

NOYB - European Center for Digital Rights  
Goldschlagstrasse 172/4/3/2 1140 Wien

20 April 2023

J.No. 2021-7329-0052  
Doc.no. 571264  
Caseworker  
[REDACTED]

---

## Complaint concerning the processing of personal data

The Danish Data Protection Agency (“Danish DPA”) hereby returns to the case where the organisation None of Your Business on behalf of [REDACTED] (“the complainant”) on 17 August 2020 has filed a complaint with the Danish DPA that BoligPortal A/S (“BoligPortal”) has transferred personal data of the complainant to the United States in connection with the complainant’s visit to BoligPortal’s website on 12 August 2020.

**The Danish Data  
Protection Agency**  
Carl Jacobsens Vej 35  
2500 Valby  
Denmark  
T 3319 3200  
dt@data.ilsynet.dk  
datatilsynet.dk

VAT No. 11883729

Firstly, the Danish DPA notes that the supervisory authority by this decision has only considered BoligPortal’s processing of personal data through its use of “Facebook Business Tools”. As such, the Danish DPA has not considered the company’s potential processing of personal data using other third-party tools.

Secondly, the Danish DPA notes that the supervisory authority by this decision has only considered Boligportal’s processing of personal data of the complainant through the use of Facebook Business Tools. As such, the decision does not take a position on neither Meta Platforms Ireland Limited (formerly Facebook Ireland Limited, hereinafter Meta Ireland) nor Meta Platforms, Inc. (formerly Facebook, Inc., hereinafter Meta Platforms) processing of personal data.

Finally, the Danish DPA notes that since the complaint was filed, Boligportal has provided additional documentation to demonstrate that the processing has been carried out in accordance with the General Data Protection Regulation. Additionally, Meta Ireland has changed the terms under which the company provides its Facebook Business Tools.

On this basis, the Danish DPA has by this decision firstly assessed whether the processing of personal data of the complainant on 12 August 2020 occurred in compliance with the General Data Protection Regulation, and secondly, whether Boligportal’s current processing of personal data of website visitors complies with the General Data Protection Regulation.

### 1. Decision and order

Upon reviewing the case, the Danish DPA finds that there are grounds for **seriously reprimanding** Boligportal for not demonstrating that its processing of personal data of the complainant on 12 August 2020 was carried out in compliance with the General Data Protection

Regulation (“GDPR”)<sup>1</sup> and for not demonstrating that its current processing of personal data of website visitors takes place in compliance with Article 26 GDPR pursuant to Articles 5(1)(a), 5(2), and 24(1) GDPR.

Firstly, the Danish DPA considers that the supervisory authority cannot adopt a decision specifically on Boligportal’s possible transfer of personal data of the complainant to the United States as there is disagreement between the parties as to whether personal data of the complainant was in fact transferred to the United States.

However, the fact that the Danish DPA cannot decide on the possible transfer of personal data of the complainant to the United States gives the supervisory authority rise to assess whether Boligportal has complied with its obligations under the GDPR, in particular its obligation to demonstrate its compliance with the GDPR under Articles 5(1)(a), 5(2), and 24(1).

In this regard, the Danish DPA considers that – at the time of the complainant’s visit to Boligportal’s website on 12 August 2020 – there has been an insufficient allocation of roles and responsibilities between Boligportal and Meta Ireland in light of the processing of personal data that occurred.

Considering the processing activity and the purposes for which Boligportal, per its own submission as detailed in section 3.3 below, has processed the complainant’s personal data, the parties must be considered as joint controllers for the processing of personal data of the complainant.

In view of this, and considering that at the time of the complainant’s visit to Boligportal’s website there was no arrangement pursuant to Article 26 GDPR in place which in a transparent manner determined the parties’ respective responsibilities for compliance with the GDPR, the Danish DPA finds that Boligportal has not demonstrated that its processing of personal data of the complainant was carried out in compliance with Article 26 GDPR pursuant to Articles 5(1)(a), 5(2), and 24(1).

Additionally, the Danish DPA finds that it is unclear from the current arrangement concluded between Boligportal and Meta Ireland as joint controllers pursuant to Article 26 GDPR whether personal data of website visitors is processed by means located outside the EU/EEA and where, including, if applicable, by the use of processors outside the EU/EEA in the context of processing activities under the parties’ joint controllership and, consequently, which party is responsible for ensuring compliance with Article 44 GDPR.

As such, the Danish DPA considers that Boligportal has not, in general, demonstrated that its current processing of personal data takes place in compliance with Articles 26 GDPR pursuant to Articles 5(1)(a), 5(2), and 24(1) GDPR, as Boligportal has not fully identified whether personal data of visitors to its website is processed by means located outside the EU/EEA and where including, if applicable, by the use of processors outside the EU/EEA, in the context of the processing activities for which the Boligportal and Meta Ireland are joint controllers.

On this basis, the Danish DPA **orders** Boligportal to bring its processing of personal data into compliance with Articles 5(1)(a), 5(2), 24(1) and 26 GDPR and to be able to demonstrate compliance with these provisions.

---

<sup>1</sup> 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).

Boligportal shall comply with the order **no later than 18 May 2023**. The Danish DPA requests confirmation and documentation that the order has been complied with no later than the same date.

In the view of the Danish DPA, this order may *inter alia* be complied with by clarifying the allocation of roles and responsibilities between Boligportal and Meta Ireland, so that it is apparent from the arrangement between the parties whether personal data of website visitors in the context of the joint controllership is processed by means located outside the EU/EEA including, if applicable, by the use of processors outside the EU/EEA and, consequently, how Article 44 GDPR is complied with as well as which party must ensure compliance with that provision. Alternatively, compliance with the order may be done by ceasing the processing activity in question.

The Danish DPA notes that the above-mentioned suggested solutions are not exclusive and do not constitute the only options for how Boligportal may comply with the order. As the controller, Boligportal has full freedom of choice in accordance with Articles 5(2) and 24(1) GDPR as to how it demonstrates its compliance with the GDPR.

This order is notified pursuant to Article 58(2)(d) GDPR.

According to Section 41(2)(4) of the Danish Data Protection Act, a fine or imprisonment of up to 6 months shall be imposed on persons who fail to comply with an order issued by the Danish DPA pursuant to Article 58(2)(d) GDPR.

Below is a detailed examination of the case and a statement of reasons for the Danish DPA's decision.

## **2. Facts of the case**

On 12 August 2020, the complainant visited Boligportal's website. During the visit, the complainant was logged into her account on Facebook which is a social media platform operated by Meta Ireland.

Boligportal has embedded "Facebook Connect" tools on its website which are the subject of the complaint. The Danish DPA understands that "Facebook Connect" refers to several tools provided by Meta Ireland, in particular "Facebook Login" and "Facebook Pixel".

The tools are provided by Meta Ireland to website operators under the terms "*Facebook Business Tools Terms*" and "*Facebook Data Processing Terms*". Since the complainant's visit to Boligportal's website on 12 August 2020, the terms have been updated on 31 August 2020.

### **2.1. Meta Ireland's Terms**

Meta Ireland's "Facebook Business Terms" of 26 December 2019, which were in force at the time of complainant's visit to Boligportal's website *inter alia* state the following:

"The Facebook Business Tools are a subset of Facebook Products that we provide to help website owners and publishers, developers, advertisers, business partners (and their customers) and others integrate, use and exchange information with Facebook. The Facebook Business Tools include APIs and SDKs, the Facebook Pixel, social plugins such as the Like and Share buttons, Facebook Login and Account Kit, as well as other platform integrations, plugins, code, specifications, documentation, technology and services. By clicking "Accept" or using any of the Facebook Business Tools, you agree to the following:

#### 1. Sharing Personal Data with Facebook

- a. You may use the Facebook Business Tools to send personal data to us about your customers and users (“Customer Data”). Depending on the Facebook Products you use, Customer Data may include:
- i. “Contact Information” consists of information that personally identifies individuals, such as names, email addresses, and phone numbers that we use for matching purposes only. We will hash Contact Information that you send to us via a Facebook javascript pixel for matching purposes prior to transmission. When using a Facebook image pixel or other Facebook Business Tools, you or your service provider must hash Contact Information in a manner specified by us before transmission.
  - ii. “Event Data” includes other information you share about your customers and the actions they take on your websites and apps or in your stores, such as visits to your sites, installations of your apps, and purchases of your products.

