EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR MOBILITY AND TRANSPORT

Director-General

Brussels,

Mr Edward Hasbrouck

By e-mail: edward@hasbrouck.org

Subject: Complaint against Sabre, Travelport and Amadeus on an alleged infringement regarding Regulation (EC) 80/2009

Letter rejecting your complaint

Dear Mr Hasbrouck,

(1) I refer to your complaint against Sabre, Travelport and Amadeus regarding an alleged infringement of Regulation (EC) No 80/2009 (hereby the "Code of Conduct")[1].

(2) I wish to inform you that, for the reasons set out below, the Commission intends to reject your complaint.

1. THE COMPLAINT

(3) By e-mail dated 28 February 2017 and e-mail dated 24 April 2017 you alleged a breach of Regulation (EC) No 80/2009 on a Code of Conduct for computerised reservation systems ("the Code of Conduct") by Sabre, Travelport, and Amadeus by insufficiently protecting personal data. You confirmed your allegations by e-mail of 8 May 2017.

(4) You allege that the three CRS providers Sabre, Travelport, and Amadeus make personal data available to anyone who has the name of the traveller in a "passenger name record" (PNR) and who has the "record locator" assigned by the CRS. In your opinion, this would constitute an infringement of Article 11 of Regulation No 80/2009 on a Code of Conduct for Computerised Reservation Systems which requires that "*technical and organisational measures shall be taken ... to ensure that personal data are only accessible for the specific purpose for which they were collected.*"

(5) In the airline industry, a PNR is a record in the database of a computerised reservation system (CRS) that consists of the personal information for a passenger and also contains the itinerary for the passenger, or a group of passengers travelling together. When a passenger books an itinerary at a travel agency, the travel agent will create a PNR in the CRS, which may be an airline's database or typically one of the global providers of CRSs, such as Amadeus, Sabre, or Travelport. A PNR includes

[1] Regulation (EC) No 80/2009 of the European Parliament and of the Council of 14 January 2009 on a Code of Conduct for computerised reservation systems and repealing Council Regulation (EEC) No 2299/89 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009R0080&from=EN

Commission européenne/Europese Commissie, 1049 Bruxelles/Brussel, BELGIQUE/BELGIË - Tel. +32 22991111
Office: DM28 8/101 - Tel. direct line +32 229-88764

Henrik.Hololei@ec.europa.eu

information such as the name of the passenger, travel dates, itineraries, seats, baggage, contact details and means of payment.

(6) The PNR is identified in the CRS by a record locator. A record locator is an alphanumeric or alpha code, typically 6 characters in length, used to access a specific record. If one puts the record locator number into the computer system, the PNR comes up.

(7) You explain that personal data would be made available on the basis of the name and the record locator through public Web sites operated by each of the three largest CRS system operators: VirtuallyThere.com (Sabre), ViewTrip.com (Travelport), and CheckMyTrip.com (Amadeus).

(8) You consider that the record locator for each PNR is not a password, but is used as though it were a password. It is short enough to be guessed by, in your terms, "brute force". More importantly, it is assigned by the CRS, and cannot be changed if compromised. It is printed (or encoded in unencrypted bar-code format) on boarding passes, baggage labels, and itineraries. Record locators do not comply with any commercial norms for passwords or for technical measures for data protection.

(9) You also point out that there are no purpose (or geographic) restrictions on access to data stored in Sabre, Travelport, or Amadeus. Users of these systems are not required to indicate the purpose for which PNR or other data are retrieved. No technical measures whatsoever are used to enforce any purpose limitations on access to personal data. Access to personal data is not logged, so it is impossible to audit the purposes for which personal data has been accessed or the countries to which personal data has been transferred in response to queries by CRS users.

(10) You request that the Commission imposes appropriate sanctions and corrective orders including "*mandating standard technical and policy measures including (a) user-designated and user-changaeble passwords for access to personal data and (b) system-level access logging including logging of the user, the stated purpose of access, and the geographic location of the user*". You also request the Commission to "*impose appropriate financial sanctions*", namely the maximum financial penalty allowed by law against each of these CRS system operators.

2. THE APPLICABLE LEGAL FRAMEWORK

(11) Article 13 of the Code of Conduct provides that the Commission upon finding an infringement of the Code of Conduct may require that the entity concerned brings such an infringement to an end. It follows that, under the Code of Conduct the Commission has the competence to require the relevant entities to remedy such an infringement only when the infringement concerns the provisions of the Code of Conduct.[2]

(12) Article 11(10), which you quote in your complaint and which you consider that Sabre, Travelport and Amadeus infringe, provides that:

---

2 Moreover, the intention of the legislator, at the time of drafting the Code of Conduct, as can be seen from Article 13 of the Code of Conduct, was to curtail any abuse of a dominant position of an undertaking and prevent any unfair trading in order to maintain effective competition between industry players.

"Where a system vendor operates databases in different capacities such as, as a CRS, or as a host for airlines, technical and organisational measures shall be taken to prevent the circumvention of data protection rules through the interconnection between the databases, and to ensure that personal data are only accessible for the specific purpose for which they were collected."

