



noyb – European Center for Digital Rights
Goldschlagstraße 172/4/3/2
1140 Wien
AUSTRIA

Data Protection Commission

21 Fitzwilliam Square South, Dublin 2, D02 RD28, Ireland

COMPLAINT UNDER ARTICLE 77(1), 80(1) GDPR

***noyb* Case-No: C029-59**

filed by

XXX, (born on XXX) and residing in XXX)
(hereinafter, the “Complainant”)

represented by

noyb – European Centre for Digital Rights, a not-for-profit organization under Article 80(1) GDPR with its registered office at Goldschlagstraße 172/4/2, 1140 Wien, Austria, and with registration number ZVR: 1354838270 (hereinafter “*noyb*”) (Attachment 9)

against

Allied Irish Banks, registered at 2 Burlington Road, Dublin 4, D04 WV00, Ireland
(hereinafter “the Controller”)

and

Facebook Ireland Ltd, 4, Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland
(hereinafter “Facebook Ireland”)

and

Facebook Inc., 471 Emerson St., Palo Alto, CA 94301-160, USA
(hereinafter “Facebook Inc.”)

Communications between *noyb* and the Data Protection Authority in the course of this procedure can be done by email at legal@noyb.eu with reference to the Case-No.as mentioned in the title of this complaint.

1. FACTS AND GROUNDS OF THE COMPLAINT

Processing of the Complainant's personal data using Facebook Connect

1. On 8/14/2020, at 9:26:00 PM the Complainant visited the Controller's website (www.aib.ie; hereinafter "the Website"), while being logged in to the Facebook account associated with the Complainant's email address email. On the Website, the Controller has embedded the HTML code for Facebook Services (including Facebook Connect).
2. Facebook Connect is a service used by third party websites, triggering the flow of the user's personal data between the website and Facebook.
3. The use of Facebook Connect is currently subject to the *Facebook Business Tools Terms* (Attachment 1) and the *Facebook Data Processing Terms* (Attachment 2). Apparently, both documents will be updated effective 31.08.2020 (*New Facebook Business Tools Terms*, Attachment 3 and *New Facebook Data Processing Terms*, Attachment 4).
4. An interpretation of both the current *Facebook Business Tools Terms* and the current *Facebook Data Processing Terms* leads to the conclusion
 - that Facebook Ireland is the contractual partner of the Controller and qualifies as the Controller's processor under Article 4(8) GDPR and
 - that Facebook Inc. qualifies as sub-processor(see Attachment 1, point 4. and Attachment 2, point 1.4.).

The same is true under the *New Facebook Business Tools Terms* and the *New Facebook Data Processing Terms* (see Attachment 3, point 4. and Attachment 4, point 12.)

5. In the course of the Complainant's visit to the Website, the Controller processed the Complainant's personal data (at least the Complainant's IP address and cookie data). Apparently, at least some of this data have been transferred to Facebook Inc. in the USA– see Attachment 5: HAR data of the website visit. The Complainant does not have the technical means to establish whether this data transfer took place directly between the Controller and Facebook Inc. or via Facebook Ireland as an "interstation".
6. In any case, there has been a transfer of the Complainant's personal data from the Controller to the USA. Such transfer from the Controller (an EEA-based company) to Facebook Inc. or any further processors in the USA (or any other non-EEA country) requires a legal basis under Article 44 et seqq. GDPR.

Transfer of the Complainant's data to the US is unlawful

7. As the CJEU has invalidated the "EU-US Privacy Shield" decision in C-311/18 ("Schrems II", hereinafter "the Judgment"), the Controller can no longer base the data transfer to Facebook Inc. on an adequacy decision under Article 45 GDPR.

8. Nevertheless, the Facebook group and the Controller still attempt to rely on the invalidated “EU-US Privacy Shield”, as evidenced by point 4 of the *Facebook Data Processing Terms* (Attachment 2):

“Facebook, Inc. has made commitments under the EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield that may apply to data transferred by you or Facebook Ireland Limited to Facebook, Inc. under the Applicable Product Terms. When applicable as the means to transfer Personal Data outside of the EU or Switzerland to Facebook, Inc. where you are in the European Union or Switzerland, you acknowledge that the Privacy Shield Terms (<https://www.facebook.com/legal/privacyshieldtermsforadvertisers>) apply to such data in addition to the Applicable Product Terms.”

9. Regarding these data transfers, the *Facebook Data Processing Terms* further contain a link to additional *Privacy Shield Terms* (Attachment 6), which in turn are linked to a document called *Facebook Inc. and the EU-U.S. and Swiss-U.S. Privacy Shield* (Attachment 7).

10. Notably, even the *New Facebook Data Processing Terms* (Attachment 4), which will become effective only 6 weeks after the Judgment (!), contain a similar reference to the “EU-US Privacy Shield” (point 12):

“Facebook, Inc., which is used by Facebook Ireland as a sub-processor, has made commitments under the EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield that may apply to Personal Information transferred by you or Facebook Ireland to Facebook, Inc. under the Applicable Product Terms. When applicable as the means to transfer Personal Information outside of the EU/EEA or Switzerland to Facebook, Inc., you acknowledge that the Privacy Shield Terms apply in addition to the Applicable Product Terms.”