[...]

## 2. Use of Customer Data

- a. We will use Customer Data for the purposes depending on which Facebook Company Products you choose to use:
- i. **Contact Information for Matching**
    1. You instruct us to process the Contact Information solely to match the Contact Information against Facebook’s or Instagram’s user IDs (“Matched User IDs”), as well as to combine those user IDs with corresponding Event Data. We will delete Contact Information following the match process.
  - ii. **Event Data for Measurement and Analytics Services**
    1. You instruct us to process Event Data (a) to prepare reports on your behalf on the impact of your advertising campaigns and other online content (“Campaign Reports”) and (b) to generate analytics and insights about your customers and their use of your apps, websites, products and services (“Analytics”).
    2. We grant to you a non-exclusive and non-transferable license to use the Campaign Reports and Analytics for your internal business purposes only and solely on an aggregated and anonymous basis for measurement purposes. You will not disclose the Campaign Reports or Analytics, or any portion thereof, to any third party, unless otherwise agreed to in writing by us. We will not disclose the Campaign Reports or Analytics, or any portion thereof, to any third party without your permission, unless (i) they have been combined with Campaigns Reports and Analytics from numerous other third parties and (ii) your identifying information is removed from the combined Campaign Reports and Analytics.
  - iii. **Event Data to Create Targetable Audiences**
    1. We may process the Event Data to create audiences (including Website Custom Audiences, Mobile App Custom Audiences and Offline Custom Audiences) that are grouped together by common Event Data, which you may use to target ad campaigns. In our sole discretion, we may also allow you to share these audiences with other advertisers.
  - iv. **Event Data to Deliver Commercial and Transactional Messages**
    1. We may use the Matched User IDs and associated Event Data to help you to reach people with transactional and other commercial messages on Messenger and other Facebook Company Products.
  - v. **Event Data to Personalize Features and Content and to Improve and Secure the Facebook Products**
    1. We use Event Data to personalize the features and content (including ads and recommendations) we show people on and off our Facebook Company Products. In connection with ad targeting and delivery optimization, we will: (i) use your Event Data for delivery optimization only after aggregating such Event Data with other data collected from other advertisers or otherwise collected on Facebook Products; and (ii) not allow other advertisers or third parties to target advertising solely on the basis of your Event Data.

2. We may also use Event Data to promote safety and security on and off the Facebook Company Products, for research and development purposes, and to maintain the integrity of and to improve the Facebook Company Products.

[...]

#### 4. A note to EU and Swiss data controllers

- a. To the extent the Customer Data contain personal data which you process subject to the General Data Protection Regulation (Regulation (EU) 2016/679) (the "GDPR"), the parties acknowledge and agree that for purposes of providing matching, measurement, and analytics services described in Paragraphs 2.a.i and 2.a.ii above, that you are the data controller in respect of such personal data, and you have instructed Facebook Ireland Limited to process such personal data on your behalf as your data processor pursuant to these terms and Facebook's Data Processing Terms, which are incorporated herein by reference. "Personal data," "data controller," and "data processor" in this paragraph have the meanings set out in the Data Processing Terms."

Meta Ireland's "Data Processing Terms" (undated), which are incorporated into Meta Ireland's terms<sup>2</sup> by reference *inter alia* state the following:

"2. You agree that Facebook may subcontract its data processing obligations under these Data Processing Terms to a subprocessor, but only by way of a written agreement with the sub-processor which imposes obligations on the sub-processor no less onerous than as are imposed on Facebook under these Data Processing Terms. Where the sub-processor fails to fulfil such obligations, Facebook shall remain fully liable to you for the performance of that sub-processor's obligations. You hereby authorize Facebook to engage Facebook Inc. (and other Facebook Companies) as its sub-processor(s). Facebook shall notify you of any additional sub-processor(s) in advance. If you reasonably object to such additional sub-processor(s), you may inform Facebook in writing of the reasons for your objections. If you object to such additional subprocessor(s), you should stop using the Services and providing data to Facebook."

Meta Ireland's "Facebook Business Terms" of 31 August 2020<sup>3</sup>, which are the latest applicable terms *inter alia* state the following:

"When you use the Facebook Business Tools to send us or otherwise enable the collection of Business Tool Data (as defined in Section 1 below), these terms govern the use of that data.

#### **Background: Ad Products and other Business Tools**

We may receive Business Tool Data as a result of your use of Facebook ad products, in connection with advertising, matching, measurement and analytics. Those ad products include, but are not limited to, Facebook Pixel, Conversions API (formerly known as Server-Side API), Facebook SDK for App Events, Offline Conversions, App Events API and Offline Events API. We also receive Business Tools Data in the form of impression data sent by Facebook Social Plugins (for example the Like and Share buttons) and Facebook Login, and data from certain APIs such as Messenger Customer Match via the Send API. Facebook may also offer pilot, test, alpha, or beta programs from time to time through which you may provide Business Tool Data. Uses of Business Tools Data are described below.

By clicking "Accept" or using any of the Facebook Business Tools, you agree to the following:

1. Sharing Business Tool Data with Facebook
  - a. You may use the Facebook Business Tools to send us one or both of the following types of personal information ("Business Tool Data") for the purposes described in Section 2:
    - i. "Contact Information" is information that personally identifies individuals, such as names, email addresses, and phone numbers, that we use for matching purposes only. We will

---

<sup>2</sup> Printed by the complainant on 10 August 2020 from <https://www.facebook.com/legal/terms/dataprocessing>

<sup>3</sup> <https://www.facebook.com/legal/terms/businessstools>

hash Contact Information that you send to us via a Facebook JavaScript pixel for matching purposes prior to transmission. When using a Facebook image pixel or other Facebook Business Tools, you or your service provider must hash Contact Information in a manner specified by us before transmission.

- ii. "Event Data" is other information that you share about people and the actions that they take on your websites and apps or in your shops, such as visits to your sites, installations of your apps, and purchases of your products. While Event Data does include information collected and transferred when people access a website or app with Facebook Login or Social Plugins (e.g. the Like button), it does not include information created when an individual interacts with our platform via Facebook Login, Social Plugins, or otherwise (e.g. by logging in, or liking or sharing an article or song). Information created when an individual interacts with our platform via Facebook Login, Social Plugins, or otherwise is governed by the Platform Terms.
- iii. Note: for purposes of these Business Tool Terms, references in existing terms or agreements to "Customer Data" will now mean "Business Tool Data."

[...]

## 2. Use of Business Tool Data

- a. We will use Business Tool Data for the following purposes depending on which Facebook Business Tools you choose to use:

### i. **Contact Information for Matching**

- 1. You instruct us to process the Contact Information solely to match the Contact Information against user IDs ("Matched User IDs"), as well as to combine those user IDs with corresponding Event Data. We will delete Contact Information following the match process.

### ii. **Event Data for Measurement and Analytics Services**

- 1. You may instruct us to process Event Data (a) to prepare reports on your behalf on the impact of your advertising campaigns and other online content ("Campaign Reports") and (b) to generate analytics and insights about people and their use of your apps, websites, products and services ("Analytics").
- 2. We grant to you a non-exclusive and non-transferable license to use the Campaign Reports and Analytics for your internal business purposes only and solely on an aggregated and anonymous basis for measurement purposes. You will not disclose the Campaign Reports or Analytics, or any portion thereof, to any third party, unless otherwise agreed to in writing by us. We will not disclose the Campaign Reports or Analytics, or any portion thereof, to any third party without your permission, unless (i) they have been combined with Campaigns Reports and Analytics from numerous other third parties and (ii) your identifying information is removed from the combined Campaign Reports and Analytics.

