THE PRACTICAL NOMAD

EDWARD HASBROUCK

1130 Treat Avenue, San Francisco, CA 94110, USA
phone +1-415-824-0214
edward@hasbrouck.org
https://hasbrouck.org

The Practical Nomad: How to Travel Around the World
The Practical Nomad Guide to the Online Travel Marketplace
Avalon Travel Publishing (Perseus Books Group / Hachette)
https://practicalnomad.com

"The Practical Nomad" books and Web site are written by union labor:
Member, National Writers Union (UAW Local 1981, AFL/CIO)

Director-General Henrik HOLOLEI
European Commission
Directorate-General for Mobility and Transport (DG MOVE)
Unit E1 – Aviation Policy
B-1049 Brussels
BELGIUM

by e-mail: move-infos@ec.europa.eu

Re: Your letter of 18 June 2019 proposing to reject my complaint against Sabre, Travelport, and Amadeus for infringement of Regulation (EC) 80/2009

Your reference: Ares(2019)388-4257-18/06/2019

Dear Director-General Hololei:

I have received your letter of 18 June 2019 whereby you inform me that the European Commission intends to reject my complaint against Sabre, Travelport, and Amadeus – the three dominant computerized reservation systems subject to the "Code of Conduct for Computerized Reservation Systems" imposed by Regulation (EC) 80/2009 and subject to enforcement by the Commission through your Directorate.

Pursuant to Article 16(3) of the Code of Conduct, the following are my views concerning your proposal to deny my complaint.

I believe that your proposed rationale for denial of my complaint is fundamentally in error with respect to the factual allegations and the nature of the complaint itself, the applicability of the Code of Conduct to the actions forming the basis for this complaint, and the extent of, and reasons for, the Commission's jurisdiction to act on this complaint.

Dismissal of this complaint for lack of jurisdiction, as contemplated by your letter, would amount to an abrogation of the Commission's responsibility to enforce the Code of Conduct, contrary to the intention of the legislation, the reasons why provisions for the protection of personal data were included in the Code of Conduct, and the reasons the Commission was given jurisdiction – independently out of and in parallel with other data protection authorities – for the enforcement of these provisions of the Code of Conduct.

According to your letter (footnote 2. p.2), " the intention of the legislat[ure] 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."

While this may be true of the legislature's intent with respect to some portions of the Code of Conduct, this is clearly neither true nor relevant with respect to Article 11 of the Code of Conduct, which concerns the processing, access, and storage of personal data.

The rights guaranteed by Article 11 of the Code of Conduct are personal rights of data subjects, which do not depend on, and are entirely independent of, any rights of "industry players" to protection against unfair competition.

Article 13 concerns the power of the Commission to investigate possible infringements of the Code of Conduct, acting on a complaint or on its own initiative, and to compel compliance with the Code of Conduct if infringements are found. Nothing in Article 13 excludes infringements of Article 11 from the Commission's authority to investigate or impose sanctions for infringements of any Article or provision of the Code of Conduct, or limits the Commission's authority to cases in which infringements of the Code of Conduct result from abuse of dominant positions or unfair trading or interfere with effective competition between industry players. Protection of personal data is an independent goal of the Code of Conduct, and infringements of Article 11 provide a basis for the exercise by the Commission of its powers of investigation pursuant to Article 13.

According to Paragraph 19 of your letter, "The situation you described might raise issues of data security which is regulated in the GDPR and not in the Code of Conduct." This is in error both because data security is, in fact, regulated by the Code of Conduct (as well as by the GDPR), and because whether data security is (also) regulated by the GDPR is independent of and irrelevant to whether it is (also) regulated by, and subject to the Commission's authority to enforce, the code of conduct – as in fact it is.

As for whether "data security" is regulated by the Code of Conduct, Article 11(10) of the Code of Conduct requires, as cited in my complaint, that, "Where a system vendor operates databases in different capacities such as, as a CRS, or as a host for airlines technical and organizational 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."

