noyb - European Center for Digital Rights
Goldschlagstraße 172/4/3/2
1140 Vienna
Austria

Data Protection Authority Rue de la
Presse 35
1000 Brussels by
e-Mail: [redacted]

Vienna, 23 June 2023

coreb Case-No: C-063

Plaintiffs: [redacted], domiciled [redacted]
[redacted] a [redacted]
[redacted] t home [redacted]
[redacted], domicil [redacted]
[redacted] residing at [redacted]
[redacted] residing at [redacted]
[redacted] residing at [redacted]
[redacted] residing at [redacted]
[redacted] residing at
, domiciled at

Represented by: *noyb* - European Center for Digital Rights
Goldschlagstraße 172/4/3/2, 1140 Vienna, Austria, pursuant to Article 80 of the RGPD

Against:

BICS SA
Boulevard du Roi Albert II 27, 1030 Brussels

TELESIGN
13274 Fiji Way Suite 600, Marina del Rey CA 90292, United States having a representative within the meaning of Article 27 of the GDPR in the person of TeleSign Netherlands B.V., a company registered in the Netherlands.

PROXIMUS
Boulevard du Roi Albert II 27, 1030 Brussels.

And any other person, controller or processor who may be identified in the course of the procedure.

COMPLA
INT

1. REPRESENTATION

1. *noyb* - European Center for Digital Rights is a non-profit association active in the field of personal data protection. Its offices are located at Goldschlagstraße 172/4/2, 1140 Vienna, Austria, and it is registered under ZVR number: 1354838270 (hereinafter: *("noyb")* (Exhibit 1).

2. *noyb* represents complainants who have mandated it to do so under Article 80 of the GDPR (Exhibits 2).

2. BACKGROUND TO THE COMPLAINT

2.1 Introduction

3. As explained in the present complaint (see section 2.3), an article in the newspaper *Le Soir* revealed in March 2022 that BICS, a subsidiary of Proximus, was transferring data passing through its services to another subsidiary of Proximus in the USA, the company TeleSign.

4. The article in Le Soir explained that TeleSign assigns a 'reputation score' to the telephone numbers of millions of end users, and feeds its algorithms with telecommunications data received by BICS. This trust score is resold to TeleSign customers (such as Skype, LinkedIn and Microsoft), who also use it without informing their users. TeleSign claims to use this data for the vague purpose of "fraud detection".

5. Following this revelation, several users of communications services residing in different countries of the European Union submitted a request for information to their telephony provider, BICS and TeleSign, to find out whether and under what conditions their data was sent and processed by TeleSign.

6. The responses received showed that TeleSign did receive data from users in order to profile them and assign them a reputation score. TeleSign also informed these users of the score assigned to them. It therefore appears that millions of users of communications services were profiled by an American company with which they had never had any contact, whose existence they were not even aware of, and which never informed them of the existence, purpose or conditions of this processing, even though it had their telephone numbers for this very purpose. TeleSign itself confirms that it checks more than five

billion telephone numbers per month, representing half of the world's mobile telephone subscribers.[1]

7. Given BICS' market share, it would appear that TeleSign has collected data from more than half of the world's users, generating considerable revenue without any legal basis and without informing users. TeleSign also uses an algorithm to automatically adopt a score on the basis of which access to its customers' services can be refused. These are therefore unlawful automated decisions within the meaning of the GDPR. Lastly, as TeleSign is subject to US surveillance laws, the processing of this data is contrary to the rules on data transfers laid down by the RGPD, and to the *Schrems I* and *Schrems II* judgments of the Court of Justice.

8. In addition to the unlawful processing carried out by TeleSign, this complaint also concerns the failure to respond to the request for access made by two complainants to Proximus. The complaint also concerns the misuse of the data processed by BICS, which shares its data for purposes that are prohibited both by the GDPR and by the Electronic Communications Act. The complaint also raises the illegality of the transfer of data by BICS to TeleSign in the United States, a transfer organised and governed by a contract between the two companies and which provides for the systematic and massive sending of communications data by BICS to TeleSign.

9. Finally, given the vague, even obscure, and sometimes even contradictory answers provided by TeleSign, it remains difficult to understand precisely what this company does with user data, where it collects it, and with whom it shares it. TeleSign invokes the
TeleSign does not intend to use "anti-fraud" as a purpose in responding to access requests. However, if fraud detection is a legally permissible purpose for the use of electronic communications data by operators, TeleSign is not supposed to receive or use such electronic communications data, even for fraud prevention purposes, as discussed in this complaint. In any event, it is more than doubtful that TeleSign's use of such data reflects any fraud detection purpose that meets the statutory requirement. The DPA's inspection department will not fail to enlighten the complainants about this data processing, the existence of which would still have been a secret had it not been for the revelations of a well-informed press.

2.2 Presentations of the various entities involved in the complaint: BICS, TeleSign and Proximus

2.2.1 BICS

10. BICS ("Belgacom International Carrier Services") is the leading operator in the field of international communications, one of the leading voice operators and the leading provider of mobile data services in the world.[2]

[1] https://www.telesign.com/press/telesign-unveils-new-brand-identity-reflecting-companys-transformation-and-commitment-to-making-the-digital-world-more-trustworthy-for-everyone.

[2] Report annual 2022 of Proximus http://www.proximus.com/dam/jcr:7cf6d111-cf0b-4c3d-a764-201c9bd93283/proximus-rapport-annuel-integre-2022_fr.pdf, p. 12.

11. BICS is a subsidiary of the Proximus Group. The company was founded in 1997 and is headquartered in Brussels, with offices in Dubai, Singapore, Berne, San Francisco and New York. BICS provides services in more than 200 countries, handles half of the world's roaming traffic[3], enables global mobility for more than 150 million terminals and has partnerships with more than 500 mobile operators. [4] BICS transmitted 20.5 billion messages across the globe, and 26 billion minutes via 550 direct connections.

12. BICS also offers protection services against various forms of telecommunications fraud. These services include prevention of SMS fraud, voice fraud, roaming fraud and IPX interconnection security.[5]

2.2.2 TeleSign

13. TeleSign describes itself as a leader in digital identity and programmable communications.[6] TeleSign is *"a fast-growing leader in digital identity and programmable communications solutions. A trusted partner to businesses worldwide, Telesign counts eight of the world's top ten digital companies among its customers and provides services in more than 230 countries and territories"*.[7]

14. TeleSign "provides *solutions for security, authentication, fraud detection, compliance management, reputation scores and secure communications* "[8] by combining digital identity services and global communications solutions,
"TeleSign helps businesses connect, protect and interact with their customers, while enabling them to communicate securely on their preferred digital platforms. [9]

15. TeleSign offers a fraud prevention tool called 'Intelligence API' (formerly known as 'Score'). This tool is based on a "reliability score" that TeleSign assigns to each telephone number in its database, based on "information about telephone numbers, traffic patterns, machine learning and a global data consortium".[10] Again according to TeleSign, the information used by TeleSign uses two global databases to detect and identify fraud: TeleBureau, TeleSign's database for measuring the reputation of a telephone number, and the BICS database (BICS Global Telco Fraud Data).[11]

---

[3] https://www.bics.com/global-roaming/

[4] https://www.bics.com/wp-content/uploads/2021/07/BICS-Roaming-brochure.pdf

[5] https://www.bics.com/wp-content/uploads/2022/02/Telco-Fraud-Whitepaper.pdf

[6] https://www.telesign.com/company

[7] Report annual report 2022 of Proximus, http://www.proximus.com/dam/jcr:7cf6d111-cf0b-4c3d-a764- 201c9bd93283/proximus-rapport-annuel-integre-2022_fr.pdf, p. 12.