### iii. **Event Data for Targeting Your Ads**

- 1. You may provide Event Data to target your ad campaigns to people who interact with your business. You may direct us to create custom audiences, which are groups of Facebook users based on Event Data, to target ad campaigns (including Website Custom Audiences, Mobile App Custom Audiences, and Offline Custom Audiences). Facebook will process Event Data to create such audiences for you. You may not sell or transfer these audiences, or authorize any third party to sell or transfer these audiences. Facebook will not provide such audiences to other advertisers unless you or your service providers share audiences with other advertisers through tools we make available for that

purpose, subject to the restrictions and requirements of those tools and our terms.

2. These terms apply to the use of Website Custom Audiences, Mobile App Custom Audiences, and Offline Custom Audiences created through Facebook's Business Tools. Customer List Custom Audiences provided through our separate custom audience feature are subject to the Customer List Custom Audience Terms.

**iv. Event Data to Deliver Commercial and Transactional Messages**

1. We may use the Matched User IDs and associated Event Data to help you reach people with transactional and other commercial messages on Messenger and other Facebook Company Products.

**v. Event Data to Improve Ad Delivery, Personalise Features and Content and to Improve and Secure the Facebook Products**

1. You may provide Event Data to improve ad targeting and delivery optimization of your ad campaigns. We may correlate that Event Data to people who use Facebook Company Products to support the objectives of your ad campaign, improve the effectiveness of ad delivery models, and determine the relevance of ads to people. We may use Event Data to personalize the features and content (including ads and recommendations) that we show people on and off our Facebook Company Products. In connection with ad targeting and delivery optimization, we will: (i) use your Event Data for delivery optimization only after aggregating such Event Data with other data collected from other advertisers or otherwise collected on Facebook Products; and (ii) not allow other advertisers or third parties to target advertising solely on the basis of your Event Data.
2. To improve the experience for people who use Facebook Company Products, we may also use Event Data to promote safety and security on and off the Facebook Company Products, for research and development purposes and to maintain the integrity of and to improve the Facebook Company Products.

[...]

**5. Additional Terms for Processing of Personal Information**

- a. To the extent the Business Tool Data contain Personal Information which you Process subject to the General Data Protection Regulation (Regulation (EU) 2016/679) (the "GDPR"), the following terms apply:
  - i. The parties acknowledge and agree that you are the Controller in respect of the Processing of Personal Information in Business Tool Data for purposes of providing matching, measurement and analytics services described in Sections 2.a.i and 2.a.ii above (e.g. to provide you with Analytics and Campaign Reports), and that you instruct Facebook Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, Dublin 2 Ireland ("Facebook Ireland") to Process such Personal Information for those purposes on your behalf as your Processor pursuant to these Business Tools Terms and Facebook's Data Processing Terms. The Data Processing Terms are expressly incorporated herein by reference and apply between you and Facebook Ireland together with these Business Tools Terms.
  - ii. Regarding Personal Information in Event Data referring to people's actions on your websites and apps which integrate Facebook Business Tools for whose Processing you and Facebook Ireland jointly determine the means and purposes, you and Facebook Ireland acknowledge and agree to be Joint Controllers in accordance with Article 26 GDPR. The joint controllership extends to the collection of such Personal

Information via the Facebook Business Tools and its subsequent transmission to Facebook Ireland in order to be used for the purposes set out above under Sections 2.a.iii to 2.a.v.1 (“Joint Processing”). For further information, click here. The Joint Processing is subject to the Controller Addendum, which is expressly incorporated herein by reference and applies between you and Facebook Ireland together with these Business Tools Terms. Facebook Ireland remains an independent Controller in accordance with Article 4(7) GDPR for any Processing of such data that takes place after it has been transmitted to Facebook Ireland.

- iii. You, as the case may be, and Facebook Ireland remain independent Controllers in accordance with Article 4(7) GDPR for any Processing of Personal Information in Business Tool Data under GDPR not subject to Sections 5.a.i and 5.a.ii.”

Meta Ireland’s “Controller Addendum” of 31 August 2020<sup>4</sup>, which are incorporated into Meta Ireland’s terms by reference *inter alia* state the following:

“This Controller Addendum applies when it is expressly incorporated by reference into terms for Facebook Products, such as the Facebook Business Tools Terms (any such terms, “**Applicable Product Terms**”, any covered Facebook Products, “**Applicable Products**”). Capitalized terms used but not defined in this Controller Addendum have the meanings given in the Applicable Product Terms. In the event of any conflict between the Applicable Product Terms and this Controller Addendum, this Controller Addendum will govern solely to the extent of the conflict.

Facebook and you agree to the following:

- Facebook Ireland Limited, 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland (“**Facebook Ireland**” or “**we**”) and you (each a “**Party**”, together the “**Parties**”) are Joint Controllers in accordance with Article 26 GDPR for the Joint Processing specified by the Applicable Product Terms. The scope of the Joint Processing and this Controller Addendum covers the collection of the Personal Data specified by the Applicable Product Terms and its transmission to Facebook Ireland; the subsequent processing of data by Facebook Ireland does not form part of the Joint Processing. More information on the Joint Processing can be found in the Applicable Product Terms.
- This Controller Addendum determines Facebook Ireland’s and your responsibilities for compliance with the obligations under the GDPR with regard to the Joint Processing. The Joint Processing is subject to the provisions of this Controller Addendum. They apply to all activities in which the Parties, their employees or their Processors are involved in the Joint Processing.
- You agree to follow the available documentation regarding the correct technical implementation of the Applicable Products into your websites or apps and their configuration.
- Facebook Ireland’s and your responsibilities for compliance with the obligations under the GDPR with regard to the Joint Processing are determined as follows:

No, no.	Obligation under GDPR	Facebook Ireland	You
1	Article 6: Requirement of legal basis for Joint Processing	X (regarding Facebook Ireland’s processing)	X (regarding your own processing)
2	Articles 13,14: Providing information on Joint Processing of Personal Data		X  This includes as a minimum the provision of the following information in addition to your standard data policy or similar document: That Facebook Ireland is a Joint Controller of the Joint Processing and that the information required by Article 13(1)(a) and (b) GDPR can be found in Facebook Ireland’s Data Policy at

<sup>4</sup> [https://www.facebook.com/legal/controller\\_addendum](https://www.facebook.com/legal/controller_addendum)



			<p><a href="https://www.facebook.com/about/privacy">https://www.facebook.com/about/privacy</a>.</p> <p>The information that you use Applicable Products as well as the purposes for which the collection and transmission of Personal Data that constitutes the Joint Processing takes place as set out in the Applicable Product Terms.</p> <p>That further information on how Facebook Ireland processes Personal Data, including the legal basis Facebook Ireland relies on and the ways to exercise Data Subject rights against Facebook Ireland, can be found in Facebook Ireland's Data Policy at <a href="https://www.facebook.com/about/privacy">https://www.facebook.com/about/privacy</a>. (please see Applicable Product Terms for further information on the Joint Processing)</p>
3	Article 26(2): Making available the essence of this Controller Addendum		<p>X</p> <p>This includes as a minimum the provision of the following information:</p> <p>That you and Facebook Ireland have:</p> <p>entered into this Controller Addendum to determine the respective responsibilities for compliance with the obligations under the GDPR with regard to the Joint Processing (as specified in the Applicable Product Terms);</p> <p>agreed that you are responsible for providing Data Subjects as a minimum with the information listed under no. 2;</p> <p>agreed that between the Parties, Facebook Ireland is responsible for enabling Data Subjects' rights under Articles 15-20 of the GDPR with regard to the Personal Data stored by Facebook Ireland after the Joint Processing.</p>
4	Articles 15-20: Rights of the Data Subject with regard to the Personal Data stored by Facebook after the Joint Processing	X	
5	Article 21: Right to object insofar as the Joint Processing is based on Article 6(1)(f)	X (regarding Facebook Ireland's processing)	X (regarding your own processing)
6	Article 32: Security of the Joint Processing	X (regarding the security of the Applicable Products)	X (regarding the correct technical implementation and configuration of the Applicable Products)
7	Articles 33, 34: Personal Data Breaches concerning the Joint Processing	X (insofar as a Personal Data Breach concerns Facebook Ireland's bond under this Controller Addendum)	X (insofar as a Personal Data Breach concerns your obligations under this Controller Addendum)

- All other responsibilities for compliance with obligations under the GDPR regarding the Joint Processing remain with each Party individually. [...]