11. A regular data transfer system based on an invalidated adequacy decision constitutes a severe, systematic, and, with a view of the *New Facebook Data Processing Terms* (Attachment 4), intentional violation of Article 45 et seqq. GDPR.

12. The Controller may also not base the data transfer on standard data protection clauses under Article 46(2)(c) and (d) GDPR if the third country of destination does not ensure adequate protection, under EU law, of personal data transferred pursuant to those clauses (see para. 135 of the Judgment). The CJEU has explicitly found that further transfers to companies that fall under 50 U.S. Code § 1881a not only violate the relevant Articles in Chapter 5 of the GDPR but also Article 7 and 8 CFR as well as the essence of Article 47 CFR (see C-362/14 (“Schrems I”), para. 95.) Any further transfer therefore violates the fundamental right to privacy, data protection and the right to an effective remedy and to a fair trial.

13. Facebook Inc. qualifies as an electronic communication service provider within the meaning of 50 U.S. Code § 1881(b)(4) and as such is subject to US intelligence surveillance under 50 U.S. Code § 1881a (“FISA 702”). As apparent from the “Snowden Slides” (Attachment 8) and Facebook’s own Transparency Report (see <https://transparency.facebook.com/government-data-requests/country/US>), Facebook Inc. is actively providing personal data to the US government under 50 U.S. Code § 1881a.

14. Consequently, the Controller is unable to ensure an adequate protection of the Complainant’s personal data that are transferred to Facebook Inc. Hence, the Controller is under a legal obligation to refrain from transferring the Complainant’s – or any other personal data – to Facebook Inc. More than one month after the Judgment, the Controller has still not done so.

15. Equally, the Facebook group continues to accept data transfers from the EU/EEA under both the invalidated (!) “EU-US Privacy Shield” and the standard data protection clauses, despite the clear judgment by the CJEU and the violation of Articles 44 to 49 GDPR. Facebook Inc. further discloses EU/EEA personal data to the US government in violation of Article 48 GDPR.
16. Under Article 3(2)(a) GDPR the GDPR extends to (sub-)processors not established in the Union, where the processing activities are *related* to the offering of services to data subjects in the Union. Consequently, there is direct jurisdiction over Facebook Inc. While Facebook Ireland may claim to fall under the jurisdiction of the Irish DPC as lead supervisory authority (Article 56 GDPR) there is no main establishment of Facebook Inc. in the European Union. Therefore, any European data protection authority has direct jurisdiction over Facebook Inc. in its function as sub-processor.
17. Under Articles 58 and 83 GDPR, the Data Protection Authority can use its corrective and sanctioning powers both against the Controller, its processor Facebook Ireland and its sub-processor Facebook Inc.
18. According to the Judgment, the Data Protection Authority must suspend or end the transfer of personal data to the third country concerned under Article 58(2)(f) and (j) GDPR (see para. 135 of the Judgment).

2. APPLICATIONS

The Complainant hereby requests that the Data Protection Authority, by virtue of the powers provided by Article 58 GDPR

- (1) fully investigates the complaint under Article 58(1) and establishes
 - (a) which personal data were transferred from the Controller and/or from Facebook Ireland to Facebook Inc. in the United States of America or to any other third country or international organisation;
 - (b) which transfer mechanism under Article 44 et seqq. GDPR the Controller and/or Facebook Ireland based this data transfer on;
 - (c) whether or not the provisions of the applicable *Facebook Business Tools Terms* and *Facebook Data Processing Terms* (in their current version and as effective 31.08.2020) meet the requirements of Article 28 GDPR with regards to the transfer of personal data to third countries;
- (2) immediately imposes a ban or suspension of any data flows from the Controller and/or from Facebook Ireland to Facebook Inc. in the United States of America and order the return of such data to the EU/EEA or another country that provides adequate protection under Article 58(2)(d), (f) and (j) GDPR;
- (3) imposes an effective, proportionate and dissuasive fine against the Controller, Facebook Ireland and Facebook Inc. under Article 83(5)(c) GDPR, taking into account that
 - (a) the data subject is most likely only one of thousands of users (Article 83(2)(a) GDPR);
 - (b) more than one month has passed since the CJEU judgement C-311/18 and the Controller has not taken any steps to bring its processing operations into compliance with the provisions of the GDPR (Article 83(2)(b) GDPR).

Vienna, 17.08.2020

Attachments:

- 01 – Facebook Business Tools Terms
- 02 – Facebook Data Processing Terms
- 03 – New Facebook Business Tools Terms
- 04 – New Facebook Data Processing Terms
- 05 – HAR data of the website visit
- 06 – Facebook Privacy Shield Terms
- 07 – Facebook Inc. and the EU-U.S. and Swiss-U.S. Privacy Shield
- 08 – “Snowden Slides”
- 09 – Representation Agreement