8 SIS Compliance with Article 8 ECHR and Data Protection Principles

8.1 Introduction

This chapter is devoted to the evaluation of the SIS compliance with Article 8 ECHR and data protection principles. The human rights evaluation criteria analysed in Chapter 4 and the data protection transparency and proportionality model developed in Chapter 6 are used as evaluation tools. The discussion in this chapter is not based on the factual situation, but on the formal situation. It is a discussion on the obligations and rights. The conclusions arrived at may not necessarily be the same conclusions that the ECtHR may make. The conclusions reached are based on the writer’s interpretation of the obligations and rights in the Convention. The lack of Schengen case law at the ECHR level makes it difficult to say what the law is. The developments at the national level, however, seem to agree with what the writer thinks the law should be (see 8.2.5 below).

8.2 SIS and Article 8 ECHR

8.2.1 The Principle under Examination

The four criteria that are used as evaluation criteria of Article 8 ECHR are:
- Interference under Article 8 (1),
- In accordance with the law,
- Legitimate aims, and
- Necessary in a democratic society.

8.2.2 Interference under Article 8 (1)

According to the Klass and Others case, the very existence of a measure amounts to interference with respect for private life under Article 8 (1). The measure does not have to be applied for interference to be inferred. This has been confirmed in subsequent cases of Amann v. Switzerland, Kopp v. Switzerland and Rotaru v. Romania. Similarly, the existence of the SIS would amount to interference with respect for private life under Article 8 (1). The very establishment of the SIS is in itself interference with respect for private
life. This is true also for other systems such as Europol, Eurodac, Interpol, Customs Information System and Visa Information System discussed in the next chapter.

Systematic registration of personal information also amounts to interference with the respect for private life. In addition, the information need not be used (Amann v. Switzerland, Kopp v. Switzerland and Rotaru v. Romania). The Schengen Convention allows systematic registration of personal data under Article 94 (1). The registration would amount to interference under Article 8 (1) even if the information was not put to use. The information recorded in the SIS, however, is systematically used for purposes of crime and border control. The storage of personal information also amounts to interference as the Court ruled in the cases of Leander v. Sweden and Amann v. Switzerland. Again here the information need not be used, the act of storage in itself amounts to interference for the purposes of Article 8 (1). Even where the information is used for the purpose intended or the purpose for which it was collected, it could also amount to interference (Rotaru v. Romania). For example, in SIS, the information is recorded for purpose of identification. Even where the information is used for this purpose it could still amount to interference with the respect for private life.

The human rights law under Article 8 (1) also places importance on individual access to registered information. Where access to information is denied, the Court has found this to amount to interference (Leander v. Sweden, McMichael v. United Kingdom, Gaskin v. United Kingdom and M.G. v. United Kingdom). In the last two cases, the Court applied the doctrine of State's positive obligation to find interference where access was denied. Although the right of access is recognised and provided for in the Schengen Convention, it has many obstacles which make it difficult to exercise and as such one may not necessarily get access to the information.1 Where the exercise of a right is difficult, it cannot be said that a person has a right. Similarly, the disclosure of information can amount to interference with private life under Article 8 (1) (M. S. v. Sweden, Leander v. Sweden, Z v. Finland and Peck v. United Kingdom). The Schengen Convention allows disclosure of information to persons who need the information so as to perform their legal duties. While such disclosure or access to information is in accordance with personal data protection laws, under human rights law, the disclosure, even where allowed, can amount to interference with the respect for private life.

Lack of deletion of information procedure amounts to interference with the respect of private life (Amann v. Switzerland and Rotaru v. Romania). The Schengen Convention stipulates deletion procedure and as such interference is difficult to construe purely by the lack of deletion procedures. If, however, the procedures are not followed, it would be possible to infer interference. The JSA had reported that Member States were, after deletion of the information in the SIS, retaining the same information in the SIRENE system. Such practice would amount to interference because there are no clear deletion procedures under the SIRENE system. The information could be retained in the SIRENE for an indefinite duration.

It may be difficult for the SIS to comply with non-interference criterion unless the system does not exist. Most critics of the SIS have argued that the system should not have been brought into existence as its existence is a threat to privacy. The reality is that

1 See 8.3.2.2.