(13) That provisions forms part of Article 11 of the Code of Conduct which contains various provisions on the processing, access and storage of personal data collected in the course of the activities of a CRS. Those provisions were intended to particularise and complement the horizontally applicable EU data protection rules, which, at the time of the adoption of the Code of Conduct in 2009, were contained in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p.31). Directive 95/46/EC was repealed and replaced by 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 (OJ L 119, 4.5.2016, p. 1). Regulation (EU) 2016/679 applies since 25 May 2018 (GDPR).[3]

(14) The following provisions of Article 11 are of relevance for personal data:

- Paragraphs 1 and 2 which impose a generally recognised rule that personal data shall be processed only in line with the purpose for which the data controller received such data: i.e. paragraph 1 "*Personal data collected in the course of the activities of a CRS for the purpose of making reservations or issuing tickets for transport products shall only be processed in a way compatible with these purposes"*, and *"Personal data shall only be processed in so far as processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract*";

- Paragraph 3 which repeats a general rule on the need to give explicit and well informed consent to the processing;

- Paragraph 7 which repeats a general rule that the access to personal data related to a data subject shall be free of charge;

- Paragraphs 4, 5 and 10 containing specific provisions on the processing, storage and access to personal data managed by CRS, namely the specifiifities of offline storage (paragraph 4), treatment of marketing, booking and sales data (paragraph 5) and obligation to take technical and organisational measures to separate databases when a CRS vendor is also a host for airlines (paragraph 10).

3. ASSESSMENT OF THE COMPLAINT

(15) Article 11(10) to which you refer deals with a situation in which a system vendor operates databases in different capacities such as a CRS or a host for airlines. The aim of this provision is to ensure that there are no interconnection between these databases, so that data from various databases would not be accessed and used for purposes other than for which it has been collected.

3 Article 9(2) of the GDPR: "References to the repealed Directive shall be construed as references to this Regulation."

(16) This interpretation is confirmed by the documents produced during the legislative process of the Code of Conduct. The report of the European Parliament which introduced this provision confirms that its aim is to reinforce "the Chinese wall" between CRS and hosting activities[4].

(17) The situation that you describe does not concern a situation in which a system vendor operates databases in different capacities such as a CRS or a host for airlines. Article 11(10) thus does not apply to the situation you described. There are thus no grounds to act on the complaint on the basis of this paragraph.

(18) As regards the possible infringement of other provisions of Article 11, none of the specific provisions contained in that Article on the processing, access and storage of personal data by CRS applies to the situation described in your complainant.

(19) The situation you described might raise issues of data security which is regulated in the GDPR and not in the Code of Conduct. The GDPR provides rules on the secure processing of personal data, in particular in section 2 in Chapter IV.

(20) Without prejudice to the powers of the Commission as a guardian of the Treaties, the monitoring and enforcement of the application of the GDPR falls primarily under the competence of the national supervisory authorities (see Article 51 of the GDPR).

(21) Chapter VIII of the GDPR contains rules on the possibility to lodge a complant with a supervisory authority (in particular in the Member State of complainant's habitual residence, place of work or place of the alleged infringement). Chapter VIII of the GDPR also contains further remedies available to an aggrieved person.

(22) It follows from the above that it would in the first place be for the relevant supervisory authority to assess whether the situation you described indeed complies with the GDPR rules on security of personal data.

4. CONCLUSION

(23) In light of the circumstances set out above, and on the basis of the information in its possession, the Commission considers that there are no indications that the CRS providers (Sabre, Travelport, and Amadeus) infringe Article 11 of the Code of Conduct.

(24) The Commission therefore concludes that there are insufficient grounds to act on your complaint pursuant to Article 16(3) of the Code of Conduct.

(25) The complainant can consider launching a complaint pursuant to the GDPR to a relevant supervisory authority.

5. FINAL PROCEDURAL COMMENTS

(26) In accordance with Article 16(3) of the Code of Conduct, you may choose to submit written observations on this letter. The time-limit for submitting observations expires

---

[4] Report of the European Parliament on the proposal for a regulation of the European Parliament and of the Council on a Code of Conduct for computerised reservation systems, 10 June 2008, A6-0248/2008, amendment 39, available at:

http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A6-2008-0248+0+DOC+XML+V0//EN

eight weeks from the date of receipt of this letter. Please note that the Commission is not obliged to take into account any submissions made after the expiry of the time limit.

(27) If you do not submit written observations within the time limit, your complaint shall be deemed to have been withdrawn.

(28) If you consider that certain parts of this letter contain confidential information, please inform Mr Christophe Dussart (e-mail: christophe.dussart@ec.europa.eu) and Ms Sabine Crome (e-mail: sabine.crome@ec.europa.eu) within two weeks of the date of receipt of this letter. Please identify clearly confidential information and substantiate reasons for confidential treatment.

(29) If you decide to submit written observations on this letter and those observations would contain confidential information, please submit also a non-confidential version of those observations.

Yours sincerely,

Henrik HOLOLEI