representations in relation to the advance notification in question by 8 April 2022. However, Zalaris did not submit any written representations to Datatilsynet within the said deadline.

On 11 April 2022, Datatilsynet submitted a draft decision—which essentially reproduced the above advance notification—to the other supervisory authorities concerned in accordance with Article 60(3) GDPR. None of the other supervisory authorities concerned expressed a relevant and reasoned objection to the draft decision within four weeks after having been consulted by Datatilsynet.

Thus, the present decision is adopted in conformity with the advance notification we sent to Zalaris and the draft decision we submitted to the other supervisory authorities concerned.

2. Decision

Pursuant to Article 58(2)(d), we order Zalaris to:

[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 [2016] L 119/1.

> Provide the complainant with all of the information he requested and is entitled to receive pursuant to Article 15 GDPR, including complete information on the purposes of the processing, the categories of personal data concerned, and the relevant storage period(s). Further, Zalaris shall provide the complainant with a copy of all of his personal data that are being processed by the company and have not yet been sent to him, unless Zalaris is able to demonstrate that one of the exceptions set out in Articles 12(5) and 15(4) GDPR or Article 16 of the Norwegian Personal Data Act applies. The information shall be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Zalaris shall notify the measures taken for complying with this decision to Datatilsynet within four weeks after having received the present decision.

Our inquiry has only focused on Zalaris' compliance with Articles 12 and 15 GDPR in connection with the above-mentioned complaint. Thus, the present decision is without prejudice to the possibility of opening future inquiries into Zalaris' compliance with other provisions of the GDPR, including with the broader transparency requirements imposed by Articles 5(1)(a) and 13 GDPR, as well as the data erasure requirements set out in Articles 5(1)(e) and 17.

3. Factual Background

On 14 July 2021, the complainant—i.e. a data subject residing in Germany who used to be employed in the German subsidiary of Zalaris (i.e., Zalaris Deutschland GmbH, which was merged with Zalaris Deutschland AG)—wrote to [redacted]—to exercise his right of access under Article 15 GDPR.[2] In particular, he requested the following information:

> […] [*sic*] *due to article 15 EU GDPR I would like to obtain following information from ZALARIS ASA:*
> • *Information about Automated Decision Logic if applicable*
> • *Information about the Right of correction and limitation*
> • *Information about the Right to complaint*
> • *The name and contact data of Controller*
> • *The name and contact data of Data protection officer*
> • *The Data Protection Guarantee if applicable*
> • *A complete copy of personal data in an easily visible, intelligible and clearly legible manner*
> • *The purposes of processing*
> • *The period of storage*
> • *The categories of personal data*
> • *The recipients of data transfer*
> • *The data source* […].[3]

[2] See complaint dated 26 August 2021.
[3] Ibid.

As he received no response from the company, on 26 August 2021, the data subject filed a complaint against Zalaris with Datatilsynet.[4]

After having received such a complaint, on 26 September 2021, Datatilsynet recommended the complainant to resubmit his access request by sending an email to gdpr@zalaris.com (i.e. the email address for submitting data protection inquiries provided in the privacy policy on Zalaris' website).[5] Thus, on 28 September 2021, the complainant resubmitted his access request by forwarding the email he had sent to [redacted] to gdpr@zalaris.com.[6] However, on 31 October 2021, the complainant informed Datatilsynet that, even after having sent this second email, he had not received any response from Zalaris.[7]

On 1 November 2021, Datatilsynet wrote to Zalaris to inquire about the aforementioned access requests.[8] Datatilsynet's letter ordered Zalaris to respond to several questions on the case at hand by 30 November 2021. However, on 1 December 2021, Datatilsynet had still not received any answer from Zalaris. Thus, we sent a reminder to the company on the same date.[9]

Further to the above reminder, on 1 December 2021, Zalaris replied to Datatilsynet and claimed that the delay was due to the fact that the email with the response for Datatilsynet had remained in the outbox folder of the sender without him noticing it.[10]

As for the access request(s) at issue in the present case, in its reply to Datatilsynet, Zalaris stated that the company processed only the personal data that were relevant for the data subject's employment in Germany.[11] However, Zalaris' reply referred to a different email that [redacted] received from the complainant on 14 July 2021, which he (rightfully) did not interpret as an access request pursuant to Article 15 GDPR.[12]

After having received Zalaris' reply, on 1 December 2021, Datatilsynet wrote to Zalaris to stress that our inquiry concerned a different email, and once again asked the company to provide information on the access request that the complainant sent to [redacted] on 14 July 2021 at 17:23, and to gdpr@zalaris.com on 28 September 2021 at 13:29.[13]

