CEEMC 2014

Judgment of 27 April 2014

DISCLAIMER

For the purposes of the CEEMC 2014, the Court delivers the following judgment in the case regarding the request for a preliminary ruling made by the Administrative Court of Eripme. This judgment is not to be relied upon in any other context.

Applicable law

The questions referred to the Court for a preliminary ruling are based on the assumption that Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters ('the 2008 FD') applies. If that assumption is wrong, several of the questions would no longer need to be answered by the Court.

The Court will therefore first consider the applicable law.

Article 1(3), read together with Article 1(1) and (2) and recitals 2 to 6 in the preamble to the 2008 FD, provides that the decision applies to the processing (wholly or partly by automatic means or otherwise if part of a filing system or intended to form part of a filing system) of personal data in the framework of police and judicial cooperation in criminal matters. Recital 7 in the preamble to the 2008 FD emphasises that its scope '… is limited to the processing of personal data transmitted or made available between Member States'. Recital 9 also makes it clear that the 2008 FD does not apply '… to personal data which a Member State has obtained within the scope of [this FD] and which originated in that Member State'. Provided that a transmission between Member States has taken place, the 2008 FD does apply to the transfer of personal data to a third State, an international organisation, and possibly private parties subject to the conditions of the 2008 FD.

Some of the transferred data in the present case constitute personal data within the meaning of Article 2(a) of the 2008 FD and were obtained from another Member State. They were transferred from a Member State to a third country in the context of a criminal investigation in the third country regarding a sabotage threat. Therefore, the Court concludes that the 2008 FD applies to a transfer in circumstances such as those at issue in the present case.

That conclusion is not affected by the fact that a bilateral treaty regarding the exchange of data is also in place between the Member State transferring data and the third country receiving the data and that the data are said to have been exchanged on the basis of that treaty. The Court's conclusion is reinforced by the fact that the bilateral treaty in question provides a basis for exchange of data between both countries but does not contain guarantees regarding the retention and protection of that data, including as regards considerations of human rights and data protection by the third country.

It is true that the first paragraph of Article 26 of the 2008 FD states that that decision is 'without prejudice' to obligations and commitments under bilateral treaties between Member States and third countries existing when the 2008 FD was adopted. Whilst that provision applies here (the bilateral treaty at issue dates from 1980 and Eripme joined the EU in 1992), that does not mean that the bilateral treaty governs the transfer of the data at issue to the exclusion of the 2008 FD and possibly other parts of EU law.

Rather, the Court finds that the phrase 'without prejudice' in the first part of Article 26 means that the 2008 FD does not per se preclude Member States from transferring personal data on the basis of a bilateral treaty with a third country that provides for no guarantees governing the retention and protection of that data. However, any transfer of personal data pursuant to that treaty after the adoption of the 2008 FD must comply with the conditions set out therein. The Court does not accept that, in such circumstances, such a transfer is not subject to the relevant conditions under EU law.

It may indeed be right that Article 351 TFEU imposes an obligation on Eripme to remove any inconsistencies between the bilateral treaty and the Treaties, and Article 26 of the 2008 FD must of course be interpreted in the light of Article 351 TFEU. However, the Court does not consider it necessary to interpret Article 351 TFEU here. Any incompatibilities that may exist between the bilateral treaty and EU law, in particular primary law, cannot affect the conditions governing the transfer of the data at issue in the present case because the bilateral treaty does not contain any obligations as such in that regard.

It follows that the third question referred by the national court is hypothetical and does not need to be answered by the Court: where the 2008 FD applies, the Charter also applies.

Finally, as regards data transferred to a third state which were *not* obtained from another Member State, the Court finds that such data in principle fall outside the scope of

application of the 2008 FD. They nevertheless benefit from general protection under EU primary law, in particular Article 16(1) TFEU. In those circumstances, the Charter also applies subject to conditions as regards its territorial scope of application.

Moreover, in circumstances where data are transferred in a form that does not permit distinguishing between personal data falling within the scope of the 2008 FD and personal data falling outside, the provisions of EU law guaranteeing the higher level of protection must apply.

Against that background, the Court now turns to the first question.

Question 1

The question essentially asks whether a statement by a person that he or she has 'no belief in politics' constitutes data revealing a political opinion within the meaning of Article 6 of the 2008 FD.

Special categories of personal data are included within the wider concept of personal data within the meaning of Article 1(a) of the 2008 FD, the objective of which is to ensure a high level of protection of fundamental rights and freedoms of natural persons whilst guaranteeing a high level of public safety.

