Datatilsynet

[redacted]

*Exempt from public disclosure:*
*Offl. § 13, jf. Personopplysningsloven § 24 første led 2. punktum*

| Your reference | Our reference | Date |
|---|---|---|
| | 20/01693-16 | 11.11.2022 |

## Final Decision - Equinor ASA

| | |
|---|---|
| **IMI article 56 entry number:** | 363967 |
| **IMI case register:** | 427314 |
| **National case reference:** | NO SA: 20/01693 & 19/03512 |
| **Controller:** | Equinor ASA |
| **Date of complaint:** | 14 November 2019 |

We refer to the abovementioned cross-border case where Datatilsynet (the Norwegian Data Protection Authority, hereinafter "**NO SA**") has been identified as the lead supervisory authority pursuant to Article 56(1) GDPR[1]. The data protection authorities in the following countries have indicated that they are supervisory authorities concerned pursuant to Article 4(22) GDPR: Belgium, Denmark, France, Germany and the Netherlands.

The NO SA adopts the following decision:

> *The NO SA rejects the complaint submitted against Equinor ASA (Case 20/01693 & 19/03512).*

### Factual Background

Complaint

On 14 November 2019, the NO SA received a complaint against Equinor ASA ("**Equinor**"). The complainant alleged:

[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 L 119/1.

- Equinor had not complied with the complainants request to have their personal data deleted in time, as Equinor deleted the personal data 38 days after having received the complainant's request for deletion;
- Equinor outsource their recruitment process to the British company Alexander Mann Solutions and job seekers do not have control over their data and do not know what is saved on Alexander Mann Solutions' servers, where, how long, how it is processed, how it is used etc.

On 26 January 2020, the NO SA received further correspondence from the complainant with further information in relation to their complaint against Equinor. The complainant further alleged:

- Equinor uses the job seeker platform "www.peopleclick.eu", and the websites of Alexander Mann Solutions and www.peopleclick.eu are unsecure as they use http and not https.

On 13 April 2022, the NO SA received further correspondence from the complainant with updated information, the salient points of which were:

- Jobseekers using peopleclick cannot update or delete their information (applications, CV, e-mail address), nor can jobseekers delete their account;
- Equinor's privacy policy does not give jobseekers open and satisfactory information about the recruitment process, recruitment platform, recruitment partners etc. that are used by Equinor.

Investigation by the NO SA

From the documentation received from the complainant, the NO SA considers that the complaint covers the following issues:

- Transparent information, communication and modalities for the exercise of the rights of the data subject (Article 12 GDPR)
- Information to be provided where personal data are collected from the data subject (Article 13 GDPR)
- The right to erasure (Article 17 GDPR)
- Security of processing (Article 32 GDPR) in relation to the encryption of data in transit regarding Equinor's recruitment management system

The NO SA notes from the documentation provided by the complainant that the complainant had sent an e-mail to Equinor on 11 June 2019 requesting deletion of their profile. Equinor responded to the complainant on 10 July 2019 confirming that their profile had been deleted. The NO SA cannot find a breach of Articles 12(3) or 16 GDPR in this regard, as Equnior responded to the complainant and deleted the complainant's personal data within 1 month from the complainant's request. The NO SA did not take any further action with regard to the complainant's allegations in relation to the deletion request.

On 6 April 2022, the NO SA sent Equinor an order to provide information requesting them, in relation to the period between around summer 2019 and January 2020 (the relevant period) and currently to:

- Describe and explain Equinor's use of Alexander Mann Solutions and the platform «www.peopleclick.eu» in Equinor's recruitment process, including
  - The relationship between Peopleclick, AMS and Equinor
  - Which processing activities AMS carries out on behalf of Equinor, and how Peopleclick is used in this regard
  - How you have taken into consideration the security of processing in relation to the relevant processing activities pursuant to Article 32
  - Whether and how you have ensured that job applicants are provided with information about the relevant processing activities pursuant to Articles 12, 13 and if applicable 14, including in relation to the relevant processing activities.

On 19 May 2022, Equinor responded to the NO SA's order to provide information dated 6 April 2022. The salient points from such response are detailed below:

- Equinor use both Alexander Mann Solutions AS ("**AMS**") and Peoplefluent Ltd ("**PeopleFluent**") as data processors in their general external and internal recruitment process. Equinor further provided the NO SA with copies of their data processing agreements with both AMS and PeopleFluent.
- Equinor has since 2012 utilised a recruitment management system delivered as a software as a service solution by PeopleFluent (the "**RMS**"). The personal data for the recruitment processes are stored and processed in the RMS.
- AMS has since 2014 been Equinor's main supplier of recruitment assistance. Only authorised personnel from AMS have role-based access to the RMS to carry out their tasks, meaning they have access to the RMS and all data stored in the system. Access to the RMS is controlled by Equinor, and the access is removed when any resources from AMS leave the Equinor account. AMS does not process personal data in their own systems on behalf of Equinor, but rather have access to the RMS.
- Equinor states that the RMS is and was during the relevant time period encrypted. PeopleFluent use encryption protocols for data at rest and in back-up, as well as transport layer security (TLS) for data in transfer. Equinor provided the NO SA with PeopleFluent's security documentation overview as well as extracts of audits of the RMS between 1 October 2018 and 31 October 2020 in relation to this matter showing that no exceptions were noted in relation to encryption in transit or at rest.
- Equinor uses a layered approach to informing data subjects about the processing of personal data it carries out, depending on the purposes for the processing and whether or not the data subject is an internal or external applicant. Equinor provided the NO SA with copies of privacy policies in force in the relevant period and currently, as well as explained with screenshots how such privacy policies are displayed to users.
- Job candidates applying for positions with Equinor can view their personal data and application status in the PeopleFluent system by logging in to their profile. Personal

data is automatically deleted after 12 months, but candidates can request to have their data deleted sooner by contacting Equinor through Equinor's contact form.