[8] Report annual 2021 of Proximus http://www.proximus.com/dam/jcr:7ee0f496-f68e-4161-aa09-c2df5f16f1d0/Proximus-rapport-annuel-integre-2021_fr.pdf, p. 11.

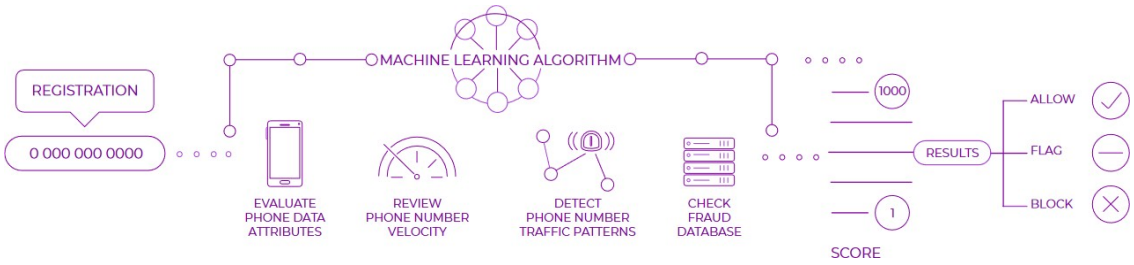
[9] Proximus Annual Report 2021, p. 12.

[10] https://ts.telesign.com/hubfs/Product-Datasheets/Score-Datasheet.pdf

[11] https://ts.telesign.com/hubfs/Product-Datasheets/Score-Datasheet.pdf

16. TeleSign says it uses information from more than 5 billion unique phone numbers, combined with 2,200 digital identity signals (IP address, device ID).[12] TeleSign says it verifies more than 5 billion phone numbers a month, which represents half of the world's mobile users.[13] TeleSign counts 8 of the world's top 10 digital companies among its customers, including SalesForce, Skype, Ubisoft and ByteDance (which provides the TikTok platform).

17. The diagram above summarises the process in place for the reliability score solution provided by TeleSign to these customers:



18. TeleSign first evaluates the attributes of telephone numbers, i.e. a whole series of information relating to the telephone number, such as the type of telephone (fixed line, mobile, VOIP), the telephone operator, the user's address, the status of the telephone, the geographical location and the operator's country code. According to TeleSign, this information can be used to identify any red flags.

19. TeleSign also assesses phone number velocity. This relates to the usage and activity associated with a phone number, for example whether that number has been viewed several times on one or more websites within a relatively short period of time.

20. TeleSign then detects unusual behaviour and carries out a fraud history check on a telephone number.

21. Finally, TeleSign delivers a score consisting of a risk level and a recommendation relating to the number. This score ranges from 0 to 1000 and helps web or mobile applications (TeleSign's customers) in their decision process to block, authorise or flag a user in the account creation process. If the score indicates that the user should be verified, TeleSign can then verify the user by means of a code sent by SMS or by means of a call.

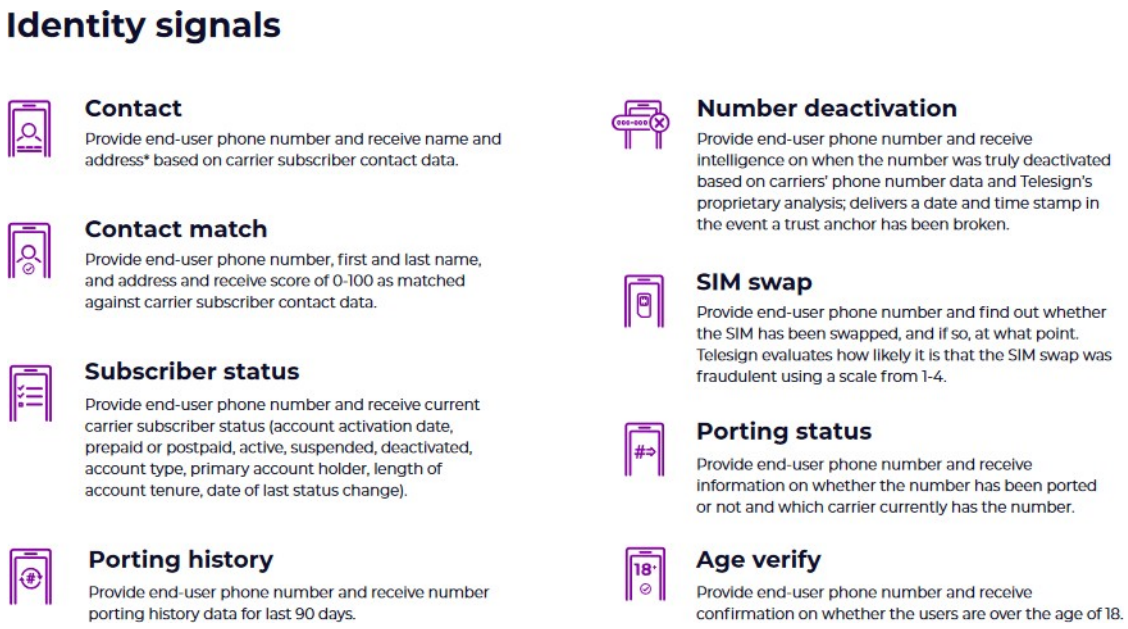
22. In addition to this "Intelligence API" service, TeleSign also offers, among other services, information about the users of TeleSign customers by means of a telephone number, as shown in the extract below. TeleSign offers this "Identity signal" service via its Phone ID API service.[14]

---

[12] https://www.telesign.com/products/intelligence

[13] https://www.telesign.com/press/media-alert-telesign-demonstrates-comprehensive-line-of-digital-identity-solutions-at-money-20-20-amsterdam

[14] "Phone ID identity signals allow you to find out many kinds of information associated with a phone number": see https://developer.telesign.com/enterprise/docs/phone-id-get-started-with-identity-attributes. See also Exhibit 12, accessed on 20 March 2022.



23. As the description shows, TeleSign can, at the request of its customers (the provider of the mobile or web application, such as TikTok, Skype, or Salesforce) :
    - provide the user name ;
    - check whether the user's name, telephone number and address match the data held by TeleSign, which will then give a score from 0 to 100 ;
    - determine the user's status on the network: active, deactivated, suspended, duration o f number activation; and
    - determine whether the user is over 18 or not.

24. TeleSign also provides other services which, again according to TeleSign, are linked to fraud prevention, such as the verification service, which helps to prevent "IRSF" (International Revenue Share Fraud) or a user verification service that sends a password by SMS.