In clause 5.a.ii of its “Facebook Business Tools” terms, Meta Ireland refers to further information.<sup>5</sup> This information provides an overview of the personal data collected and transmitted to Meta Ireland as part of the processing activity for which the parties are joint controllers.

This overview shows *inter alia* that the tools Facebook Login and Facebook Pixel collect information about “http header information, which include information about the web browser or app used (e.g. user agent, locale country-level/language)” and “online identifiers including IP addresses and, insofar as provided, FB-related identifiers or device identifiers (such as mobile OS advertising IDs) as well as information on opt-out/limited ad tracking status”.

## 2.2. Complainant’s submissions

In general, the complainant has stated that in connection with her visit to Boligportal’s website, Boligportal has processed information about her IP address and information collected through cookies and transferred (some of) this information to Meta Platforms in the United States.

To support this, the complainant has submitted technical documentation for her visit to Boligportal’s website on 12 August 2020.

Additionally, the complainant has stated that the transfer is unlawful as the Court of Justice of the European Union (“CJEU”) in its so-called *Schrems II*-decision<sup>6</sup> invalidated the European Commission’s adequacy decision concerning the United States (more specifically US organisations certified under the Privacy Shield-scheme). Therefore, there is no transfer basis for transfers to the United States pursuant to Article 45 GDPR.

Furthermore, the complainant has stated that the transfer cannot take place on the basis of standard contractual clauses pursuant to Article 46(2)(c) and (d) GDPR if an essentially equivalent level of data protection cannot be ensured by the SCCs in the third country to which the data are transferred.

In this regard, the complainant has stated that Meta Platforms is considered an *electronic communications service provider* and is thus covered by Section 702 of the Foreign Intelligence Surveillance Act (FISA 702). According to the CJEU, transfer of personal data to companies that are subject to FISA 702 constitutes an infringement of Articles 7 and 8 and the essence of Article 47 of the Charter of Fundamental Rights of the European Union. Finally, the complainant refers to the fact that Meta Platforms *inter alia* according to its own Transparency Report actively discloses personal data to U.S. authorities under FISA 702.

In summary, the complainant argues that Boligportal cannot ensure an essentially equivalent level of data protection for personal data of the complainant that is transferred to Meta Platforms.

With regard to the allocation of roles and responsibilities between Boligportal and Meta Ireland, the complainant has generally stated that Boligportal has entered into a contract with Meta

---

<sup>5</sup> Under clause 5.2.ii Meta Ireland refers to the following website: [https://www.facebook.com/legal/terms/businessstools\\_jointprocessing](https://www.facebook.com/legal/terms/businessstools_jointprocessing)

<sup>6</sup> Judgment of the Court of Justice of the European Union of 16 July 2020 in Case C-311/18, *Schrems II*.

Ireland under which Meta Ireland acts as a processor on behalf of Boligportal and that Boligportal has authorised the use of Meta Platforms as subprocessor for Boligportal. The complainant refers to clause 4 of the Facebook Business Tools Terms of 26 December 2019 and clause 1.4 of the Facebook Data Processing Terms. The complainant also refers to point 4 of the Facebook Business Tool Terms of 31 August 2020.

The complainant has stated that Boligportal cannot accept Meta Ireland's standard terms and at the same time claim in good faith that no personal data is transferred to the United States. These transfers were the subject of the case in the judgment of the Irish Supreme Court "*Data Protection Commission — v. Facebook and Schrems, No.2016 4809P*", which led to the judgment of the CJEU in the *Schrems II*-decision. As such, there is a presumption that Meta Ireland transfers personal data to Meta Platforms in the United States. In the complainant's view, Boligportal must – pursuant the provisions on accountability in Articles 5(2) and 24(1) GDPR – be able to prove that, despite the existing contractual relationship and the technical arrangement of Meta's platform, no personal data is transferred to the United States.

To the extent that Meta Ireland cannot be considered a processor for Boligportal, the complainant has further stated that Meta Ireland and Boligportal are joint controllers for the processing of personal data. The parties have made a joint decision on the purposes and means of the processing of personal data by embedding Meta Ireland's tools on Boligportal's website which include transfers of personal data to the United States.

Finally, the complainant submits that according to the principle of accountability in Articles 5(2) and 24 GDPR, it is for the controller to demonstrate that the processing of personal data is carried out in compliance with data protection law.

The complainant states in this regard that she does not have the technical means of providing certain proof that the transfer has actually taken place as Meta Ireland is unlikely to provide the complainant with the necessary access to demonstrate this. However, according to the complainant, Boligportal is as the controller required to demonstrate that personal data of the complainant are not transferred to Meta Platforms, in particular in view of the publicly known fact that Meta Ireland uses Meta Platforms' infrastructure. It is insufficient to submit that the complainant must demonstrate that her personal data has been transferred to the United States and it is insufficient to refer to the fact that the IP addresses to which the data were transferred are registered to Meta Ireland.

### **2.3. Boligportal's comments**

Boligportal has generally stated that, according to the technical information immediately available to the company, it did not transfer personal data of the complainant to the United States using the tools provided by Meta Ireland.

Boligportal has stated that, on the basis of an examination of the documentation submitted by the complainant, it is the company's view that the complainant has visited the front page of Boligportal's website, that the complainant has not used her Facebook account to create a profile on Boligportal's website, and that the complainant has not searched for housing or leases on the website.

Additionally, Boligportal has stated that in the abovementioned documentation the company has identified three scripts which were loaded from the domain "connect.facebook.com" and that those scripts were loaded from the IP address [REDACTED]. From these three scripts, a pixel is loaded from the facebook.com domain which is retrieved from the IP address [REDACTED]

Boligportal has further stated that by looking up the IP addresses in the *Réseaux IP Européens Network Coordination Centre (RIPE NCC)*<sup>7</sup>, Boligportal finds that the two IP addresses form part of a pool of IP addresses registered to “Facebook Ireland Ltd” and that the IP addresses belong to “IE”, that is to say, Ireland. Boligportal submits that the company has no reason to assume that the same should not have been the case on 12 August 2020 when the complainant visited the website.

Boligportal has also stated that by embedding the scripts and pixels in question, Boligportal has accepted the standard terms of use of those scripts. However, Boligportal’s assessment is that the provisions governing the transfer to third countries are irrelevant to the complaint as Boligportal has neither transferred nor contributed to the transfer of personal data of the complainant to the United States. Personal data appear to only have been transmitted to Ireland.

As regards the allocation of roles and responsibilities between Boligportal and Meta Ireland, Boligportal has generally stated that none of the services for which Boligportal has used the tools from Meta Ireland entail that Meta Ireland has been a processor for Boligportal, including for the processing of personal data of the complainant in connection with the complainant’s visit to Boligportal’s website on 12 August 2020.

Boligportal has stated that the company subsequently made a general update of its privacy policy on 19 February 2021 clarifying the correct context. It follows from the updated privacy policy that there is joint controllership for the given processing of personal data which does not involve the transfer of personal data to third countries.

Boligportal has further stated that Meta Ireland’s terms cover a wide variety of Meta Ireland’s services and that Boligportal uses Meta Ireland’s tools for limited activities. None of the services for which Boligportal has used Meta Ireland’s tools entail that Meta Ireland is a processor for Boligportal.