**Legal Background**

Pursuant to Article 12(1), (2) and (3) GDPR:

***Transparent information, communication and modalities for the exercise of the rights of the data subject***

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.*

   *...*

Pursuant to Article 13 GDPR, as adapted pursuant to Annex XI of the EEA Agreement as amended by the Decision of the EEA Joint Committee No 154/2018 of 6 July 2018:

***Information to be provided where personal data are collected from the data subject***

1. *Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:*

   a. *the identity and the contact details of the controller and, where applicable, of the controller's representative;*

b. *the contact details of the data protection officer, where applicable;*
c. *the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;*
d. *where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;*
e. *the recipients or categories of recipients of the personal data, if any;*
f. *where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission* [applicable pursuant to the EEA Agreement]*, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.*

2. *In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:*

   a. *the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;*
   b. *the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;*
   c. *where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;*
   d. *the right to lodge a complaint with a supervisory authority;*
   e. *whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;*
   f. *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.*

3. *Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.*

4. *Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.*

Pursuant to Article 17 (1)(a) and (b) GDPR:

***Right to erasure ('right to be forgotten')***

1. *The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:*

    a. *the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;*
    b. *the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;*

*...*

Pursuant to Article 32(1) and (2) GDPR:

***Security of processing***

1. *Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:*

    a. *the pseudonymisation and encryption of personal data;*
    b. *the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;*
    c. *the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;*
    d. *a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.*

2. *In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.*

    *...*

**Findings**

The complainant alleged that Equinor had not complied with their request to have their personal data deleted in time as Equinor deleted the personal data 38 days after having received the complainant's request for deletion. In addition, the complainant alleged that jobseekers using "peopleclick" cannot update or delete their information (applications, CV, e-mail address), nor

can jobseekers delete their account. The NO SA has interpreted this allegation as being related to Equinor's RMS. Based on the documentation provided by the complainant themselves, it appears that the time between the complainant requesting deletion of their personal data and Equinor responding to the complainant confirming that their personal data had been deleted was less than one month. The NO SA also notes that Equinor's privacy policies, in force both in the relevant period and currently, tell data subjects that they may update or delete their personal data as well as how they may contact Equinor, as controller, to exercise these rights. The NO SA cannot see that Equinor has breached Articles 12, 13 or 17 GDPR, and therefore rejects these parts of the complaint.

The complainant alleged that Equinor outsource their recruitment process to the British company Alexander Mann Solutions and job seekers do not have control over their data and do not know what is saved on Alexander Mann Solutions' servers, where, how long, how it is processed, how it is used etc. In addition, the complainant alleged Equinor's privacy policy does not give jobseekers open and satisfactory information about the recruitment process, recruitment platform, recruitment partners etc. that are used by Equinor. Based on the documentation provided by Equinor, PeopleFluent and AMS are processors of Equinor. PeopleFluent is specifically mentioned in Equinor's recruitment privacy policy in force both in the relevant period and currently, and AMS would fall under the category of "external recruitment / employment verification service providers contracted by the Equinor Group" mentioned in such privacy policy. The NO SA notes Equinor's general or recruitment-specific privacy policies, in force in the relevant period and currently, mention amongst other things what personal data are stored and where, for how long, and why and how it is processed and used - which the complainant specifically stated were missing. In addition, the NO SA has been provided with screenshots showing that the privacy policy specific to recruitment is accessible prior to creating an account in Equinor's RMS, and one must confirm that this privacy policy has been read before creating an account. The NO SA therefore rejects these parts of the complaint.

The complainant alleged that Equinor uses the job seeker platform "www.peopleclick.eu", and the websites of Alexander Mann Solutions and www.peopleclick.eu are unsecure as they use http and not https. Equinor provided the NO SA with PeopleFluent's security documentation overview as well as extracts of audits of the RMS between 1 October 2018 and 31 October 2020 in relation to this matter showing that no exceptions were noted in relation to encryption in transit or at rest. As such, the NO SA cannot find any substantiation to this matter raised by the complainant, and Equinor has provided the NO SA with evidence to the contrary of such allegation. The NO SA therefore rejects this part of the complaint.

In light of the above, the NO SA considers that the subject matter of the complaint has been investigated to the extent appropriate in accordance with Article 57(1)(f) GDPR. The NO SA has not been able to identify a breach of the GDPR based on such investigation, and the complaint as a whole is therefore rejected.

**Right of appeal**
As this decision has been adopted by the NO SA pursuant to Article 56 and Chapter VII GDPR, it is not possible to appeal it before the Norwegian Privacy Appeals Board pursuant to Section

22 of the Norwegian Data Protection Act. This decision may nevertheless be appealed before the Norwegian courts in accordance with Article 78(1) GDPR.

Kind regards

Tobias Judin
Head of Section

Sebastian Forbes
Legal Adviser

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

Copy to: Equinor ASA