2.2.3 Proximus

25. In October 2017, BICS acquired TeleSign for $230 million. In 2021, Proximus acquired all the shares in BICS for €569 million. BICS and TeleSign are therefore fully controlled subsidiaries of Proximus.

26. Proximus is the incumbent operator in Belgium and provides communications solutions in Belgium (via Proximus, Scarlet and Mobile Vikings), in Europe (via Tango, Telindus) and worldwide through its subsidiaries BICS and Telesign.

27. With 1,634 employees, the Proximus group generated sales of €5.909 billion in 2022.[15]

2.3 The processing operations complained of

28. A press article in the newspaper *Le Soir* on 22 March 2022 revealed that Proximus was transferring customer data to its US subsidiary TeleSign, via its other subsidiary BICS (Exhibit 3).

29. According to *Le Soir*, and as confirmed above, TeleSign uses an algorithm to assign a score to each telephone number and thus measure the reliability of these telephone numbers.

30. Following these articles, the complainants, residing in various European Union countries, submitted access requests on the basis of Article 15 of the GDPR to their mobile operator, BICS and TeleSign, in order to obtain information on the processing operations in question. The following paragraphs summarise the information obtained by the complainants concerning the processing operations to which they were - and probably still are - subjected. This processing mainly (or only?) concerned the "Intelligence API" (formerly "score") service, as shown by the replies provided by TeleSign to the complainants' requests for access.

2.3.1 Response from Proximus

31. Proximus has responded to the comp[redacted] an[redacted] that it was not transmitting data directly to TeleSign but to BICS for interconnection purposes (Exhibit 4).

32. Proximus also sent the complainants concerned a copy of the standard contractual clauses ("SCC") that it had signed with another data controller or processor in the United States (Exhibit 5), after having taken care to black out the fields relating to the description of the data transferred, the names of the parties, the countries to which the data were transferred, and the name of the competent authority with which the data subjects could exercise their rights. Proximus has taken refuge behind the alleged confidentiality of commercial information in this respect.

33. Following a reminder from the complainants, Proximus undertook to get back to them in June 2022 to satisfy their request for access, but they have had no news since.

2.3.2 BICS

34. The responses given by BICS to the complainants in the context of the request for access make it possible to identify the following points (Exhibits 6).

[15] Proximus Annual Report 2022, p. 19.

35. BICS confirms that it is the data controller. BICS also confirms that it transfers to its subsidiary TeleSign certain specific information relevant to fraud control and detection. Among this information, BICS sends users' telephone numbers, which are encrypted and hashed before being sent. BICS also sends TeleSign "certain specific information that is relevant to BICS' efforts to control and detect fraud".[16]

    BICS states that it has "a legitimate interest in detecting and combating telecommunications fraud". According to BICS, the data only comes from the complainants' mobile operators, if the latter have decided to use BICS for call routing purposes.[17]

36. BICS also declares that it is putting in place the following additional measures surrounding the transfer of data to TeleSign in the US, to comply with the terms of the *Schrems II* judgment of the Court of Justice of the EU:
    - data minimization ;
    - pseudonymisation ;
    - encryption ;
    - transfer via SFTP protocol ;
    - a strict data access policy; and
    - file access and audit rights. [18]

37. BICS' transfers to TeleSign are governed by SCCs, which - again according to BICS - were adapted shortly before its response to use the new SCCs adopted by the European Commission (Exhibit 7). These SCCs were communicated to the complainants and are described below.

38. The SCCs use module 1 "controller to controller" and module 2 "controller to processor" and date from 1 December 2021. No version of the SCCs in force prior to this date has been sent to the complainants. These SCCs are signed as addenda to "one or more principal agreements", including the "Data processing agreement" (see page 1 of the SCCs, Exhibit 7).

39. **Module 1** concerns the transfer of data from BICS (as data controller) to TeleSign (as data processor) for the purpose of executing the "various agreements between companies as described in the table" of Annex I.B of Module 1. The last line of the said table refers only to a "Schedule 9" without any further explanation, and states that it concerns "end-user data" for the purpose of "improving TeleSign's scoring service".

40. **Module 2** concerns the transfer of data from BICS (as data controller) to TeleSign (as data processor). Module 2 merely states that the data importer (TeleSign) may process the data in accordance with the purposes described in the main agreement, and more generally for the provision of the said service to the data exporter (BICS).

---

[16] See for example response to [redacted] Exhibit 6.3. BICS also confirms that it sends the telephone number of the data subjects, with specific information derived from activities observed on the BICS network: see, for example, the response given to [redacted] Exhibit 6.10.

[17] See for example Exhibit 6.3.

[18] See for example Exhibit 6.3.

and the detection and reduction of fraud. The data subjects have not received the main agreement referred to in module 2 and are not aware of any other purposes being pursued.

41. Both modules designate the Belgian data protection authority as the competent authority (see Annexes I.C of the two CSC modules, Exhibit 7).

2.3.3 TeleSign

42. The complainants also made access requests to TeleSign, to which TeleSign responded (Exhibit 8). These responses are summarised below.

a) Data processed

43. TeleSign confirmed that it processed the complainants' telephone number at the time of the access request, and that it generated a score linked to this number (Exhibit 8). For one of the complainants, the data processed also included the type of telephone number (mobile), the name of the operator and the complainant's countr[redacted]8.1, reply to).

44. For example, the complainant [redacted] received the score assigned to her as well as the the following information from TeleSign (see Exhibit 8.1, response to [redacted]):

> *Scores = Ranging between 1 - 300*
>
> *Reason codes = Ranging from:*
>
> • *low activity; pp: low number of completed calls, irregular call duration, no long-term activity, no range activity*
>
> • *low activity; p2p: low number of completed calls, regular call duration, no long-term activity, no range activity*
>
> • *low activity; p2p: low number of completed calls, regular call duration, sparse long-term activity, no range activity*
>
> • *low activity; p2p: very low number of completed calls, irregular call duration, no long-term activity, no range activity*
>
> • *low activity; p2p: very low number of completed calls, irregular call duration, sparse long-term activity, no range activity*
>
> • *low regular activity; p2p: low number of completed calls, regular call duration, no long- term activity, no range activity, low successful outgoing traffic*
>
> • *low regular activity; p2p: regular number of completed calls, regular call duration, no long-term activity, no range activity, low successful incoming traffic*
>
> • *regular activity; p2p: high number of completed calls, regular call duration, sparse long-term activity, no range activity*
>
> • *regular activity; p2p: low number of completed calls, regular call duration, sparse long- term activity, no range activity*

• regular activity; p2p: regular number of completed calls, regular call duration, no long-term activity, no range activity

• regular activity; p2p: regular number of completed calls, regular call duration, sparse long-term activity, no range activity

In translation, this means that the Phone Number was recommended as "medium - low" risk level.

45. In addition, the compla[redacted] was informed that the following additional data would were processed as part of an Amazon SMS service, about which the complainant in question has received no further information.