On 2 December 2021, [redacted] wrote the following to Datatilsynet:

---

[4] Ibid.
[5] See Datatilsynet's email to the complainant dated 26 September 2021.
[6] See complanaint's email to Zalaris dated 28 September 2021.
[7] See complanaint's email to Datatilsynet dated 31 October 2021.
[8] See Krav om redegjørelse - innsyn i personopplysninger (ref: 21/02873-9) dated 1 November 2021.
[9] See Datatilsynet's email to Zalaris dated 1 December 2021 (sent at 15:56).
[10] See Zalaris' email to Datatilsynet dated 1 December 2021 (stating: "Beklageligvis så gikk denne ikke ut umiddelbart den 8.11 da den ble skrevet da den ble liggende som draft i min utboks"). This appears to be evidenced by the fact that the letter with Zalaris' response that was eventually sent to Datatilsynet was dated 8 November 2021.
[11] See Zalaris' letter to Datatilsynet dated 8 November 2021 (but received by Datatilsynet on 1 December 2021) (stating: "Vi behandlet kun personopplysninger relevant for hans ansattforhold og utbetaling av lønn.").
[12] Ibid. See too the email that the complainant sent to [redacted] on 14 July 2021 at 18:02 (annexed to Zalaris' reply to Datatilsynet).
[13] See Datatilsynet's email to Zalaris dated 1 December 2021 (sent at 17:44).

[…] *We have now investigated the case further.*

It now turns out that I, as CEO of Zalaris, received an email on July 14 while I was on vacation. For information, Zalaris has approximately 880 employees in 14 countries and I receive at least 200+ emails daily. I have not had any direct relationship with the complainant as he was previously employed by our German subsidiary Zalaris Deutschland AG. The email was forwarded to the management in Germany on 16 July, where the former employee – [i.e., the complainant] *– who demanded access had been employed until the end of September 2019.*

Our German management responded to a similar request from [the complainant's] *lawyer in April 2021, and a copy of the stored data was sent in electronic format to the lawyer as part of the conclusion of a settlement agreement. As the case was considered closed, the inquiry dated 14 July was therefore not answered further.*

The inquiry to gdpr@zalaris.com seems to have been treated as spam due to the form and unknown email address in our systems. We have not received any other reminders or requests for access through another channel.

We from the Zalaris Group will now answer the relevant inquiry in the next few days and at the same time review the quality of our routines to ensure that similar future inquiries are answered in a timely manner […] (our translation).[14]

On 22 December 2021, Zalaris replied to the data subject's access request as follows:

[…] *We have received a notification by the Norwegian Data Protection authority that you have not received a response on the below article 15 request dated 14th of July and a similar request that shall have been sent to gdpr@zalaris.com on the 28th of September.*

As your initial request was sent to my private email in the middle of my vacation, I forwarded this to our German management for action. As they were of the opinion that they had responded to a similar request by your lawyer in April 2021 where a copy of your data was requested, and they were of the opinion that they had settled outstanding issues with you, they did not proceed with a further response.

[14] See Zalaris' email to Datatilsynet dated 2 December 2021 (stating in Norwegian: "Vi har nå undersøkt saken nærmere. Det viser seg nå at jeg som CEO for Zalaris har mottatt mail som referert til 14. juli mens jeg var på ferie. Til info så har Zalaris ca. 880 ansatte i 14 land og jeg mottar minst 200+ mail daglig. Jeg har ikke hatt noen direkte relasjon med klageren da denne tidligere var ansatt i vårt tyske datterselskap Zalaris Deutschland AG. Emailen ble den 16.7 videresendt til ledelsen i Tyskland hvor den tidligere ansatte – [klageren] - som krevet innsyn hadde vært ansatt frem til slutten av september 2019. Vår tyske ledelse besvarte en tilsvarende henvendelse fra [klageren]'s advokat i April 2021 hvorpå kopi av lagrede data ble oversendt i elektronisk format til advokaten som et ledd i inngåelse av et forlik om sluttavtale. Da saken var ansett som avsluttet ble det derfor ikke henvendelsen datert 14. juli besvart ytterligere. Henvendelsen til gdpr@zalaris.com ser ut til å ha blitt oppfattet som søppelpost pga form og ukjent mail adresse i våre systemer. Vi har ikke fått andre påminnelser eller ønske om innsyn formidlet i annen kanal. Fra Zalaris Group vil vi nå besvare den aktuelle henvendelsen ila de nærmeste dagene og samtidig kvalitetssikre våre rutiner med mål at tilsvarende fremtidige saker blir besvart rettidig.").