Paragraph 17 of your letter claims that, "The situation that you described does not concern a situation in which a system vendor operates databases in different capacities such as a CRS or host for airlines. Article 11(10) thus does not apply to the situation you described." This statement in your letter is unsupported, and is clearly and demonstrably false. In fact, as would be confirmed by even cursory investigation, Sabre, Travelport, and Amadeus each operate databases both as a CRS and as a host for airlines. Each is thus subject to the two requirements imposed by Article 11(10).

If the triggering condition is met ("Where a system vendor operates databases in different capacities such as, as a CRS or as a host for airlines"), then both of the two independent requirements of Article 11(10) apply. In such circumstances, a CRS must take measures both (A) "to prevent the circumvention of data protection rules through the interconnection between the databases" and (B) "to ensure that personal data are only accessible for the specific purpose for which they were collected."

These additional requirements were imposed in such cases because of recognition that commingling data collected by multiple entities for multiple purposes inevitably carries heightened risk of failure to keep track of, and to act in accordance with, the different purposes for which particular elements of the same record were collected, and that aggregated storage of data collected and potentially deemed to be controlled by different entities makes it more difficult for data subjects to know who is responsible for data protection or to obtain redress for violations of data protection rights in an environment of aggregated, outsourced cloud storage – of which CRSs were one of the first and remain one of the paradigmatic and most significant examples. It is deliberately and for good reason that the subjects of this complaint are subject to these requirements.

The two requirements of Article 11(10) are both, independently, being violated.

The risk to data subjects' rights is significantly enhanced by the interconnection of databases, including the aggregation of data collected from CRS subscribers and from host airlines as well as the connection of PNR and departure control system databases to public gateways and backend systems for PNR viewing and check-in Web sites. Many of these problems result from the failure to implement access controls when databases formerly accessible only to airline staff, contractors, and/or CRS subscribers were made accessible to the general public through these PNR viewing and check-in Web sites. Interconnection of databases with different purposes without adequate access controls is, in fact, one source (although not the only one) of the problem I have complained of.

Article 11(10) also requires in such cases that that measures be taken "to ensure that personal data are only accessible for the specific purpose for which they were collected." Adequate access controls are an essential element of such measures for purpose limitation. If personal data can be accessed – as, in fact, they can be, and as is the primary basis of my complaint – by anyone, from anywhere, for any purpose, without a password, then it is impossible to ensure that data is only accessible for the purpose for

which it was collected. Lack of adequate access controls necessarily implies and constitutes a failure to take adequate measures for purpose or geographic limitation.

Similarly, without access logging – a standard technical measure to enable auditing and oversight of access to data – it is likely to be impossible to ensure compliance with access limitations. Lack of access logging, which is another basis for my complaint, implies and constitutes a failure to take adequate measures to ensure compliance with purpose or geographic limitations on access, and is thus a violation of Article 11(10).

Similarly, each of the other provisions of Article 11 of the Code of Conduct pertaining to limitations on purposes for which personal data is processed effectively requires both adequate access controls and access logging to permit auditing and oversight. The claim in Paragraph 18 of your letter that, "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 complain[t]" is both unsupported and incorrect. Each of the provisions of Article 11 requiring limitations on the purposes for which personal data can be processed is implicated by the failure of the CRS operators to adequately control access to personal data, so that anyone, anywhere can obtain and process it for any purpose.

With respect to the relationship of the data protection provisions of the Code of Conduct to the GDPR, Article 11(8) of the Code of Conduct provides that, "The rights recognized in this Article are complementary to and shall exist in addition to the data subject rights laid down by Directive 95/46/EC [which was superseded by the GDPR], by the national provisions adopted pursuant thereto and by the provisions of international agreements to which the Community is party."

The Code of Conduct, including the data protection provisions in Article 11, were enacted consciously and deliberately in parallel with other data protection regulations. When the GDPR was enacted, it could have repealed the data protection provisions of the Code of Conduct or made them secondary to the GDPR – but deliberately did not do so.