It is well established that the concept of personal data is broad. As Advocate General Sharpston wrote in her Opinion in *Y.S.* and *M. & S.*, the Court's case-law shows that it covers, at least, any facts regarding a person's private life and possibly, where relevant, his professional life. As the Court stated in *Schwarz*, the concept also covers data that contain unique information about individuals which allows those individuals to be identified with precision. In *Schwarz*, the Court was not defining personal data in an exhaustive manner so as to mean that *only* information through which a person can be identified is information 'relating to' an identified or identifiable person. The text of Article 2(a) makes it clear that personal data can cover information regarding a person *already identified*.

Whether or not the statement 'no belief in politics' expresses a political opinion, the Court finds that the statement was made in the exercise of freedom of expression as guaranteed by Article 11(1) of the Charter, which 'include[s] freedom to hold opinions'.

Article 6 of the 2008 FD does not define what constitutes a political opinion. The Court holds that the term should be given its ordinary meaning, namely that a political opinion is an expression of an individual's beliefs as regards matters falling within the political

sphere. The text of the 2008 FD makes no distinction based on the content of that belief or on whether it is expressed in positive or negative terms. This 'plain meaning interpretation' is supported by the context, object and purpose of the 2008 FD and in particular Article 6. The Court therefore concludes that the term 'political opinion' within the meaning of Article 6 of the 2008 FD must be interpreted as covering a statement such as that at issue.

The Court now turns to part b) of the first question referred by the national court.

That question consists of two further parts.

As regards the first part of question 1(b), the Court finds that the level of protection that applies to 'ordinary' personal data necessarily also applies to special categories of personal data. Indeed, the words 'strictly necessary' suggest a stricter standard of protection. When read within the context of Article 3 of the 2008 FD, the Court holds that the standard of strict necessity in Article 6 is higher (and hence more difficult to satisfy) than the generally applicable standard of proportionality. Any analysis of strict necessity should comprise at least the following steps: (i) examining the purpose (which should be both legitimate and specified) of collecting and then further processing the data; (ii) determining whether processing the data contributes to achieving the objective identified; (iii) weighing and balancing the different interests at stake in order to determine strict necessity; and (iv) examining whether less intrusive measures are available that would still achieve the objective pursued.

The Court does not consider that the set of legitimate purposes for which special categories of personal data can be processed is narrower than that justifying the processing of other types of personal data. However, it does find that the relation between the measure and objective pursued should be closer to the standard of 'indispensable to attaining the objective' than 'aimed at attaining the objective'. In this regard, the Court has taken note of the fact that, unlike Article 8 of Directive 95/46, Article 6 of the 2008 FD does not limit the objectives that may justify processing the special categories of personal data. However, reading the 2008 FD in the light of the Charter, the Court considers that the strict necessity standard under Article 6 of the 2008 FD cannot imply a lower level of protection than that guaranteed by the Charter.

The answer to the second part of question 1(b), regarding the so-called 'unfettered discretion' of the police authorities, does not depend specifically on Article 6 of the 2008 FD. Rather, Article 25 of the 2008 FD, especially when read within the broader context

of the new Articles 39 TEU and 16(2) TFEU, provides for independent monitoring and review by a supervisory authority. That obligation is separate from the requirement for judicial remedies in Article 20 of the 2008 FD. The Court interprets Article 25 of the 2008 FD to mean that EU law requires review by an authority independent from the entity processing (and possibly transferring) the personal data. The requirement of complete independence precludes the possibility of a single authority (as, here, the Eripmean Police Authority) functioning both as the processor and the supervisory authority within the meaning of the 2008 FD. Article 8(3) of the Charter, which provides that compliance with the rules on the protection of personal data in Article 8 'shall be subject to control by an independent authority', confirms that interpretation.

The Court now turns to the second question.

Question 2

In response to part a) of question 2, the Court holds that Article 13 of the 2008 FD precludes Member States from transferring personal data to third countries where the Member State from which that personal data was obtained has not consented to the transfer of those specific data to that specific third country. The reference in Article 13(1)(c) to 'transfer' must be understood as shorthand for 'the transfer that is the subject of that specific provision and for which consent must be given by the Member State from which the data was obtained'. That concept of *transfer* used in Article 13 of the 2008 FD is separate from that of *disclosure by transmission* in Article 2(a) of the 2008 FD. The Court interprets Article 13 to mean that the consent must be explicit in expressing agreement that the other Member State may transfer the data in question to a third state or international body.

Article 13(1)(c) must also be read within the context of recital 24 in the preamble to the 2008 FD. The first sentence of that recital confirms the requirement of consent in Article 13(1)(c). Although the second sentence leaves it to the Member States to determine 'the modalities of such consent', the recital goes on to give the example of 'general consent for categories of information or for specified third States'. The sentence thus confirms the Court's interpretation: irrespective of whether the consent is characterised by the Member State as 'general', it is in any event necessary to specify to which third States data can be transferred.