> *The email sent to gdpr@zalaris.com appears to have been caught by our junk mail filter and has as such not been processed in due time in our systems. We are changing our solution for gdpr@zalaris.com to a forms based process on our web site with the goal of limiting the likelihood of similar incidents in the future.*
>
> *Attached you will find a copy of our policy on GDRP article 15 responding to the items listed in your email. You will receive a copy of the data that we have about you in our systems via registered mail to your official address of residence. This will be delivered on print and on electronic format in the form of a password protected USB stick. Upon your response to the receipt of this email, we will forward you the password.*
>
> *We apologize for the inconvenience that the delay has caused as both adhering to GDPR requirements and responding to previous employees requests has the highest priority.* […][15]

On 26 January 2022, the complainant wrote to Datatilsynet that he had received a USB stick from Zalaris, but not the password to open the files contained in it.[16] In response to a query from Datatilsynet, the complainant also claimed that he did not receive any email from Zalaris on 22 December 2021.[17] Thereafter, Datatilsynet advised the complainant to contact Zalaris to ask the company to send such an email once again, as well as the password.[18]

On 28 January 2022, the complainant wrote to Zalaris and asked the company to resend the email Zalaris had sent to him on 22 December 2021, as well as the password to access the files in the USB stick he had received.[19] On the same date, Zalaris forwarded the requested email to the complainant, and provided the relevant password.[20]

On 2 March 2022, the complainant wrote to Datatilsynet that—in his view, after having examined Zalaris' response—the company had not fully complied with his access request.[21] On the same date, the complainant also wrote the following to Zalaris:

> […] [*sic*] *After checking the USB stick, it shows that there is no password protection. All files are freely accessible.*
>
> *I'm amazed that most of the data belongs to the ZALARIS Deutschland AG and ZALARIS Deutschland GmbH. I had requested the data that is processed at ZALARIS ASA.*

[15] See Zalaris' email to the complainant dated 22 December 2021. The email also included Zalaris' privacy policy (entitled "Regulation of Zalaris ASA's processing of personal data", and dated 21 December 2021) as an attachment (hereinafter "Regulation of Zalaris ASA's processing of personal data"). Zalaris forwarded that email to Datatilsynet on the same date.
[16] See complainant's email to Datatilsynet dated 26 January 2022.
[17] See complainant's email to Datatilsynet dated 28 January 2022. This appears to be due to some technical issues on the complainant's end, as Datatilsynet had received a copy of the email in question from Zalaris on 22 December 2022.
[18] See Datatilsynet's email to the complainant dated 28 January 2022.
[19] See complainant's email to Zalaris dated 28 January 2022.
[20] See Zalaris' email to the complainant dated 28 January 2022.
[21] See complainant's email to Datatilsynet dated 2 March 2022.

I.e. the ZALARIS ASA has no data from me!

So this means:

i) I received a letter from ZALARIS Deutschland attorney that there are no personal information from me! But you have it.
ii) You have no purpose and no confirmation to process personal data of me regarding ZALARIS Deutschland.
iii) There is no group privilege to use data from subsidiaries. You are not authorized to process incorrect or unauthorized data.
iv) The information about the ZALARIS ASA is wrong. You have at least my claim from 19.11.2021 and the personal data from the contract documents for the purchase/sale of ROC Ltd. But this is not part of your answer!

Therefore I request the following:

1. Immediate deletion of all my personal data regarding ZALARIS Deutschland incl. all data transferred to third parties.
2. Immediate payment of my claim from 19.11.2022
3. Immediate payment of the second rate for the purchase/sale of ROC Ltd.
4. Immediate information about my personal data processed at Zalaris ASA.

Please inform me about the implementation within the next 2 weeks.

[…]

PS: Some notes regarding transparency.

The data sent does not correspond to the legal requirements (see Art. 15 GDPR):

missing: the purposes of the processing;

missing: the categories of personal data concerned;

missing: the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

missing: the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

missing: the right to lodge a complaint with a supervisory authority;

where the personal data are not collected from the data subject, any available information as to their source;

missing: the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

missing: Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

Sometimes (for SAP data) there are some screenshots only, many dates (e.g. data from cluster tables) missing: The controller shall provide a copy of the personal data undergoing processing. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

Due to art. 12 GDPR the date must be "in a concise, transparent, intelligible and easily accessible form, using clear and plain language". There are many unknown data and data in English (e.g. for legal German topics) included.