Boligportal has also stated that the company is not aware of whether there is a transfer of personal data between Meta Ireland and Meta Platforms, but this is also irrelevant as – under Chapter V GDPR – Boligportal’s controllership and liability ends upon the company’s transmission of personal data to Meta Ireland as an independent controller.

Boligportal has stated that there has been no evidence to support that the company had transferred personal data to the United States and that the facts of a 2016 case from the Irish Data Protection Commission are not relevant to the present case.

Finally, on the limits of joint controllership with Meta Ireland, Boligportal has stated the following:

“[Boligportal] collects information on both its own and Facebook Ireland Ltd’s behalf, and subsequently [Boligportal] and Facebook Ireland Ltd. are each controllers for the respective further use of the personal data. This is also stated in [Boligportal’s] privacy policy at [...] under point “Social media” ([Boligportal’s emphasis]):

“For some of our partners, we have a joint controllership, i.e. Boligportal collects information on both our own behalf and a partner’s. **Subsequently, Boligportal and the partners are each a controller for the respective further use of the data.** Below you can see with which partners we are joint controllers and how the responsibility is allocated.

---

<sup>7</sup> RIPE NCC is the Regional Internet Register (RIR) for Europe. A RIR is an organisation that handles the assignment and registration of, *inter alia*, IP addresses within a specific region. There are a total of five regional registers.

Login using your Facebook profile on Boligportal

Facebook Ireland, 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland. You can read about

- data processing here – Facebook Login, which is Event Data in section 2.a.ii and section 5.a.ii on joint controllership: <https://www.facebook.com/legal/terms/businessstools>
- allocation of responsibilities here: [https://www.facebook.com/legal/controller\\_addendum](https://www.facebook.com/legal/controller_addendum)
- information about Facebook’s privacy information here: <https://www.facebook.com/about/privacy> including the basis for Facebook’s processing and exercise of rights with Facebook”

Despite [Boligportal’s] unambiguous indication of the allocation of responsibilities, which has been available on [Boligportal’s] website since the update on 19 February 2021, [the complainant] writes in the letter of 29 November 2021:

“... in any case there is a joint controllership of Facebook Ireland Ltd. and the respondent. The two companies jointly made the decision on the purposes and means of data processing by integrating Facebook tools, which involve the transfer of data to Facebook Inc. into [Boligportal’s] website.”

This view is contested in relation to the time after the transmission to Facebook Ireland Ltd. as [Boligportal] is no longer part of the joint controllership where the processing no longer relates to the use of Facebook Connect as described in the Privacy Policy.

The use of Facebook Connect does not entail a transfer to the United States. The processing consists of the collection and transmission of personal data through a cookie and the execution of scripts from the Facebook domain in Ireland. The function is used solely to support website visitors’ login options and to enable Facebook Ireland Ltd. to identify that the complainant has visited the website.

From the EDPB’s Guidance 07/2020 on joint controller follows ([Boligportal’s] highlights):

“Joint participation can take the form of **a common decision** taken by two or more entities or result from converging decisions by two or more entities, where **the decisions complement each other and are necessary for the processing to take place** in such a manner that they have a tangible impact on the determination of the purposes and means of the processing. **An important criterion is that the processing would not be possible without both parties’ participation** in the sense that the processing by each party is inseparable, i.e. inextricably linked. The joint participation needs to include the determination of purposes on the one hand and the determination of means on the other hand.”

As previously mentioned above, [Boligportal] does not exercise any influence over the processing operations carried out by Facebook Ireland Ltd. as an independent controller after the transmission from [Boligportal]. Thus, a transfer from Facebook Ireland Ltd. to a recipient in the United States will be possible without [Boligportal’s] participation in the determination of the purpose or means.

[Boligportal] further refers to the judgments of the Court of Justice of the European Union C-210/16 (“Wirtschaftsakademie-decision”) and C-40/17 (“Fashion ID-decision”) as well as to the Danish DPA’s decision in case 2018-32-0357 (“DMI-decision”).

In its Wirtschaftsakademie-decision, the CJEU clarified in para. 43 that:

“[...] the existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data. On the contrary, those operators may be involved at different stages of that processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case.”

In its later Fashion ID-decision, para. 70, the CJEU applied an identical interpretation of the scope of joint controllership. Furthermore, the CJEU expressly stated in its Fashion ID-decision, para. 74, that a [legal] person cannot be regarded as a joint controller of processing operations carried out by another controller that precede or are subsequent to the processing operations of that legal person, where he determines neither the purposes nor means of processing by the other controller. Therefore, in the specific case, the CJEU did not consider Fashion ID to be the controller in relation to Facebook’s processing of personal data after it was transferred to Facebook.

The Danish DPA has adopted the same interpretation in its DMI-decision, where, in accordance with the case-law of the CJEU, the Danish DPA stated that it is excluded that the joint controllership covers subsequent processing operations for which a company does not determine the purpose or means:

“In view of this, the Danish DPA considers that the processing operations for which DMI together with Google can determine the purposes and means are the collection and transmission of personal data of visitors to dmi.dk. On the other hand, as regards the personal data at issue, it appears prima facie impossible for DMI to determine the purposes and means of subsequent processing operations relating to personal data by Google after their transmission to Google hence DMI cannot be regarded as the controller for those operations.”

The [complainant's] submissions in the letter of 16 March 2021 that [Bolgportal] is the controller because there is a “chain of processing” directly contradicts the interpretation by the CJEU and the Danish DPA of joint controllership and the limits of the responsibilities of the actors involved.

As [Bolgportal] has already made clear, [Bolgportal] is not aware of whether Facebook Ireland Ltd. has transferred personal data to Facebook Inc. in the United States. Consequently, it is clear that [Bolgportal] could not in any way have participated in the determination of the purpose or determination of the means in the context of the alleged but still unsubstantiated transfer. Therefore, [Bolgportal] is not the controller responsible for this specific processing, which may involve a transfer to the United States.

[Bolgportal] has not carried out the specific processing to which the complaint relates. Thus, should Facebook Ireland Ltd have made the alleged transfer, it is outside the scope of [Bolgportal's] controllership within the meaning of Article 26 GDPR since [Bolgportal] cannot be regarded as a controller for processing operations subsequent to the transmission to Facebook Ireland Ltd.

No documentation has been put forward demonstrating that, following the reception of the information by the Irish subsidiary, Facebook has transferred any personal data relating to the complainant to the United States through the executed script on [Bolgportal]'s website.

It can never be detrimental to [Bolgportal] that [Bolgportal] cannot demonstrate whether a subsequent controller (Facebook) has transferred personal data to the United States or not. [Bolgportal] is simply not responsible for any transfer, nor is it obliged to demonstrate anything in this regard against the complainant or the Danish DPA. The question in principle is whether a prior controller is obligated under the GDPR or other legal provisions to demonstrate whether a subsequent controller has or has not transferred information about a complainant to the United States when the trail for the processing of personal data by the prior controller stops in Ireland. That question must necessarily be answered in the negative.

### **3. Reasons for the Danish DPA's decision**

#### **3.1. Is this processing of personal data?**

On the basis of the documentation submitted by the complainant, the Danish DPA finds that, upon the complainant's visit to Bolgportal's website, information about *inter alia* the complainant's IP address, her visit to Bolgportal's website, the time of the visit, and other information about the complainant's browser, operating system, etc. as well as information about online identifiers collected through cookies stored in the complainant's browser, has been collected and transmitted.

According to the “Facebook Business Tools Terms” of 26 December 2019 and 31 August 2020, this information, which is defined as “Event Data”, is used *inter alia* to create target groups on Facebook which can be used for targeted marketing, and to personalise features and content on Facebook.

In its decision of 11 February 2020 in the case 2018-32-0357 concerning the Danish Meteorological Institute's processing of personal data of website visitors, the Danish DPA held that such data is considered as personal data when the data makes it possible to single out the persons in question.