To support the Telesign Customer, Amazon Services LLC's request for SMS Services, the following additional data points (see source below) were generated:
o Phone type = Mobile
o Carrier Name = T-Mobile Austria GmbH
o Country = AustriaThe access requests

b) Transfers made

46. **TeleSign confirms that it received the data in question from BICS** (with the telephone number hashed). TeleSign also informed the complainants that it uses the European Commission's SCCs for transfers with BICS (to which it also appears to send data) as a TeleSign customer who requested the score, for fraud prevention by BICS.

47. In its responses to the complainants, TeleSign further confirms that it **shares the data with Amazon Web Services (AWS) as TeleSign's subcontractor,** and uses SCCs for this purpose. TeleSign adds that the data is shared with AWS in the context of real-time fraud prevention services provided to TeleSign customers via its mobile number reputation algorithm.

48. TeleSign provided the plaintiffs with the SCCs dated December 12, 2016 surrounding the transfer of data to AWS (Exhibit 9).

- These SCCs are those adopted by the European Commission in its Decision 2010/87 of 5 February 2010, which was repealed on 26 September 2021. Furthermore, the document does not specify whether the exporter of the data, TeleSign in this case, is acting as data controller, data processor, or in both capacities.
- Clause 2 refers to the following processing operations: "Compute, Storage and Content Delivery on the AWS Network" without further specification.
- Appendix 2 refers to safety measures described in an addendum not sent to the complainants.

49. With regard to [redacted] and [redacted] **TeleSign adds that their data are also shared with Microsoft**, as a TeleSign customer, "for the purposes of

fraud detection and prevention services" (Exhibit 8.4 and 8.7). TeleSign has entered into SCCs with Microsoft regarding this transfer (Exhibit 11).

- These reproduce the SCCs of Decision 2010/87, which was repealed in September 2021. Clause 9 determines the applicable law on the basis of the Member State in which the exporter is established, i.e. Microsoft, which is established in Redmond in the USA (which is not, until proven otherwise, an EU Member State).
- Point 6 of Appendix 1 refers to the processing operations covered by the SCCs and stipulates in particular that Microsoft, the exporter of the data, interrogates TeleSign's services in order to access one or more fraud prevention services. The rest of the description of the processing operations is blacked out and rendered illegible without explanation.
- Concerning the description of the safety measures to be included in Appendix 2 of the SCCs: the text describing them is also blacked out.

50. As for the complainant [redacted] TeleSign indicated that **her telephone number was was also communicated by Amazon Services LLC** for SMS services, and that additional data concerning it came from Telcordia Technologies Inc.

51. TeleSign also provided a copy of the SCCs governing transfers with Amazon Services LLC (Exhibit 10). However, the attached document is a pure copy of the European Commission's SCCs, without having been completed, signed or dated in any way, and without even indicating which modules were relevant or who was the exporter and importer of the data. To date, the complainant has received no further information about this transfer.

c) Legitimate interests and recipients of information collected by TeleSign

52. TeleSign has also indicated that it relies on legitimate interest within the meaning of Article 6(1)(f) of the GDPR to process data, for the specific purposes of *"fraud prevention, protection against spamming or phishing, promotion abuse, fake accounts, account spoofing and other costly attacks"* (see e.g. response to [redacted] see Exhibit 8.3).

53. TeleSign did not inform the complainants of the names of the customers with whom it may have shared the complainants' numbers. TeleSign does, however, state -without further explanation- that if the numbers were not shared with other entities, they are nevertheless likely to be sent to TeleSign customers to whom the complainants would subscribe and who would ask TeleSign for their score in this context.[19]

[19] "Data has not been disclosed further but the Score in relation to your Phone Number could be transferred to other TeleSign customers to which you would subscribe and who would in this context request our Score for your number for fraud prevention".

3. GROUNDS FOR THIS COMPLAINT

3.1 Infringement by Proximus of the complainants' right of access and its obligation of transparency (Articles 12, 13 and 15 of the RGPD)

54. As mentioned above, the plaintiffs [redacted] an[redacted] have both submitted an access request on the basis of Article 15 of the RGPD to Proximus concerning the data sent to the United States, and in particular what legal bases and appropriate guarantees were used (Exhibits 4).

55. Proximus replied to these two complainants that the data was sent under SCCs attached to the reply email and indicating a list of categories of recipients located in the United States to which the data "could" be transferred. Proximus also states that, in its view, *"the GDPR allows the categories of recipients to be limited and does not require Proximus to disclose confidential information, such as its network of suppliers. Attached is a copy of a concrete example of an SCC (in this case, the new SCCs) for a data transfer to the United States, in which various information has been masked."*

56. **Firstly**, it should be noted that Proximus is misreading the GDPR. In accordance with the case law of the CJEU, the data subject must be provided with a specific list of the recipients of that data, so that he or she can check who the recipients of the data are and also exercise his or her rights vis-à-vis those recipients. [20] Furthermore, it should be noted that the wording of Article 15(1)(c) of the GDPR refers specifically to recipients established in a third country.

57. **Secondly**, Proximus' first response to the two complainants in question refers to four legal bases without specifying the data processed for each legal basis and for what precise purposes. This makes it impossible to fully understand the data processing involved in the transfers.

58. The CJEU pointed out in that regard that the principles set out in Article 5 of the RGPD *"include the principle of transparency referred to in Article 5(1)(a) of the RGPD, which implies, as is clear from recital 39 in the preamble to that regulation, that the data subject must have information about the way in which his personal data are processed and that that information must be easily accessible and comprehensible"*.[21] It has to be said that this is not the case here: it is impossible to understand what data are actually transferred, for what purposes and on what precise legal basis within the meaning of Article 6 of the GDPR. Proximus is therefore in breach of its obligation of transparency and at the very least of Articles 13 and 15 of the GDPR.[22]

59. **Furthermore**, Proximus is hiding behind the excuse that *"the clauses communicated were examples of clauses signed in the context of other processing activities"*. However, the

---

[20] *RW* v. *Österreichische Post AG*, C-154/21 of 13 January 2023.

[21] *RW* v. *Österreichische Post AG*, C-154/21 of 13 January 2023, § 35.

[22] On this subject, see in particular EDPB decision 4/2022 of 5 December 2022 concerning Instagram, and more particularly §§234 and 346.

The request made to Proximus concerns data transfers that have actually taken place to the United States, and the safeguards adopted in this context, and not hypothetical transfers or transfers that could possibly concern the data of the complainants concerned.[23] In so doing, Proximus has violated Article 15 of the RGPD and more particularly §1 (c) thereof.

60. **Furthermore,** it is not at all clear what confidentiality obligation Proximus would be bound by and which would prevent it from communicating the essential elements of the transfers covered by the SCCs, such as the description of the processing operations concerned, the recipients of the data, or the competent supervisory authority to which a complaint can be made. In short, Proximus has blacked out so much information in the SCCs communicated that it is impossible for complainants to understand what happens to their data and how it is protected by the SCCs. Proximus cannot hide behind an obligation of confidentiality - which it has neither justified nor explained24 - in order to communicate SCCs that apparently do not cover the transfer of the complainants' data but concern "other processing activities". Moreover, the confidentiality exception applies only to the provision of a copy of the data under Article 15(4) of the GDPR, but not to information relating to the processing.[25]

61. **Finally,** despite Proximus' undertaking on 3 June 2022 to get back to the two above-mentioned complainants "with more information within the legal deadlines applicable to their new request", the latter two have never received a reply from Proximus. The maximum period for replying to such a request is one month under Article 12(3) of the RGPD. This time limit has therefore been exceeded without any justification from Proximus.