Due to art. 20 GDPR and due to the court verdict I havn't [*sic*] *got all in a structured, commonly used and machine-readable format (e.g. screenshots).* […].[22]

On 2 March 2022, Zalaris replied:

[…] *Zalaris ASA has no other data related to your employment with us other than the data that you have received.*

We are of the opinion that our response to you included all elements that you claim are missing.

In addition, we as Zalaris ASA signed contractual agreements with you as a commercial party and seller of shares in ROC Ltd, before you became an employee through ROC Deutschland GmbH. This is commercial documentation archived in our contract archive with you as the seller and Zalaris as the buyer. We do not consider this material in the context of GDPR related to your employment with Zalaris. […].[23]

On 18 March 2022, Datatilsynet notified Zalaris of our intention to order the company to comply in full with the access request it received on 28 September 2021 from the complainant.[24]

[22] See complainant's email to Zalaris dated 2 March 2022.
[23] See Zalaris' email to the complainant dated 2 March 2022.
[24] See Varsel om pålegg - Zalaris ASA (ref: 21/02873-15). A copy of the advance notification was also sent to the complainant on the same date.

We also informed Zalaris that it could submit written representations in relation to the advance notification in question by 8 April 2022.[25] However, Zalaris did not submit any written representations to Datatilsynet within the said deadline.

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:

[25] Ibid., section 7.

"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(9) GDPR:

"recipient" means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

4.3. The Right of Access by the Data Subject

Article 15 GDPR reads:

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(f) the right to lodge a complaint with a supervisory authority;

(g) where the personal data are not collected from the data subject, any available information as to their source;

(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the

logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

Furthermore, Article 12(1) to (4) GDPR provides that:

1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

2. The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.

3. The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

4. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

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) 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;* […].

The term "cross-border processing" is defined in Article 4(23) as follows:

> *"cross-border processing" means either:*
>
> *(a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or*
>
> *(b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.*

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. 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").[26]

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.*

[26] 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.

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.[27] The Personal Data Act and the GDPR entered into force in Norway on 20 July 2018.

5. Datatilsynet's Competence

Zalaris is a multinational company offering human resources and payroll administration services. It has its headquarter in Norway, but has operations and offices in several European countries, including in Sweden, Denmark, Finland, Germany, France, Ireland, Latvia, Lithuania, Estonia and Poland.

Thus, Zalaris 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 the employees of its group. Therefore, the GDPR applies to such data processing activities in accordance with Article 3(1) GDPR.

With respect to the processing of the personal data of the complainant, Zalaris qualifies as a controller (within the meaning of Article 4(7) GDPR), as Zalaris itself acknowledges.[28]

As Zalaris has a main establishment (within the meaning of Article 4(16) GDPR) in the EEA and its processing of the complainant's personal data is cross-border (within the meaning of Article 4(23) GDPR), the cooperation mechanism and procedure set out in Articles 56(1) and 60 GDPR apply to the present case. Further, given that Zalaris' main establishment is located in Norway, Datatilsynet is competent to act as lead supervisory authority in the case at hand pursuant to Article 56(1) GDPR.

6. Datatilsynet's Assessment

6.1. Zalaris' Failure to Respond to the Complainant's Access Request in a Timely Manner

Under Article 12(3) GDPR, controllers are required to respond to access requests submitted pursuant to Article 15 GDPR "without undue delay and in any event within one month of receipt of the request." However, in exceptional circumstances, that period may be extended by two further months.

---

[27] Act No 38 of 15 June 2018 relating to the processing of personal data ("personopplysningsloven").

[28] See Regulation of Zalaris ASA's processing of personal data (stating: "Data Controller. The responsible for the processing of personal data that we carry out about you is Zalaris ASA, represented by Managing Director, [redacted] and Data protection officer, [redacted].").

In the present case, Zalaris itself acknowledged that it failed to respond to the complainant's access requests within the above deadline.[29] However, Zalaris claimed that this was due to the fact that the first request was sent directly to the CEO of the company, while the second ended up in the spam folder of the company's email inbox.[30]

As for the request sent directly to [redacted] on 14 July 2021, our view is that not much can be reproached to Zalaris. As noted by the European Data Protection Board (EDPB):

> *The controller is* […] *not obliged to act on a request sent to the e-mail address of a controller's employee who may not be involved in the processing of requests concerning data subjects' rights* […]. *Such requests shall not be considered effective, if the controller has clearly provided the data subject with appropriate communication channel.*[31]