The fact that Article 11 of the 2008 FD authorises Member States to exchange personal data for purposes such as criminal investigations does not alter that conclusion. If that

provision were to be read as implying that any consent given automatically includes therefore mean consent for transferring data to a third state, that in effect would create an obligation for a Member State to specify when giving consent that it does *not* intend the personal data to be transferred to third countries. The Court finds no basis for reading such an obligation into Article 11 or any other provision of the 2008 FD.

As regards part b) of question 2, the Court holds that Article 13(1)(a) must be interpreted in the light of Article 13(1)(d) of the 2008 FD which refers to the 'adequate level of protection' for the 'intended data processing'. In so far as the intended processing is that of special categories of data within the meaning of Article 6 of the 2008 FD, the adequate level of protection to be verified prior to transferring data in accordance with Article 13(1), must be one that accords with 'strict necessity' for the data processing.

Thus, with respect to each transfer of personal data to a third state, the Member State transferring the data must request assurances from that state that an adequate level of protection will be given to the processing for the purposes of which the data are being transferred. Exceptions to that obligation are set out in Article 13(3). In particular, under (b), where safeguards in place in the third state are 'deemed adequate' by the transferring Member State in accordance with its national law, it will not necessarily need to obtain the relevant assurances for a specific transfer. However, the Court finds that Member States may not *deem* safeguards to be 'adequate' without examining whether the safeguards in place do in fact offer at least the level of protection that is to be guaranteed pursuant to the 2008 FD. Whilst the 2008 FD refers here to the national law of the Member State transferring the data, that national law must be interpreted in accordance with the 2008 FD and EU law more generally.

The facts set out by the national court do not indicate any basis for applying Article 13(2) of the 2008 FD (transfer without prior consent if such transfer is essential to prevent an immediate and serious threat to public security). The Court therefore considers it unnecessary to interpret that provision.

Question 3

In the light of the Court's initial remarks regarding the applicable law, the Court considers it unnecessary to answer the separate parts to question 3.

Question 4

In response to question 4, the Court holds that where a constitutional court, which is a court in accordance with the well-established criteria set out in *Dorsch Consult*, has jurisdiction to consider violations of fundamental rights under national constitutional law and where, in the exercise of that jurisdiction, EU law may be triggered and therefore national constitutional law guaranteeing fundamental rights may need to be interpreted in the light of the Charter, that court can request a preliminary ruling in accordance with Article 267 TFEU. Therefore, if such a national constitutional court would be assisted by a preliminary ruling from the Court, it should be able to make such a request.

Question 5

In response to part a) of question 5, the Court finds that the mere failure of a national court of last instance to request a preliminary ruling in accordance with Article 267 TFEU does not per se constitute a manifest breach of EU law. Nor does the failure to examine each and every element of the *CILFIT* test necessarily and automatically amount to a manifest breach of EU law. Rather, the national court of last instance must consider the substance of the dispute before it in order to determine whether there is an actual EU law point on substance. It must make an honest attempt to evaluate, according to the *CILFIT* criteria, whether the issue is acte claire (for example, by examining the various language versions as it is able to understand).

As regards part b) of question 5, the Court recalls that in *Brasserie du pêcheur* it referred to the three conditions set out in *Francovich*, in particular the second condition that the breach must be sufficiently serious, in order to introduce the idea that the decisive test as regards the second condition is whether the Member State 'manifestly and gravely disregarded' the limits on its discretion. The Court then gave guidance to the national court on what it might need to take into consideration in this regard. In *Köbler*, the Court considered State liability resulting from a decision of a national court of last instance which breached EU law. There, the Court held that such liability can be incurred only in the exceptional case where that court manifestly infringed the applicable law and treated a 'manifest' breach as 'sufficiently serious' within the meaning of *Brasserie du pêcheur*. The Court therefore now confirms that a 'manifest breach' equates to a 'sufficiently serious breach'.

Finally, in response to part c) of question 5, the Court recalls that it is not its function, in the context of a preliminary ruling, to decide whether Eripme is or is not liable in damages on either of the grounds identified in the question referred. That is for the

national court to decide. The national court should do so in accordance with the criteria set out in *Brasserie du pêcheur*. Those criteria apply to a grave and manifest breach of the 2008 FD as they do to any other grave and manifest breach of EU law.

***

The Court wishes to express its thanks to Judge Isabelle Van Damme for her invaluable help in preparing the judgment of the Court.

***

The winners of the moot are: Ljubljana.