62. For the foregoing reasons, Proximus has in particular infringed:

- Article 12 of the GDPR by failing to respond to complainants regarding their additional requests for information within the legal time limits, but also by failing to provide them with concise, transparent, understandable and easily accessible information, as demonstrated above; and

- its transparency obligations within the meaning of articles 5.1.a, 13 and 15 of the RGPD, by not submitting all the information required by these provisions, in particular that relating to transfers outside the European Union.

63. In view of the above, the DPA is asked to order Proximus, without prejudice to other remedies including a fine, to provide information to the complainants' questions regarding the transfer of their data to the United States on the basis of Articles 13 and 15 of the GDPR.[26]

---

[23] See the WP29 Guidelines of 29 November 2017 endorsed by the EDPB on 11 April 2018, §13: the use of the conditional, as in the present case, makes it difficult if not impossible for data subjects to know whether or not their data are actually being processed in the manner described.

[24] See the European Commission's Questions & Answers on SCCs, which confirm that data subjects have the right not only to obtain a copy of the clauses, but also details of the transfers they cover, and that confidentiality can only be raised under strict and justified conditions: https://commission.europa.eu/system/files/2022-05/questions_answers_on_sccs_en.pdf, question 32.

[25] See EDPB Guidelines 01/2022 of 18 January 2022, in particular § 166.

[26] For the sake of clarity, the information requested relates only to transfers to the United States.

3.2 Data processing carried out by BICS

64. BICS confirms in its replies to the complainants (Exhibit 6) that BICS acts as data controller and sends the data to its subsidiary TeleSign for fraud monitoring and detection.

65. The SCCs signed with TeleSign and mentioned above (see Section 2.3.2, Exhibit 7) refer to the following purposes:

    - improvement of TeleSign's score product, for which the data is transferred to TeleSign, which acts as data controller;
    - assistance to BICS's fraud prevention capabilities for which data is transferred to TeleSign acting as a sub-contractor to BICS.

3.2.1 Failure to provide information

66. BICS has never informed users of the processing of their data or of the existence of a transfer of their data to TeleSign. By not providing any information to users, BICS has not fulfilled its transparency obligations, and in particular those set out in Article 14 of the GDPR, in particular by not informing subscribers:
    - of its identity;
    - the identity of its DPO ;
    - the purposes of the processing and the legal basis ;
    - categories of data processed and sent to TeleSign ;
    - the recipient or recipients of the data, including TeleSign; and
    - whether data is transferred outside the EU, and the appropriate safeguards used.

67. As a result, BICS has breached its obligation to provide information and transparency, and in particular Articles 5.1.a and 14 of the GDPR.

3.2.2 Unlawful use of data and misappropriation of purpose

a) Reminder of the legal framework concerning the use of electronic communications data

68. Both BICS and Proximus are operators subject to the law of 13 June 2005 on electronic communications. This law transposes the Directive on privacy and electronic communications[27] into national law and strictly defines the conditions under which communications data may be processed by electronic communications operators.

69. Article 122 §1 of the law of 13 June 2005 states that *"Operators shall delete traffic data concerning subscribers or end-users from their traffic data or render such data anonymous, as soon as they are no longer necessary for the transmission of the communication".*

[27] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

70. Article 122 provides for some limited derogations from the prohibition in §1, allowing operators to retain the data in question without prejudice to the GDPR and the duty to inform users of the type of data processed, the precise purposes and the duration of the processing:

    - for the sole purpose of billing and paying for interconnection (see article 122 §2 of the law of 13 June 2005),
    - for marketing purposes and to offer a better price plan to users, with their consent (see article 122§3 of the law of 13 June 2005),
    - for the purposes of taking appropriate, proportionate, preventive and curative measures, taking into account the latest technical possibilities, in order to detect fraud and malicious use of their networks and services and to prevent end-users from suffering harm or inconvenience (article 122 §4 *juncto* article 121/8 §1 of the law of 13 June 2005),
    - for the purposes of establishing fraud or malicious use of the network or service or identifying its author and origin, and insofar as it processes or generates them in connection with the provision of this network or service (article 122 §4 of the law of 13 June 2005).

71. In all cases, Article 122(5) states that *"the data listed in this Article may be processed only by persons entrusted by the operator with billing or traffic management, handling subscriber enquiries, combating fraud or malicious use of the network, network security, complying with its legal obligations, marketing its own electronic communications services or providing services which make use of traffic or location data"*.

72. It should also be noted that Article 123 of the same law provides that mobile network operators may retain location data other than traffic data in the following cases:
    - where necessary for the proper functioning and security of the network or service, data being retained for as long as is necessary for this purpose;
    - where this is necessary to detect or analyse fraud or malicious use of the network, the data being kept for as long as is necessary for this purpose;
    - when the data have been rendered anonymous ;
    - where the processing is part of the provision of a traffic or location data service and the subscriber or, where applicable, the end user, has given his consent;
    - where processing is necessary to comply with a legal obligation on the part of the operator.

73. The law of 20 July 2022, which came into force on 18 August 2022, defines the concept of "fraud" as *"a dishonest act carried out with the intention of deceiving by contravening the law, regulations or the contract and of obtaining for oneself or for another an unlawful advantage to the detriment of the operator or the end user, committed through the use of an electronic communications service"*.

74. In this respect, reference is made to the critical opinion of the DPA concerning the exceptions mentioned above and introduced by the law of 20 July 2022.[28] The opinion points out in particular that the mere potential for fraud could not "*justify systematic preventive storage of traffic data of all users of an electronic communication medium necessary to combat fraud and malicious use of the network*". [29]

b) The processing of data by BICS in accordance with the above principles

75. It appears from the information received by the complainants that BICS not only does not delete user data, but transmits it to TeleSign for purposes other than the transmission of the communication, in flagrant violation of Articles 122 et seq. of the Law of 13 June 2005.

76. In its responses to the complainants' access requests, (Exhibit 6) BICS invokes its legitimate interest and the detection and prevention of fraud as the basis for the lawfulness of the transfer of data to TeleSign.

77. However, the transfer of the data to TeleSign and its use to allocate scores to telephone numbers and for other obscure "fraud prevention" purposes do not comply with the exceptions set out in §§ 2 et seq. of Article 122 of the Law of 13 June 2005, which are to be interpreted strictly. The following elements in particular should be taken into account:

- the systematic and massive transfer[30] of all telephone numbers to TeleSign so that the latter can assign a score to each number is not proportionate: it amounts to putting on file all users whose communications transit through BICS, even though such systematic retention of data for police and judicial purposes is only permitted under very strict conditions,[31]
- TeleSign's scoring service is not designed to detect fraud and malicious use of their networks and services and prevent end-users from being harmed or inconvenienced, but rather to process all traffic data to generate significant revenue and sell a solution to customers who are not electronic communications operators under the guise of "fraud prevention "[32], and
- the data is not processed or generated as part of the provision of this network or service but by a third party for uses unrelated to the operation of electronic communications networks and services.