Hence, given that the privacy policy available on Zalaris' website at the time did provide a specific email address to be used for data protection inquiries (i.e., gdpr@zalaris.com),[32] it was legitimate to expect data subjects (including the complainant) to submit access requests through such a communication channel, and not directly to the CEO of the Zalaris. Indeed, the CEO of a company of the size of Zalaris cannot be expected to be directly involved in the processing of requests concerning data subjects' rights. Therefore, in our view, Zalaris did not violate Articles 12(2) and 15 GDPR by failing to respond to the email that the complainant sent directly to [redacted] on 14 July 2021. In this regard, it should be noted that—contrary to what was argued by the complainant[33]—where personal data are processed by a company (which decides on the means and purposes of the processing) it is the company as such that qualifies as the "controller", and not its CEO.[34]

However, under Article 12(2) GDPR, controllers have an obligation to "facilitate the exercise" of the data subject right under Article 15 GDPR. This entails—among other things—that controllers should take adequate technical and organizational measures to ensure that they can receive and handle in a timely manner the access requests they receive from data subjects. In the words of the EDPB:

> *The controller should provide appropriate and user-friendly communication channels that can easily be used by the data subject*.[35]

---

[29] See Zalaris email to Datatilsynet dated 2 December 2021.
[30] Ibid.
[31] EDPB, Guidelines 01/2022 on data subject rights - Right of access (Version 1.0, Adopted on 18 January) (hereinafter "EDPB Guidelines on the Right of Access"), para. 55.
[32] See: <https://web.archive.org/web/20201123184817/https://zalaris.com/privacy/privacy-policy/#>. All web links provided in this letter were last accessed on 3 March 2022.
[33] See complainant's email to Datatilsynet dated 28 September 2021 (stating: "due to Art.15 'the data subject shall have the right to obtain from the controller'. That's what I had done! [redacted] is the controller and have to answer. So he broke the law!").
[34] Kuner et al., *The EU General Data Protection Regulation (GDPR): A Commentary* (OUP 2020), p. 149.
[35] EDPB Guidelines on the Right of Access, p. 2.

This means that, although controllers remain free to decide which specific communication channel should be used for submitting access requests, they must ensure that the communication channel they implement is easy to use and effective. Thus, if a controller decides to receive access requests via email, it must make sure that the email account it uses for this purpose implements state-of-the-art anti-spam protection—which does not treat legitimate access requests as spam—and/or that it monitors the spam folder on a regular basis to identify the presence of possible legitimate access requests. Effective anti-spam solutions (e.g., CAPTCHA solutions) do exist and should be adequately considered by the controller, in accordance with its accountability obligations under the GDPR.[36]

In the present case, Zalaris' anti-spam solution failed to "facilitate" the exercise of the right under Article 15 GDPR, in breach of Article 12(2) GDPR, as it treated a legitimate access request as spam, leading to such a request remaining unanswered for almost 3 months.

Nonetheless, we consider such an infringement to be minor,[37] for the following reasons:

- It appears to have affected a single data subject, as—to date—Datatilsynet has not received any other complaints concerning Zalaris' compliance with Articles 12(2) and 15 GDPR;

- After Datatilsynet's inquiry, Zalaris discontinued the use of the email address which treated the complainant's access request as spam, and embedded a new communication channel with a CAPTCHA solution in its privacy policy to be used for sending data protection inquiries;[38] and

- Although Zalaris did not respond to the complainant's access request submitted on 28 September 2021 within the standard statutory one month period—as it should have done under Article 12(3) GDPR—the company did respond on 22 December 2021 within the maximum 3 months period envisaged by Article 12(3) GDPR.

In light of the above, Datatilsynet considers that—in the present case—it is not warranted to issue any corrective measures for this infringement, and considers this specific matter to be settled.

6.2. Zalaris' Failure to Provide All of the Information Required under Article 15 GDPR

Under Article 15(1) (a) to (h) and 15(2) GDPR, data subjects are entitled to obtain from the controller specific information regarding the processing of their personal data. In his access request, the complainant required Zalaris to provide him with essentially all of the information that he is entitled to obtain under Article 15(1) (a) to (h) and 15(2) GDPR. Indeed, he requested:

[36] Arts. 5(2) and 24 GDPR.
[37] Cf. rec. 148 GDPR.
[38] See: <https://zalaris.com/privacy/privacy-policy/>.