The fact that a particular action might (also) be a violation of the GDPR, and might (also) give rise to rights of redress pursuant to the GDPR, cannot be deemed dispositive of whether that conduct is a violation of Article 11 of the Code of Conduct or whether the Commission has the right to investigate complaints and impose sanctions for that action as a violation of Article 11 of the Code of Conduct.

Paragraphs 20 and 21 of your letter describe rights of redress for violations of the GDPR. Paragraph 22 states that, "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."

This suggestion that a complainant must "in the first instance" bring a complaint of violation of Article 11 of the Code of Conduct to other data protection authorities pursuant to the GDPR, and may not choose to seek redress in the first instance from the Commission for a violation of Article 11 of the Code of Conduct, is clearly in error. It has

no support in the text of the Code of Conduct or that of the GDPR, and it directly contradicts the explicit provision of Article 11(8) of the Code of Conduct that, "The rights recognized in this article are complementary to and shall exist in addition to the data subject rights laid down by" the predecessor to the GDPR.

In paragraph 25 of your letter, you note that, "The complainant can consider launching a complaint pursuant to the GDPR to a relevant supervisory authority."

While that is correct, it is, as noted above, irrelevant to – and certainly not dispositive of – the Commission's jurisdiction to investigate and act on this complaint of violations of Article 11 of the Code of Conduct. And the reasons that I have, as is my right, chosen in the first instance to attempt to bring this complaint to the Commission pursuant to the Code of Conduct, rather then to other authorities pursuant to the GDPR, are exactly those reasons that led the legislature to grant the Commission *independent* authority to investigate and impose sanctions for violations of these data protection rules.

It is typically impossible for a traveler to determine, in advance, whether making an airline reservation or purchasing a ticket, whether through an airline Web site or through a travel agency or tour operator, will result in the transfer of data to one or more CRSs, and if so to which one(s). CRSs are explicitly defined as data controllers for purposes of the Code of Conduct, but are not necessarily controllers for purposes of the GDPR. The grant of jurisdiction to the Commission to enforce Article 11 of the Code of Conduct, and the definition of CRSs as data controllers for that purpose, were specifically included in the Code of Conduct to avoid situations in which CRSs would evade accountability and travellers would be denied redress because it is difficult or impossible to determine whether or which CRS or CRSs is or are data controllers, or which entity is responsible for protection of personal data included in aggregated CRS records that contain data in the same PNR or departure control system record that has been entered through multiple channels including airlines, travel agencies, and other parties.

Direct recourse to redress in the first instance through the Commission for these violations is the primary reason for the existence of Article 11 of the Code of Conduct.

In practice, only the CRSs themselves are in a position to implement the access controls and security measures, including passwords and access logging, that would be necessary in order for airlines or any CRS subscribers to be able to ensure adequate protection of personal data or to control dissemination and use of this data. Individual airlines or CRS subscribers cannot fix these vulnerabilities on their own. Enforcement by the Commission of Article 11 of the Code of Conduct is the appropriate and would be the most efficient and effective means of obtaining the desired protection of personal data.

It has now been more than two full years since your Directorate first acknowledged my complaint, and more than a decade since I first began trying to bring this complaint to the attention of the Commission. I urge you, without further delay, to investigate, uphold, and impose appropriate sanctions on the basis of this complaint, to compel the major CRS system operators to bring their systems into compliance with the Code of Conduct and with the data protection norms which are included in Article 11 of the Code of Conduct.

I will next be in Brussels in November 2019, and I would welcome an opportunity to meet with you and/or with your investigating team to discuss this complaint, the issues that it raises, and the measures that could be taken to address these violations.

I authorize publication of my complaint, your letter of 18 June 2019, and this letter, which I will also be publishing on my own Web site.

Sincerely,

Edward Hasbrouck