---

[28] APD opinion no. 108/2021 of 18 June 2021.

[29] According to the DPA opinion (no. 108/2021, p. 31), "*any person can, potentially, commit a "fraud" or a "malicious use of the network" or, be a victim thereof, but this potentiality - which also exists for serious crimes, the combating of which was the objective of the regulation to which the CJEU judgment related - cannot, under the case law of the CJEU, be considered sufficient to justify the systematic preventive retention of traffic data of all users of a means of electronic communication necessary to combat fraud and malicious use of the network*".

[30] And framed by SCCs and a contractual obligation for BICS to provide this data to TeleSign.

[31] CJEU, Judgment of 8 April 2014, Digital Rights Ireland and Others, C-293/12 and C-594/12, Judgment of 21 December 2016, Tele2 Sverige and Watson and Others, C-203/15 and C-698/15, Judgment of 2 October 2018, Ministerio Fiscal, C-207/16, Judgments of 6 October 2020, Privacy International, C-623/17, and La Quadrature du Net e.a., C-511/18, C-512/18 and C-520/18, Cour Const. judgment of 22 April 2021, 54/2021.

[32] Note that the "Controller to Controller" Module 1 used for the transfer of data from BICS to TeleSign refers to "improving TeleSign's score product". See page 13 of the SCCs between BICS and TeleSign, Exhibit 7.

78. It should also be noted by BICS that the choice of "controller to controller" SCCs, in addition to "controller to processor" SCCs, allows TeleSign itself to define the purposes and means of processing these data, without any legal basis, information to users, or derogation from the strict conditions surrounding the use of the aforementioned electronic communications data.

79. Consequently, BICS violated at least :

- Article 5(1)(e) of the RGPD and Article 122 of the Law of 13 June 2005 by storing data for a period exceeding the storage period necessary for the provision of interconnection services;
- articles 5.1.b) and c) and 6 of the RGPD by using user data for purposes that are incompatible with the uses permitted under article 122 of the law of 13 June 2005.

3.2.3 Transfer of data to TeleSign not compliant with RGPD

80. BICS transferred the data to TeleSign, a provider of electronic communication services at meaning of of §1881a of title 50 of the U.S. Code and, as such, is subject to surveillance by the U.S. intelligence services under §1881a of title 50 of the U.S. Code ("FISA 702").

81. However, in its *Schrems II* judgment[33] , the CJEU explicitly concluded that subsequent transfers to companies covered by §1881a of Title 50 of the U.S. Code not only violate the relevant articles of Chapter 5 of the GDPR but also Articles 7 and 8 of the Charter of Fundamental Rights and the essence of Article 47 of the same Charter.[34] Any new transfer therefore violates the fundamental right to privacy, data protection and the right to an effective remedy and a fair trial.

82. Under the *Schrems II* judgment cited above, the SCCs cannot guarantee the transfer of data without additional guarantees protecting them against access by the US supervisory authorities under their national law (see paragraphs 134 and 135 of the judgment).

83. However, as mentioned above, according to the information provided by BICS itself, the additional measures to ensure data protection can be summarised as follows:

- data minimization ;
- pseudonymisation ;
- encryption ;
- transfer via SFTP protocol ;
- a strict data access policy; and
- file access and audit rights.

[33] Decision of the CJEU, 20 July 2020, C-311/18.

[34] See §95 of the *Schrems II* decision.

84. It is impossible to conclude that these "additional measures" (which are very vaguely described, and which are more like basic security measures for processing of this kind) guarantee that the competent US authorities will not be able to access the data sent by BICS to TeleSign.

85. BICS has therefore breached Articles 44 et seq. of Chapter V of the GDPR by transferring data without appropriate safeguards.

86. According to the *Schrems II* judgment, the competent supervisory authority must suspend or terminate the transfer of personal data to the third country concerned pursuant to Article 58(2),
(f) and (j) of the GDPR (see paragraphs 134 and 135 of the judgment).

87. In addition, as developed above (section 3.2.2), BICS carried out a massive, recurrent and repeated transfer of data to TeleSign, by virtue of SCCs (Module 1) giving TeleSign the status of data controller for a purpose that is totally incompatible with the Law of 13 June 2005. Consequently, the legitimate interest in the detection and prevention of fraud invoked by BICS cannot justify such a transfer of data to TeleSign. BICS is therefore also in breach of Articles 6 and 14 of the GDPR, by carrying out processing (the transfer in question) without any legal basis and without informing users.

3.3 Data processing by TeleSign

3.3.1 TeleSign failed in its duty to inform complainants

88. First of all, it should be noted that it was only thanks to the revelations in the newspaper *Le Soir* (see above, section 2.3) that the complainants were informed that they were being put on file and profiled by an American company of which they had never heard. And with good reason: TeleSign had never informed them of the treatment they were receiving.

89. Following their requests for access, they also realised - much to their surprise - that this company was in fact awarding them a score, which was shared with TeleSign customers, again without them being informed (see responses to the complainants, Exhibit 8).

90. TeleSign proceeded to process the data of millions of telephone users without even providing them with the beginnings of information about this processing. Article 14 of the RGPD could not be clearer about the obligation to inform data subjects. The same applies to Article 8.2 of the SCCs signed with BICS, which requires the importer of the data, i.e. TeleSign, to inform the data subjects so that they can effectively exercise their rights under Article 10 of the SCCs. Without information, and without information in the press, the complainants would still be unaware of the processing operations at issue in this complaint.

91. Even more, when several complainants returned to TeleSign in 2023 to obtain all of the information legally required under Article 15 of the GDPR, TeleSign responded that the complainants' data had been deleted, and that TeleSign was therefore not in a position to provide the information required under Article 15 of the GDPR.

therefore no longer able to answer the question of how long the data was kept (see for example TeleSign's response of 25 March 2023 to [redacted], Exhibit 8.3a).

92. Furthermore, when asked by the complainants for clarification as to why the complainant's data had been deleted and was no longer considered necessary by TeleSign, TeleSign considered that this response went beyond its obligations under Article 15 of the GDPR.

93. However, Article 15.1.d of the RGPD expressly states that the controller must inform data subjects of *"where possible, the intended retention period of the personal data or, where that is not possible, the criteria used to determine that period"*. It has to be said that TeleSign has not responded to this request, despite the clear wording of Article 15.1.d of the GDPR.

94. It follows from the foregoing that TeleSign therefore failed in its duty to provide information by not providing any information prior to the first request for access, but also at the time of subsequent requests. TeleSign has therefore at the very least breached Articles 5.1.a, 12, 14 and 15 of the GDPR, and Article 8.2 of the SCCs signed with BICS.