• *Information about Automated Decision Logic if applicable*
• *Information about the Right of correction and limitation*
• *Information about the Right to complaint*
• *The name and contact data of Controller*
• *The name and contact data of Data protection officer*
• *The Data Protection Guarantee if applicable*
• *A complete copy of personal data in an easily visible, intelligible and clearly legible manner*
• *The purposes of processing*
• *The period of storage*
• *The categories of personal data*
• *The recipients of data transfer*
• *The data source* […].[39]

Zalaris responded to such a request essentially by sending a copy of—at least some of—the personal data of the complainant that are being processed by the company, and a copy of the company's privacy policy applicable to employees' data.[40]

While Zalaris' privacy policy does provide some of the information requested by the complainant, it does not appear to be always sufficiently granular to allow the complainant to understand and assess all of the processing operations actually carried out with regard to his personal data. As noted by the EDPB:

> *In order to comply with Art. 15(1)(a) to (h) and 15(2), controllers may carefully use text modules of their privacy notice as long as they make sure that they are of adequate actuality and preciseness with regards to the request of the data subject. Before or at the beginning of the data processing, some information, such as the identification of specific recipients or the specific duration of the data processing, will often only be possible in general terms. Furthermore, privacy notices as well as records of processing activities generally relate to processing concerning all data subjects and are often not tailored to the situation of a specific data subject. Some information, like for example the right to complain to a supervisory authority (see Art. 15(1)(f)), does not change depending on the person making the access request. Therefore, it may be communicated in general terms as it is also done in the privacy notice. Other types of information, such as the information on recipients, on categories and on the source of the data may vary depending on who makes the request and what the scope of the request is. In the context of an access request under Art. 15, any information on the processing available to the controller may therefore have to be updated and tailored for the processing operations actually carried out with regard to the data subject making the request. Thus, referring to the wording of its privacy policy would not be a sufficient way for the controller to give information required by Art. 15(1)(a) to (h) and (2) unless the «tailored» information is the same as the «general» information.*[41]

[39] See complainant's email to Zalaris dated 28 September 2021.
[40] Ibid.
[41] EDPB Guidelines on the Right of Access, para. 111.

In our view, by simply sending a copy of its privacy policy to the complainant, Zalaris has not provided sufficient information about the following:

- Purposes of the processing (Article 15(1)(a)). Zalaris' privacy policy simply states: "The purpose of Zalaris ASA's processing of personal data is primarily ensuring that we take care of you as an employee and the fulfillment of the obligations we have undertaken to implement the contract with you. We will also process personal data to the extent that the law imposes or gives us access to such processing or when you have consented to such processing. In addition to this, personal data is processed for the following purposes: […] Answer any incoming inquiries."[42] However, it would appear that Zalaris processes the personal data of the complainant also for other purposes (e.g. establishment, exercise or defence of legal claims against the complaint; performance of a settlement agreement with the complainant, etc.) which are not mentioned in the privacy policy. As noted by the EDPB, "Information on the purposes according to Art. 15(1)(a) needs to be specific as to the precise purpose(s) in the actual case of the requesting data subject. It would not be enough to list the general purposes of the controller without clarifying which purpose(s) the controller pursues in the current case of the requesting data subject."[43]

- Categories of personal data concerned (Article 15(1)(b)). Zalaris' privacy policy does not provide information on what kinds of personal data are being processed other than by stating that "Name, phone number, email address and any personal information that may result from the inquiry."[44] As noted by the EDPB, "Information on categories of data (Art. 15(1)(b)) […] may also have to be tailored to the data subject's situation. […]. If a request of access is made on the basis of Art. 15 GDPR, the data subject who makes the request must, in addition to the access to the actual data being processed (component 2), in line with Art. 15(1)(b) also be informed as to the specific categories of data which are being processed in the specific case (e.g. only e-mail address, but not the telephone number)."[45]

- Storage period(s) (Article 15(1)(d)). Zalaris' privacy policy merely states: "We will delete or anonymize personal data about you when the purpose of the specific processing is fulfilled, unless the personal data is or may be kept beyond this as a consequence of a legal requirement. This means, for example, that personal data we process on the basis of your consent will be deleted if you withdraw your consent. Personal information we process to fulfill an agreement with you will be deleted when the agreement is fulfilled and all obligations arising from the agreement are fulfilled. Zalaris has established archiving and deletion rules."[46] This information does not enable the data subject to assess, on the basis of his own situation, what the retention period will be for specific data/purposes. Indeed, as noted by the EDPB, "The information given by the controller has to be precise enough for the data subject to know how long

[42] See Regulation of Zalaris ASA's processing of personal data.
[43] EDPB Guidelines on the Right of Access, para. 112.
[44] See Regulation of Zalaris ASA's processing of personal data.
[45] EDPB Guidelines on the Right of Access, para. 113.
[46] See Regulation of Zalaris ASA's processing of personal data.