Followingly, it is the Danish DPA's assessment that the information about the complainant in the present case which is collected and transmitted to Meta Ireland constitutes personal data of the complainant.

In support of this assessment, the Danish DPA considers that the information relates to the characteristics and behaviour of the complainant and is used to treat that person in a certain manner in relation to which functions and content are displayed for the complainant on Facebook.

### **3.2. Has personal data about the complainant been transferred to the United States?**

The complainant has stated that her personal data has been collected and transferred to Meta Platforms in the United States as part of her visit to Boligportal's website.

In this regard, Boligportal has stated that according to the technical information immediately available to the company, it did not transfer personal data of the complainant to the United States and that the IP addresses to which the data was transferred upon the complainant's visit to Boligportal's website were registered with Meta Ireland located in Ireland.

The complainant has stated that she does not have the technical means to provide certain proof that the transfer has actually taken place as Meta Ireland is unlikely to provide the complainant with the necessary access to demonstrate this. However, according to the complainant, Boligportal is – as the controller – required to demonstrate that personal data of the complainant is not transferred to Meta Platforms, in particular in view of the publicly known fact that Meta Ireland uses Meta Platforms' infrastructure. In that regard, it is insufficient for Boligportal merely to refer to the fact that the IP addresses to which the complainant's data have been transferred are registered with Meta Ireland.

Regarding this, Boligportal has stated that it has only transmitted information to Ireland and that no evidence has been provided that, following its receipt of the information, Meta Ireland has transferred the personal data of the complainant to the United States by means of the executed scripts on Boligportal's website.

On this basis, the Danish DPA finds that there is disagreement between the parties as to whether there has been a specific transfer of personal data of the complainant to the United States.

The Danish DPA notes that the supervisory authority in principle only handles cases on a written basis. In cases where there is a disagreement between the parties on the facts, the Danish DPA only takes a position on such disagreement if either position can be supported by the further material of the case. The final assessment of such evidential issues can be carried out by the courts, which, unlike the Danish DPA, have the opportunity to clarify factual circumstances, including by means of questioning of witnesses.

As a result, the Danish DPA cannot clearly determine whether, in this specific case, personal data of the complainant has been transferred to third countries and, if so, which countries. Therefore, the supervisory authority cannot adopt a specific decision concerning Boligportal's possible transfer of personal data of the complainant to the United States.

However, the fact that the Danish DPA cannot decide on the possible transfer of personal data of the complainant to the United States gives the Danish DPA rise to assess whether Boligportal has complied with its obligations under the GDPR, in particular its obligation to demonstrate its compliance with the GDPR under Articles 5(1)(a), 5(2), and 24(1).

### 3.3. Roles and responsibilities

The question then arises as to the allocation of roles and responsibilities between Boligportal and Meta Ireland for the processing of the personal data at issue.

#### ***At the time of the complainant's visit to Boligportal's website on 12 August 2020***

By integrating tools from Meta Ireland on its website, Boligportal has enabled Meta Ireland to obtain personal data concerning visitors to its website, including the complainant, as this possibility arises from the moment they visit the website.

In light of this, the Danish DPA considers that it can be established that the processing operations for which Boligportal together with Meta Ireland jointly determine the purposes and means of processing are the collection and transmission of personal data concerning visitors to Boligportal's website, including the complainant.

In its decision of 11 February 2020 in the case 2018-32-0357 concerning the Danish Meteorological Institute's processing of personal data of website visitors, the Danish DPA held that embedding plug-ins on a website, which triggers the collection of personal data, means that the website operator becomes a joint controller with the provider of the plug-in in question for the collection and transmission of personal data.

With regard to the means used for the collection and transmission of personal data of visitors to Boligportal's website, including the complainant, it is apparent from sections 2 and 2.3 above that Boligportal has embedded tools from Meta Ireland on its website, which the latter provides to website operators, and that Boligportal is aware that these tools, in addition to making it possible to create an account on Boligportal's website via the visitors' Facebook account, also collect and transmit personal data of website visitors, including the complainant, to Meta Ireland.

By integrating these tools on its website, Boligportal exerts a decisive influence over the collection and transmission of personal data of visitors to its website, including the complainant, to Meta Ireland, as this processing would not have occurred had the tools not been integrated on the website.<sup>8</sup>

On this basis, the Danish DPA finds that Boligportal and Meta Ireland jointly determine the means used for the collection and transmission of personal data of visitors to Boligportal's website, including the complainant.

As for the purposes of the processing of the personal data of the complainant, the Danish DPA finds that Boligportal's embedding of the Facebook Login tool takes place *inter alia* in order to be able to perform targeted marketing on Facebook.

The Danish DPA notes that Boligportal has stated (as detailed in section 2.3 above) that at the time of the complainant's visit to Boligportal's website, it did not use tools from Meta Ireland for purposes where Meta Ireland acts as a processor, but rather for purposes where the parties act as joint controllers. The Danish DPA therefore concludes that Boligportal has used the tools for one or more of the purposes set out in section 2.a.iii-v of Meta Ireland's "Facebook Business Tools Terms" dated 26 December 2019.

---

<sup>8</sup> Judgment of the Court of Justice of the European Union of 29 July 2019 in C-40/17, *Fashion ID*, paragraph 78.



Followingly, the Danish DPA considers that by integrating these tools on its website, Boligportal has enabled the collection and transmission of personal data of the complainant as this processing activity is performed in the economic interest of both Boligportal and Meta Ireland, whereas the latter's access to this data for the purpose of evaluating and determining the preferences and behaviour of the complainant contributes to the efficacy of Meta Ireland's advertising platform which also benefits Boligportal in the form of improved marketing opportunities on Facebook.<sup>9</sup>

In light of the foregoing, it is the view of the Danish DPA that Boligportal and Meta Ireland jointly determine the purposes and means for the collection and transmission of personal data of the complainant and shall be considered as joint controllers for these processing operations.

#### ***After Meta Ireland's update of its Terms on 31 August 2020***

As Boligportal has continued to embed the tools of Meta Ireland on Boligportal's website after the complainants visit, Boligportal continues to have a decisive influence on the collection and transmission of personal data of its website visitors to Meta Ireland.

Similarly, Meta Ireland's update of its terms on 31 August 2020 has not resulted in significant changes in the purposes for which the personal data is collected and transmitted to Meta Ireland via its business partners such as Boligportal. Personal data is thus processed to enable Boligportal to perform targeted marketing on Facebook as well as the improvement and efficacy of Meta Ireland's advertising platform.

Consequently, the Danish DPA considers that the processing activity continues to take place in the economic interest of both Boligportal and Meta Ireland and that Boligportal and Meta Ireland continue to jointly determine the purposes and means for the collection and transmission of personal data of visitors to Boligportal's website. As such, the parties are joint controllers for these processing operations.

The Danish DPA has also considered that the terms have been clarified, in particular with respect to the determination of roles and responsibilities, such that it is now apparent from clause 5.a.ii of the terms that website operators and Meta Ireland are joint controllers for the processing of personal data of website visitors on websites where tools from Meta Ireland are embedded. It follows from the terms that the parties are joint controllers for the collection and transmission of the personal data to Meta Ireland.

#### **3.4. Who is responsible and for what?**

It follows from Article 26(1) GDPR that joint controllers shall determine their respective responsibilities for compliance with the obligations under the GDPR in a transparent manner.

In its Guidelines 7/2020<sup>10</sup> on controllers and processors, the European Data Protection Board has elaborated on what this obligation entails in practice:

“Joint controllers thus need to set “who does what” by deciding between themselves who will have to carry out which tasks in order to make sure that the processing complies with the applicable obligations under the GDPR in relation to the joint processing at stake. In other words, a distribution of responsibilities for compliance is to be made as resulting from the use of the term “respective” in Article 26(1). [...]

<sup>9</sup> Judgment of the Court of Justice of the European Union of 29 July 2019 in Case C- 40/17 *Fashion ID*, paragraph 80.