3.3.2 TeleSign processes complainants' data without a valid legal basis within the meaning of the RGPD and the law.

of 13 June 2005 and in breach of the SCCs

95. TeleSign considers that it processes data on the basis of legitimate interest within the meaning of Article 6.1.f of the GDPR, for reasons of *"fraud prevention, protection against spamming, phishing, promotion abuse, fake accounts, unlawful account takeovers and any other attack entailing costs"* (see for example response to [redacted] see Exhibit 8.3).[35]

96. However, under the terms of the SCCs signed with BICS, TeleSign receives data from BICS for two purposes:

- "TeleSign's Score product enhancement" when TeleSign receives the data as the data controller receiving the data from BICS (Exhibit 7, Module 1, table page 13),
- "BICS fraud prevention assistance" where TeleSign receives data as a subcontractor receiving data from BICS (Exhibit 7, Module 2, table page 31).

97. As regards the use of the data for the purpose of improving Telesign's Score product, it has to be said that improving a product that assigns a confidence score is not compatible with the initial processing of the data by BICS, as already explained above (see section 3.2.2). Clearly, if a processing operation is not compatible with the strict purposes prescribed by the Law of 13 June 2005, simply transferring it to a third company cannot allow it to be used freely without the same restrictions, otherwise the principles of the Directive on privacy and electronic communications would be rendered meaningless.[36]

---

[35] *"Our phone number reputation and risk assessment tool is offered to our customers for fraud prevention purposes; protecting against spam, phishing, promotion abuse, fake accounts, account takeovers and other costly attacks.*

[36] It would be sufficient for an operator subject to the strict conditions of the Law of 13 June 2005 to transfer the data to an operator that is not, in order to make free use of the data.

98. Moreover, even though the link between these different purposes is not clear to the complainants who received the information from TeleSign, it should be noted that TeleSign is in breach of Article 8.1 of the SCCs (Module 1) when it processes the data received from BICS, since it uses them for purposes[37] other than those described in the SCCs ("improvement of TeleSign's score product").

99. Finally, as already developed (section 3.2.2), the choice of "controller to controller" SCCs, in addition to "controller to processor" SCCs, is likely to allow TeleSign to define the purposes and means of processing this data itself, without any legal basis, information to users, or derogation from the strict conditions surrounding the use of the aforementioned electronic communications data.

100. With regard to "BICS's assistance in fraud prevention", it has already been pointed out that, in the light of the information available to the complainants, the fraud prevention purposes of BICS - and at the very least of TeleSign - do not fall within the exceptions of the "fraud prevention" provisions.
§§4 et seq. of Article 122 of the Law of 13 June 2005. However, it remains difficult to distinguish between processing operations for which TeleSign is a data controller or a data processor, despite an update by TeleSign in a March 2023 version of its privacy notice, in which TeleSign attempts to clarify in which cases it is acting as a data processor or data controller.

101. It follows from the foregoing that TeleSign is in breach of Articles 5.1 and 6 of the GDPR, as well as Article
8.1 of the SCCs signed with BICS, in conjunction with articles 122 et seq. of the law of 13 June 2005.

3.3.3 TeleSign is unlawfully profiling and making automated decisions

102. TeleSign evaluates telephone number user profiles using algorithms to detect users even before they create an account with its customers.[38]

103. TeleSign is therefore profiling and taking automated decisions within the meaning of Article 22 of the GDPR. Indeed, TeleSign's score product is indisputably a profiling tool (which is moreover based on unlawful processing, see section 3.3.2 above), defined by Article 4 of the GDPR as "*any form of automated processing of personal data which consists in using such personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict factors concerning the*

---

[37] "*Fraud prevention, protection against spamming, phishing, promotion abuse, fake accounts, illicit account takeovers and any other attack resulting in costs".*

[38] *"Leveraging our proprietary insight into the volume of traffic around the world and the data captured by our products, we've developed the ability to predict potential fraud based on a variety of phone attributes, machine learning algorithms, data and behavioral patterns.*

Today our expanded products and solutions allow you to both preserve your ecosystem and your user base by detecting a suspicious user before account creation and identifying and blocking account takeover attacks before they occur.", taken from the TeleSign website: https://www.telesign.com/security.

work performance, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements of that natural person".

104. TeleSign also implements an automated decision-making system within the meaning of Article 22 of the RGPD. TeleSign establishes a "score" of the users concerned and shares them with its "customers" who then adopt a decision on the basis of this score.

105. Advocate General Pikamäe has recently held, in relation to a similar treatment, that *"The automated establishment of a probability value relating to the ability of the data subject to honour a loan in the future already constitutes a decision based exclusively on automated processing, including profiling, producing legal effects concerning that person or affecting him significantly in a similar way where that value, established by means of personal data relating to that person, is communicated by the controller to a third party controller and, in accordance with established practice, the latter bases its decision relating to the establishment, performance or termination of a contractual relationship with that person decisively on that value".*[39]

106. This profiling is even more alarming when it is noted that none of the complainants had been informed that their data had been transferred to TeleSign to be profiled without their knowledge. No information on the profiling was given to the people concerned, and the precise purposes of this scoring are still unclear to the complainants (who are these customers to whom TeleSign provides scores, when, why and on what basis?)

107. It follows from the above that TeleSign has carried out (and is still carrying out) unlawful processing under Article 22 of the GDPR. TeleSign should be ordered to cease such processing without prejudice to any other appropriate remedies against TeleSign.

3.3.4 Infringement of rules on transfers outside the EU

108. For the reasons already set out above in Section 3.2.3, the transfer of telephony user data to TeleSign violates the provisions of Chapter V of the GDPR insofar as TeleSign is a company falling under the US FISA.

109. Additional measures adopted by TeleSign include the following[40] :

- data minimization ;
- pseudonymisation (hashing) ;
- encryption with AWS ;
- transfer via SFTP protocol ;
- strict security and privacy policies; and
- use of the Commission's new standard clauses .

110. As already developed above in Section 3.2.3, these measures cannot be considered sufficient under the *Schrems II* case law of the Court of Justice. We

[39] Advocate General's Opinion of 16 March 2023 in Case C-634/21 *OQ v Land Hessen*.

[40] See, for example, responses to [redacted], [redacted] or [redacted], Parts 8.

It should also be noted that TeleSign refers to the standard clauses as "additional measures", whereas the signing of these standard clauses is the minimum legally required for the transfer of data. It is therefore hard to see how they would be
"additional".

111. By virtue of the foregoing, TeleSign also breached Article 14 of the SCCs signed with BICS for, inter alia, failing to notify BICS of the existence of legislation preventing it from fulfilling its obligations as an importer of the data.

3.3.5 Illegal onward transfers

a) Transfers to Microsoft

112. As explained above (see §§49 et seq.), TeleSign transferred the complainants' data and to Microsoft c[redacted]SC[redacted]ted to the complainants (Exhibit 11). It is impossible to know in particular when these SCCs were signed, the transfers they cover, and the security measures undertaken, since all this information is simply non-existent in the document.