> the data relating to the data subject will continue to be stored. If it is not possible to specify the time of deletion, the duration of storage periods and the beginning of this period or the triggering event (e.g. termination of a contract, expiration of a warranty period, etc.) shall be specified."[47] This is particularly relevant in this case, given that the employment contract with the complainant has already been terminated.

In contrast, contrary to what has been claimed by the complainant,[48] the privacy policy seems to provide sufficient information on recipients (Article 15(1)(c)),[49] the existence of the right to rectification, erasure, restriction of processing and to object to such processing (Article 15(1)(e)),[50] the right to lodge a complaint with a supervisory authority (Article 15(1)(f)),[51] the source of the personal data (Article 15(1)(g)),[52] automated decision-making (Article 15(1)(h)),[53] and international transfers (Article 15(2)).[54]

Further, it appears that Zalaris has not provided the complainant with a copy of *all* of his personal data that are being processed by the company. For instance, Zalaris denied to grant access to the complainant's personal data contained in documents regarding the purchase/sale of ROC Ltd on the basis of the following:

> *Zalaris ASA signed contractual agreements with you as a commercial party and seller of shares in ROC Ltd, before you became an employee through ROC Deutschland*

[47] EDPB Guidelines on the Right of Access, para. 116.
[48] See complainant's email to Zalaris dated 2 March 2022.
[49] Zalaris' privacy policy specifies that "Zalaris ASA uses the following data processors: Telecomputing (IT Supplier), Cut-e (Assessment tests), Meditor (Backgrund checks), Netigate (invitations to events, internal temperature index survey)" (See Regulation of Zalaris ASA's processing of personal data). We assume that these are the only relevant recipients. If that is not the case, Zalaris should also provide the complainant with complete information about recipients.
[50] Zalaris' privacy policy states: "you may require access, correction or deletion of the personal information we process about you. You also have the right to demand us to limit the processing, to object to the processing, and request data portability". See Regulation of Zalaris ASA's processing of personal data.
[51] Zalaris' privacy policy states: "The Data Protection Authority's task is to check that the privacy policy is being followed. Any complaints about Zalaris ASA's processing of personal data that concerns you may be directed to your local Data Protection Authority or directly to the Norwegian Data Protection Authority." See Regulation of Zalaris ASA's processing of personal data.
[52] Under Article 15(1)(g) GDPR, information on the source of personal data must be provided only insofar as they are "available" and "where the personal data are not collected from the data subject". We understand that this is not applicable in this case. However, if Zalaris processed personal data that it has not collected from the complainant, it should provide him with any available information as to their source.
[53] Under Article 15(1)(h) GDPR, information on automated decision-making must be provided only insofar as it "exists". This does not seem to be applicable in this case, as it does not seem that Zalaris engages in any automated decision-making with respect to the complainant.
[54] Zalaris' privacy policy states: "We transfer personal data to countries outside the EU/EEA area in the following situations: According to DPA and internal agreements employee data management related to new hire, changes, terminations, payroll, travel etc. for Zalaris employees are handled by the HR team in India. The legal basis for such transfer is the Zalaris DPA" (See Regulation of Zalaris ASA's processing of personal data). Based on this, we understand that Zalaris does not transfer the complainant's personal data outside the EU/EEA, as the complainant's is no longer an employee of Zalaris in Germany. Thus, Article 15(2) does not seem to be applicable in this case, as that provision only applies "where personal data are transferred to a third country". However, if Zalaris transfers the personal data of the complainant outside the EU/EEA, the company should provide the complainant with the information required under Article 15(2) GDPR.

> *GmbH. This is commercial documentation archived in our contract archive with you as the seller and Zalaris as the buyer. We do not consider this material in the context of GDPR related to your employment with Zalaris.* […]. (emphasis added).[55]

In this regard, we note that the fact that the personal data that Zalaris processes are *not* related to the employment relationship with the complainant is not *per se* sufficient to deny access to such data. As noted by the EDPB:

> *If no limits or restrictions apply, data subjects are entitled to have access to all data processed relating to them, or to parts of the data, depending on the scope of the request* […] *The obligation to provide access to the data does not depend on the type or source of those data. It applies to its full extent even in cases where the requesting person had initially provided the controller with the data, because its aim is to let the data subject know about the actual processing of those data by the controller.*[56]

Thus, Zalaris must provide the complainant with a copy of *all* of his personal data that are being processed by the company, unless Zalaris is able to demonstrate that one of the exceptions set out in Articles 12(5) and 15(4) GDPR or Article 16 of the Norwegian Personal Data Act applies to such data.