<sup>10</sup> European Data Protection Board's guidelines 7/2020 on the concepts of controller and processor in the GDPR, version 2, adopted on 7 July 2021, para. 162, 163, 165 & 166.

The objective of these rules is to ensure that where multiple actors are involved, especially in complex data processing environments, responsibility for compliance with data protection rules is clearly allocated in order to avoid that the protection of personal data is reduced, or that a negative conflict of competence lead to loopholes whereby some obligations are not complied with by any of the parties involved in the processing. It should be made clear here that all responsibilities have to be allocated according to the factual circumstances in order to achieve an operative agreement. The EDPB observes that there are situations occurring in which the influence of one joint controller and its factual influence complicate the achievement of an agreement. However, those circumstances do not negate the joint controllership and cannot serve to exempt either party from its obligations under the GDPR. [...]

However, the use of the terms “in particular” indicates that the obligations subject to the allocation of responsibilities for compliance by each party involved as referred in this provision are non-exhaustive. It follows that the distribution of the responsibilities for compliance among joint controllers is not limited to the topics referred in Article 26(1) but extends to other controller’s obligations under the GDPR. Indeed, joint controllers need to ensure that the whole joint processing fully complies with the GDPR.

In this perspective, the compliance measures and related obligations joint controllers should consider when determining their respective responsibilities, in addition to those specifically referred in Article 26(1), include amongst others without limitation:

- Implementation of general data protection principles (Article 5)
- Legal basis of the processing (Article 6)
- Security measures (Article 32)
- Notification of a personal data breach to the supervisory authority and to the data subject (Articles 33 and 34)
- Data Protection Impact Assessments (Articles 35 and 36)
- The use of a processor (Article 28)
- Transfers of data to third countries (Chapter V)
- Organisation of contact with data subjects and supervisory authorities”

In the view of the Danish DPA, two or more parties who are joint controllers must therefore jointly comply with the obligations of controllers under the GDPR. The parties are jointly responsible for ensuring that the processing operations in question are carried out in compliance with data protection law.

As such, Boligportal is, in principle, as (one of) the controller(s) subject to the obligations arising *inter alia* from Articles 5-22, 24-28, 30 to 39 and 44 to 49 GDPR.

In this context, the CJEU has clarified that the existence of joint liability does not necessarily imply equal responsibility of the various operators engaged in the processing of personal data. On the contrary, those operators may be involved at different stages of that processing of personal data and to different degrees, with the result that the level of liability of each of them must be assessed with regard to all the relevant circumstances of the particular case.<sup>11</sup>

In other words, joint controllership only covers those processing operations for which the parties jointly determine the purpose(s) and means.

In line with the case-law of the CJEU and the Danish DPA, the Danish DPA considers that Boligportal – as mentioned above in section 3.2 – is a joint controller for the processing operations of collection and transmission of personal data of website visitors, including the complainant. Boligportal is therefore not responsible for the processing of personal data carried out by Meta Ireland after its transmission to the latter as Boligportal does not determine the purposes and means of that subsequent processing.

---

<sup>11</sup> Judgment of the Court of Justice of the European Union of 29 July 2019 in Case C-40/17 Fashion ID, paragraph 70, as well as the references therein.

However, Boligportal is a joint controller together with Meta Ireland for the collection and transmission of personal data about website visitors, including personal data of the complainant.

In particular, the Danish DPA considers that there are certain obligations which generally fall on the controller that Boligportal is precluded from observing given the nature of the processing operations. For example, it would appear to be impossible for Boligportal to comply with the right of access or the right to rectification since it is solely responsible for the processing of personal data in the form of collection and transmission and subsequently does not have access to the personal data.<sup>12</sup>

On the other hand, Boligportal does not appear as precluded from complying – together with Meta Ireland – with the obligations relating to the transfer of personal data to third countries as set out in Article 44 GDPR, if and to the extent that personal data is processed by means located outside the EU/EEA in the context of collection and transmission of that personal data.

In view of the fact that collection and transmission can occur by means located outside the EU/EEA, it is the Danish DPA's view that Boligportal is at least jointly responsible for ensuring compliance with Article 26 GDPR, in particular with regards to the allocation of roles and responsibilities concerning transfers of personal data to third countries. The Danish DPA places significant importance on the fact that personal data may as part of these processing operations be transferred outside the EU/EEA, for instance, if the processing – in this case collection and transmission – is carried out by processors outside the EU/EEA.

The Danish DPA also considers that these processing operations are only made possible by the fact that Boligportal has embedded tools from Meta Ireland on its website while being fully aware that these tools serve as a means of collecting and transmitting personal data of visitors to Boligportal's website, including the complainant, to Meta Ireland. By Boligportal's decision to embed these tools on its website, Boligportal exerts a decisive influence on how and where the processing of personal data of website visitors takes place, including, if applicable, whether the processing may occur by means located outside the EU/EEA.

Specifically, the Danish DPA notes that unlike disclosure of personal data between two individual controllers where Boligportal, prior to disclosure, would be obligated, in particular, to (i) ensure a lawful basis for the disclosure and (ii) comply with its notification obligation under Articles 13 and 14 GDPR, joint controllership exists for the processing operations of collection and transmission.

In light of this and having regard to the fact that one of the fundamental objectives of the GDPR is to ensure effective and complete protection of the fundamental rights and freedoms of natural persons, in particular the right to privacy and the right to data protection, the Danish DPA considers that Article 26 GDPR must be understood as an obligation for two or more parties who are joint controllers for processing of personal data to jointly ensure compliance with the GDPR and must jointly be able to demonstrate this.

It is thus the Danish DPA's view that the underlying premise of joint controllership is that the parties must jointly demonstrate compliance with their obligations as controllers under the GDPR.

---

12 Opinion of Advocate General Bobek of 19 December 2018 in Case C-40/17 Fashion ID, paragraphs 83, 135-136.

If the parties were individually obligated to ensure compliance with the GDPR, it would, in the view of the Danish DPA, entail a risk that the data subject would not be guaranteed a full and effective protection of his or her rights and freedoms as certain obligations could be overlooked by both parties with the consequence that neither party complies with those obligations.

However, the parties who are joint controllers are not precluded from, taking into account the specific processing activity, from organising themselves in such a way that *inter alia* the obligations pursuant to Article 44 is effectively observed by one of the parties. For instance, where collection and processing of personal data occurs by means located outside the EU/EEA, e.g. by way of a processor outside of the EU/EEA, the parties may organise themselves so that Article 44 is effectively observed by the party who has the contractual relationship with that processor(s). However, where appropriate, this must be made transparent and clear from the arrangement between the parties under Article 26 GDPR.

### 3.5. The principle of accountability

The GDPR contains a general principle of accountability in Article 5(2) GDPR. It follows that the controller is responsible for and must be able to demonstrate *inter alia* that personal data is lawfully processed.

The principle of accountability is further developed in Article 24 GDPR, from which it follows that, depending on the specific processing operation, the controller must take appropriate measures to ensure and be able to demonstrate that the processing is carried out in accordance with data protection rules.

Further, in its so-called *Proximus*-decision, the CJEU held that Articles 5(2) and Article 24 GDPR impose general accountability and compliance requirements upon controllers. In particular, those provisions require controllers to take appropriate measures to prevent possible infringements of the rules laid down by the GDPR in order to ensure the right to data protection.<sup>13</sup>

In the view of the Danish DPA, Articles 5(2) and Article 24 GDPR therefore impose an obligation on the controller to be able to document and present this documentation, in particular to the supervisory authority, that the processing of personal data is carried out in compliance with data protection law.

It is the Danish DPA's view that Boligportal has not, in connection with its embedding of tools from Meta Ireland, demonstrated that its processing of personal data of the complainant on 12 August 2020 was lawful, nor has the company demonstrated that its current processing of personal data of visitors to Boligportal's website is lawful pursuant to Articles 5(1)(a), 5(2) and 24(1) GDPR.