113. It is therefore certain that these contractual clauses do not provide the appropriate guarantees for a subsequent transfer of the data, and in any event do not provide the same level of protection as the clauses signed between BICS and TeleSign. This transfer therefore violates Article 8.7 of the SCCs in question, and more specifically Article 8.7.iii).

b) Transfers to AWS

114. As developed above (§§47 et seq.), TeleSign confirmed transferred the data with AWS. TeleSign shared SCCs dated 12 December 2016 surrounding this transfer (Exhibit 9). These SCCs list AWS as a subcontractor.

- These SCCs are those adopted by the European Commission in its Decision 2010/87 of 5 February 2010, which was repealed on 26 September 2021. Furthermore, it is not specified whether the exporter of the data, TeleSign here, is acting as data controller, data processor, or in both capacities.
- Clause 2 on the details of the transfer refers to the description in Appendix 1, which simply states that the categories of data transferred are data about individuals who are loaded onto AWS services by the exporter of the data, without any further details.
- Appendix 2 refers to safety measures described in an addendum which was not sent to the complainants.

115. In these circumstances, it is submitted that TeleSign is in breach of Article 8.1 of the SCCs signed with BICS by making a subsequent transfer that does not comply with its contractual obligations.

c) Transfers to Amazon LLC

116. TeleSign also shared with [redacted] a copy of the SCCs for transfers with AMAZON SERVICES LLC (Exhibit 10 AMAZON LLC SCCS, see section 2.3.3). However, the document provided by TeleSign is a pure copy of the European Commission's SCCs, without having been filled in, signed, dated, and without even having indicated which modules were relevant or who was the exporter and importer of the data. To date, the complainant has no further information about this transfer.

117. In these circumstances, it is submitted that TeleSign is also in breach of Article 8.1 of the SCCs signed with BICS by carrying out a subsequent transfer that does not comply with its contractual obligations.

3.3.6 Accuracy and limitation of data retention

118. In accordance with Article 8.3 of the SCCs signed by TeleSign with BICS, TeleSign is obliged to ensure that data is adequate, relevant and limited to what is necessary for the purpose(s) of processing. In addition, article 8.4 of the same SCCs states that the importer may not keep the data longer than necessary and shall put in place the technical and organisational measures to guarantee compliance with this obligation. In line with the principle of accountability set out in Article 5.2 of the RGPD, Article 8.9 of the SCCs signed with BICS stipulates that each party must be able to demonstrate its obligations, in particular by documenting the processing activities carried out under its responsibility.

119. Nonetheless, it appears that following a further request for information from several of the complainants, TeleSign informed them that their data was no longer being processed and that, as a result, TeleSign could no longer tell them when the processing of their data began or when it ceased (see Exhibits 8.1.a, 8.2.a, 8.3.a, 8.4.a, 8.7.a and 8.10a).

120. Furthermore, when asked why the complainants' data, which seemed so necessary for the purposes pursued by TeleSign (i.e. scoring telephone numbers for their customers) was suddenly no longer necessary when the complainants contacted TeleSign again, TeleSign considered that this information fell outside the scope of Article 15 of the GDPR.[41]

121. It also states that the fact that the data is no longer processed by TeleSign
This "does not prevent TeleSign from receiving complainants' telephone numbers from their partners in the future in order to provide them with the scoring service". How and why would TeleSign still receive the telephone number from third parties to provide a score based on a number that TeleSign claims it no longer processes? TeleSign does not explain.

[41] *"While we appreciate your inquiry in this respect, it goes beyond the scope of Article 15 of the GDPR.*
We do nevertheless wish to point out that although your personal data ceased to be used for fraud prevention in the context of Score, we cannot prevent our current and future customers, with whom you share your phone number, from sharing your phone number with us (again) in connection with the services that we provide to them".

122. Under the principle of responsibility, necessity (underlying Article 6.1.f of the GDPR) and data limitation, it is clear that TeleSign should be able to answer questions concerning:

- how long the data received will be retained. If the answer to this question cannot relate to specific data, the retention policy should at least allow TeleSign to answer the question in accordance with Article 14.2a. of the GDPR,
- the justification of the need (and *a contrario* the disappearance of this need) to process the data for the purpose put forward (in this case, the prevention of fraud on the basis of legitimate interest within the meaning of Article 6.1.f of the RGPD),
- justification of the above even after processing, on the basis of up-to-date documentation describing the processing processes implemented and the conditions surrounding them.

123. On the basis of the foregoing, it is submitted that TeleSign has at the very least infringed Articles

5.1.e, 5.2, and 24 of the GDPR, as well as articles 8.3, 8.4 and 8.9 of the SCCs signed with BICS.

4. CONCLUSION

4.1 Reservations concerning this complaint

124. The content of this complaint is without prejudice to any new factual elements or possible breaches that may be revealed in the course of the proceedings on the basis of the findings and information provided by and to the DPA and any other party in the course of the proceedings.

125. Given the lack of transparency regarding the various processing operations concerned, it is difficult for complainants to understand them and to assert their rights properly and effectively.

126. It appears that TeleSign updated its privacy policy in March 2023.[42] The purpose announced by TeleSign on its web page is, in particular, to make this policy clearer, to make it explicit when TeleSign or its customers are acting as data controller or data processor, and to provide more details on why TeleSign processes data, how it uses it and for what purposes.

127. It cannot be ruled out that TeleSign, becoming aware of the complainants' requests, not only changed its privacy notice, but also its practices, for example, by adopting a data retention policy or by modifying the data processing concerned. In any event, it is submitted that the changes made by TeleSign after the access requests did not prevent the various breaches referred to in this complaint from actually having occurred, and that they are likely to have affected several million users, not just the complainants.

128. In this context, *noyb* also reserves the right to attach new documents, to add new elements, to raise other points of law and to represent other plaintiffs in these proceedings.

4.2 Request for investigation

129. The supervisory authority is asked to investigate the processing operations covered by this complaint, in particular

- obtain confirmation that the complainants' data has been, or is still being, processed by TeleSign and for what purposes;
- to obtain more information about the various transfers made by BICS to TeleSign and vice versa, in particular as regards their legal basis and precise purposes;
- to obtain complete and intelligible information about TeleSign's processing of complainants' data; and
- to request from any other party not yet identified in this complaint the information necessary for the investigation and resolution of the complaint.

[42] https://www.telesign.com/our-updated-privacy-notice-protecting-you-and-your-identity.

4.3 Corrective measures

130. In addition to acknowledging the breaches of the complainants' rights and of the legal provisions identified in this complaint (and subject to any other breaches that may be identified by the complainants or the DPA in the course of the proceedings, in particular by its inspection service), the DPA should issue at least the following remedies:

- the cessation of transfers from BICS to TeleSign ;
- the cessation of all data processing by TeleSign;
- deletion of unlawfully transferred and processed data;
- the obligation on all parties involved to inform complainants and any data subjects of past processing operations and the fate of their data;
- the imposition of an appropriate fine, taking into account not only the seriousness of the breaches observed, but also the potentially very large number of people concerned and the profit made by the companies concerned from their illegal processing activities.

4.4 Contact and communication

131. For any contact, the authority can contact *noyb* by email at [redacted] under reference C-063.

132. As the complaint was lodged in French, the language of the proceedings will also be French.

Vienna, 23 June 2023

[redacted]