However, this does not mean that Zalaris must necessarily provide a copy of the entire documents in which such personal data are contained. In this regard, the EDPB noted:

> […] *access to the data under Art. 15(1) comprises complete information on all data and cannot be understood as granting only a summary of the data. At the same time, the obligation to provide a copy is not designed to widen the scope of the right of access: it refers (only) to a copy of the personal data undergoing processing, not necessarily to a reproduction of the original documents* […].[57]

It further opined:

> […] *the GDPR expressly contains an obligation to provide the data subject with a copy of the personal data undergoing processing. This, however, does not mean that the data subject always has the right to obtain a copy of the documents containing the personal data, but an unaltered copy of the personal data being processed in these documents. Such copy of the personal data could be provided through a compilation containing all personal data covered by the right of access as long as the compilation makes it possible for the data subject to be made aware and verify the lawfulness of the processing.*[58]

Therefore, we deem it necessary to order Zalaris, pursuant to Article 58(2)(d) GDPR, to provide the complainant with all of the information he requested and is entitled to receive pursuant to Article 15 GDPR. In particular, Zalaris shall provide the complainant with complete

[55] See Zalaris' email to the complainant dated 2 March 2022.
[56] EDPB Guidelines on the Right of Access, para. 19.
[57] Ibid., para. 23.
[58] Ibid., para. 150.

information on the following: (1) purposes of the processing; (2) categories of personal data concerned; and (3) relevant storage period(s). Further, Zalaris must provide the complainant with a copy of *all* of his personal data that are being processed by the company and have not yet been sent to the complainant, unless Zalaris is able to demonstrate that one of the exceptions set of in Articles 12(5) and 15(4) GDPR or Article 16 of the Norwegian Personal Data Act applies to such data.

The information and data provided to the complainant shall be understandable and clear to the complainant (see Article 12(1) GDPR). This entails—among other things—that Zalaris might need to supply the complainant with additional information that explains the data provided, if such data are not immediately intelligible. In this regard, the EDPB noted:

> *The requirement that the information is "intelligible" means that it should be understood by the intended audience, whilst keeping in mind any special needs that the data subject might have that is known to the controller. Since the right of access often enables the exercise of other data subject rights, it is crucial that the information provided is made understandable and clear. This is because data subjects will only be able to consider whether to invoke their right to, for example, rectification under Art. 16 once they know what personal data are being processed, for what purposes etc. As a result, the controller might need to supply the data subject with additional information that explains the data provided. It should be emphasised that the complexity of data processing puts an obligation on the controller to provide the means to make the data understandable and could not be used as an argument to limit the access to all data. Similarly, the obligation on the controller to provide data in a concise manner cannot be used as an argument to limit access to all data.*[59]

For completeness purposes, it should be noted that—contrary to what was argued by the complainant[60]—Zalaris may provide the relevant information in English, as the complainant's access request was written in English, and the complainant has been corresponding with Zalaris in English, which shows that he is sufficiently familiar with the English language. Further—also contrary to what was argued by the complainant[61]—the information does not need to be provided in a machine-readable format. In this regard, the EDPB opined:

> *It should be noted that the provisions on format requirements are different regarding the right of access and the right of data portability. Whilst the right of data portability under Art. 20 GDPR requires that the information is provided in a machine readable format, the right to information under Art. 15 does not. Hence, formats that are considered not to be appropriate when complying with a data portability request, for example pdf-files, could still be suitable when complying with a request of access*.[62]

While the present inquiry has only focused on Zalaris' compliance with Articles 12 and 15 GDPR in connection with the above-mentioned complaint, this is without prejudice to the

[59] Ibid., para. 139.
[60] See complainant's email to Zalaris dated 2 March 2022.
[61] Ibid.
[62] EDPB Guidelines on the Right of Access, para. 154.

possibility of opening future inquiries to assess Zalaris' compliance with its broader obligations under the GDPR, including with the transparency requirements imposed by Articles 5(1)(a) and 13 GDPR as well as the data deletion requirements laid down in Articles 5(1)(e) and 17.

7. Right of Appeal

As this decision has been adopted pursuant to Article 56 and Chapter VII GDPR, the present decision may be appealed before Oslo District Court ("Oslo tingrett") in accordance with Article 78(1) GDPR, Article 25 of the Norwegian Data Protection Act, and Article 4-4(4) of the Norwegian Dispute Act.[63]

Kind regards

Tobias Judin
Head of International

Luca Tosoni
Senior Legal Advisor

This letter has electronic approval and is therefore not signed

[63] Act of 17 June 2005 no. 90 relating to mediation and procedure in civil disputes (Lov om mekling og rettergang i sivile tvister (tvisteloven)).