As regards the processing of personal data of the complainant in connection with her visit to Boligportal's website on 12 August 2020, the Danish DPA considers in particular that there has been an insufficient allocation of roles and responsibilities between Boligportal and Meta Ireland considering the processing activity and the purposes for which Boligportal, per its own submission as detailed in section 3.3 above, has processed the complainant's personal data, and therefore that Boligportal has not been aware of whether personal data has been processed by means located outside the EU/EEA, e.g. by the use of processors outside the EU/EEA, in the context of processing activities for which the parties are joint controllers.

---

<sup>13</sup> Judgment of the Court of Justice of the European Union of 27 October 2022 in Case C-129/21, *Proximus*, paragraph 81.

The Danish DPA also considers that Boligportal itself has stated that it is not aware of whether personal data as part of the collection and transmission to Meta Ireland are processed by means located outside the EU/EEA, e.g. by the use of processors outside the EU/EEA, and that it is not apparent from Meta Ireland's terms and documentation, to which Boligportal has referred, whether this is the case.

With regard to the processing of personal data of website visitors since Meta Ireland's update of its terms on 31 August 2020, the Danish DPA considers, in particular, that it is not apparent from the current arrangement between Boligportal and Meta Ireland as joint controllers under Article 26 GDPR whether personal data is processed by means located outside the EU/EEA and where, including, if applicable, by the use of processors outside the EU/EEA in the context of processing activities for which the parties are joint controllers and, consequently, which party is responsible for ensuring compliance with Article 44 GDPR. The Danish DPA also considers that Boligportal has not taken independent action to clarify these matters in greater detail.

It is the Danish DPA's fundamental view that a controller cannot demonstrate its compliance with data protection law when the controller is not fully aware of the facts relevant to its processing of personal data.

On the contrary, when processing personal data – whether alone or jointly with others – a controller must provide the supervisory authority with the necessary and relevant information on how the processing of personal data, for which the organisation is (co-)responsible, takes place.

In the view of the Danish DPA, this applies in particular where the controller, by not providing the necessary information, avoids taking into account and assessing publicly known circumstances relevant to the processing activity. In the present case, this includes e.g. the publicly known fact that Meta Ireland (with which Boligportal is a joint controller), as part of its ordinary business operations generally processes personal data by means, such as technical infrastructure, provided by Meta Platforms, Inc. in the United States.

In view of the fact that it is not apparent from the current arrangement between Boligportal and Meta Ireland as joint controllers under Article 26 GDPR whether the processing for which the parties are joint controllers takes place by means located outside the EU/EEA and where, and consequently, which party must, in practice, ensure compliance with Article 44 GDPR, and that Boligportal has not provided sufficient documentation to the Danish DPA in order to demonstrate this, the Danish DPA considers that Boligportal has not demonstrated that its processing of personal data is carried out in compliance with Article 26 GDPR pursuant to Articles 5(1)(a), 5(2), and 24(1) GDPR.

#### **4. Summary: Decision and order**

The Danish DPA finds that there are grounds for **seriously reprimanding** Boligportal for not demonstrating that its processing of personal data of the complainant on 12 August 2020 was carried out in compliance with the GDPR and for not demonstrating that its current processing of personal data of website visitors takes place in compliance with Article 26 GDPR pursuant to Articles 5(1)(a), 5(2), and 24(1) GDPR.

Firstly, the Danish DPA considers that the supervisory authority cannot adopt a decision specifically on Boligportal's possible transfer of personal data of the complainant to the United States as there is disagreement between the parties as to whether personal data of the complainant was in fact transferred to the United States.

However, the fact that the Danish DPA cannot decide on the possible transfer of personal data of the complainant to the United States gives the supervisory authority rise to assess whether Boligportal has complied with its obligations under the GDPR, in particular its obligation to demonstrate its compliance with the GDPR under Articles 5(1)(a), 5(2), and 24(1).

In this regard, the Danish DPA considers that – at the time of the complainant's visit to Boligportal's website on 12 August 2020 – there has been an insufficient allocation of roles and responsibilities between Boligportal and Meta Ireland in light of the processing of personal data that occurred.

Considering the processing activity and the purposes for which Boligportal, per its own submission as detailed in section 3.3 above, has processed the complainant's personal data, the parties must be considered as joint controllers for the processing of personal data of the complainant.

In view of this, and considering that at the time of complainant's visit to Boligportal's website there was no arrangement pursuant to Article 26 GDPR in place which in a transparent manner determined the parties' respective responsibilities for compliance with the GDPR, the Danish DPA finds that Boligportal has not demonstrated that its processing of personal data of the complainant was carried out in compliance with Article 26 GDPR pursuant to Articles 5(1)(a), 5(2), and 24(1).

Additionally, the Danish DPA finds that it is unclear from the current arrangement concluded between Boligportal and Meta Ireland as joint controllers pursuant to Article 26 GDPR whether personal data of website visitors are processed by means located outside the EU/EEA including, if applicable, by the use of processors outside the EU/EEA in with the context of processing activities under the parties' joint controllership and, consequently, which party is responsible for complying with Article 44 GDPR.

As such, the Danish DPA considers that Boligportal has not, in general, demonstrated that its current processing of personal data takes place in compliance with Articles 26 GDPR pursuant to Articles 5(1)(a), 5(2), and 24(1) GDPR as Boligportal has not fully identified whether personal data of visitors to its website is processed by means located outside the EU/EEA and where, including, if applicable, by the use of processors outside the EU/EEA in the context of processing activities for which Boligportal and Meta Ireland are joint controllers.

On this basis, the Danish DPA **orders** Boligportal to bring its processing of personal data into compliance with Articles 5(1)(a), 5(2), 24(1) and 26 GDPR and to be able to demonstrate compliance with these provisions.

Boligportal shall comply with the order **no later than 18 May 2023**. The Danish DPA requests confirmation and documentation that the order has been complied with no later than the same date.

In the view of the Danish DPA, this order may *inter alia* be complied with by clarifying the allocation of roles and responsibilities between Boligportal and Meta Ireland, so that it is apparent from the arrangement between the parties whether personal data of website visitors in the context of the joint controllership is processed by means located outside the EU/EEA including, if applicable, by the use of processors outside the EU/EEA and, consequently, how Article 44 GDPR is complied with as well as which party must ensure compliance with that

provision. Alternatively, compliance with the order may be done by ceasing the processing activity in question.

The Danish DPA notes that the above-mentioned suggested solutions are not exclusive and do not constitute the only options for how Boligportal may comply with the order. As the controller, Boligportal has full freedom of choice in accordance with Articles 5(2) and 24(1) GDPR as to how it demonstrates its compliance with the GDPR.

This order is notified pursuant to Article 58(2)(d) GDPR.

According to Section 41(2)(4) of the Danish Data Protection Act, a fine or imprisonment of up to 6 months shall be imposed on persons who fail to comply with an order issued by the Danish DPA pursuant to Article 58(2)(d) GDPR.

## **5. Final remarks**

The Danish DPA regrets the lengthy consideration of the case and that Boligportal has not been continuously informed of delays in reaching a decision, etc.

A copy of this decision will be forwarded to the complainant.

For completeness, the Danish DPA notes that the authority intends to publish this decision on its website.

Kind regards

████████████████████

**Annex:**        Legal basis.

## **Annex: Legal basis**

### **Excerpts from 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)**

#### *Chapter II*

#### **Principles**

#### Article 5

#### **Principles relating to processing of personal data**

##### 1. Personal data shall be:

- a) processed lawfully fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
- b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
- c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
- e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
- f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

##### 2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').



*Chapter IV*

**Controller and processor**

Article 24

**Responsibility of the controller**

1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. 2 Those measures shall be reviewed and updated where necessary.
2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.
3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.

Article 26

**Joint controllers**

1. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.
2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.
3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.

*CHAPTER V*

***Transfers of personal data to third countries or international organisations***

Article 44

**General principle for transfers**

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place

only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.