

Franziska Boehm

Information Sharing and Data Protection in the Area of Freedom, Security and Justice

Towards Harmonised Data Protection
Principles for Information Exchange
at EU-level

Franziska Boehm

Information Sharing and Data Protection in the Area of Freedom, Security and Justice

Towards Harmonised Data Protection
Principles for Information Exchange
at EU-level



Dr. Franziska Boehm
University of Luxembourg
Interdisciplinary Centre for Security, Reliability and Trust (SnT)
6, rue Richard Coudenhove Kalergi
1359 Luxembourg
Luxembourg
franziskaboehm1@aol.de
or franziska.boehm@uni.lu



Fonds National de la
Recherche Luxembourg

Printed with the support of the FNR Luxembourg

ISBN 978-3-642-22391-4 e-ISBN 978-3-642-22392-1
DOI 10.1007/978-3-642-22392-1
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011941399

© Springer-Verlag Berlin Heidelberg 2012

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilm or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Information Sharing and Data Protection in the Area of Freedom, Security and Justice

Acknowledgements

This thesis is the result of my work as a research assistant from 2007 to 2011 under the guidance of Professor Herwig Hofmann at the University of Luxembourg. It was defended in April 2011.

First and foremost, I wish to express my gratitude to my supervisor, Professor Herwig Hofmann. His support and guidance during the years of my research have made it possible for me to write and finish this thesis. My profound thanks go to him for his confidence in my work. It was also an extraordinary privilege to have been guided by Professor Spiros Simitis who not only took part in my jury, but who was always available for discussions over the last few years when I needed his advice. He and his publications have been a constant inspiration and an important guide during the research. I would like to express my deepest appreciation and I profoundly thank him for his encouragement and his indispensable advice. I would also like to thank Mark Cole, Associate Professor at the University of Luxembourg, for his invaluable comments and his continual academic support over the last years. He always had the time to discuss and was open to my ideas. The thesis would look far less complete without his contributions.

The idea for the research dates back to my years at the University of Gießen where I wrote my master thesis on a data protection related topic under the supervision of Professor Thilo Marauhn, who continuously supported my scientific interest and whom I thank for his support also in the framework of my thesis. Hielke Hijmans from the European Data Protection Supervisor and Professor Stefan Braum, at the University of Luxembourg, took part in my Jury and gave tips and advice along the way. I am likewise indebted to Garth Hall and Lawrence Siry who improved the legibility of the manuscript. Their annotations have been always very helpful.

Very warm thanks go to my colleagues at the University of Luxembourg. I have made good friends in this faculty and I am deeply grateful for the moments I have shared with you, be it for a chat or a scientific discussion. It is difficult to mention names, some are Dr. Florence Giorgi, Sandra Schmitz, Lawrence Siry, Miroslava Borissova, Jenny Metzdorf, Dr. Roger Tafoti, Mariana Ignatescu and Dr. Isabelle

Rueda but there are many more, and I would like to thank all of them for their help, time and encouragement, especially during the final stage of the PhD. Of course, friends from outside the University, especially from Berlin and Gießen deserve a special mention as well. Without their moral, emotional and social support, this thesis would never have been written. Ida Danke, Julia Horländer, Johanna Schmidt, Maïke Gappa, Christin Noak, Lars Hoffmann, and Ole Westphal are only a few Berlin friends of so many others. Thorsten Dreimann, Markus Berliner, Ines Heylmann, Dr. Kai Purnhagen and Til Kappen as well as Julia Heieis, Andrea Kristekova, Jan Lizak, Jörg Piper, Anja Pavlenko, Martin Faix and Sonia Kienitz, all of whom I met in Gießen, supported me in every imaginable way. I also would like to thank my family, especially my parents, Evelyne and Clemens, and my sisters, Annina and Nina, for their constant and unconditional support. I owe all of you more than just the mentioning in the thesis.

Most of all, I am particularly thankful to Dr. Tobias Lochen, who stood always by me through the last years and was there when I needed his support. He spent so many hours reading the manuscript and encouraging me in difficult moments. I am more than grateful for his companionship and his belief in me.

Finally, without the indestructible belief in my abilities shown to me by my dear grandparents, Gertrud and Georg Libor, I would have never had the strength to start (and to finish) the PhD project. Their constant support and encouragement has led me to this result. This book is therefore dedicated to them.

Luxembourg

Franziska Boehm

Abbreviations

AFIS	Anti-fraud information system (in context of OLAF)
AFIS	Automated fingerprint information system (in context of Eurodac)
AG	Advocate general
AZR	Ausländerzentralregister
CCTV	Closed-circuit television
CEPOL	European police college
CIS	Customs information system
CMS	Case management system
C-SIS	Central EU section of the Schengen information system
C-VIS	Central EU section of the visa information system
Doc	Document
DPA	Data protection authority
DPO	Data protection officer
EC Treaty	Treaty establishing the European community
ECHR	European convention of human rights
ECRIS	European criminal records information system
ECtHR	European court of human rights
EDPS	European data protection supervisor
EEAS	European external action service
e.g.	<i>exempli gratia</i> (for example)
EIS	Europol information system
EJN	European judicial network
EMCDDA	European monitoring centre for drugs and drugs addiction
et seq.	<i>et sequens</i> (and the following)
EU	European Union
Eurodac	European dactyloscopy
Eurojust	European Union's judicial cooperation unit
Europol	European police office
FBI	Federal Bureau of Investigation

FDPJ	Framework decision on the protection of personal data in police and judicial cooperation in criminal Matters
FIDE	Fichier d'Identification des Dossiers d'Enquête Douanière (Customs File Identification Database)
FRG	Federal Republic of Germany
FYROM	Former Yugoslav Republic of Macedonia
G-10 Act	German Act to monitor mail and telephone communication (Gesetz zu Artikel 10 des Grundgesetzes vom 13. August 1968, BGBl. I p. 949)
GDR	German Democratic Republic
i.e.	<i>id est</i> (that is)
Info-ex	(Former) Information exchange system at Europol
Interpol	International criminal police organisation
IT	Information technology
JIT	Joint investigations team
JSA	Joint supervisory authority (SIS, CIS)
JSB	Joint supervisory body (Europol)
MRS	Mail registration system of OLAF
N-SIS	National section of the Schengen information system
N-VIS	National section of the visa information system
OECD	Organisation for economic cooperation and development
OJ	Official journal of the European Union
OLAF	European Anti-Fraud Office, Office européen de lutte Antifraude
p.; pp.	Page, pages
Para	Paragraph
PNR	Passenger name record
RABITs	Rapid border interventions teams (of Frontex)
SIENA	Secure information exchange network
SIRENE	Supplementary information request at the national entry (additional data exchange possbilitiy in the framework of the SIS)
SIS II	Second generation of the Schengen information system
SIS	Schengen information system
SITCen	Joint situation centre
SSMA	Special surveillance means act
TEU	Treaty on European Union
TFEU	Treaty on the functioning of the European Union
UK	United Kingdom
UNDOC	United Nations Office on drugs and crime
US	United States
v.	Versus
VAT	Value added tax
VIS	Visa information system
Vol.	Volume

Contents

Introduction	1
I. Brief Background on Data Protection in EU Law	3
II. What is the Area of Freedom, Security and Justice?	6
III. Research Topic: Information Sharing in the AFSJ and Data Protection Rights	8
IV. Terminology	12
V. Limitations of the Research	15
VI. Sources	16
VII. Outline of the Research	16
A Data Protection Standard in the AFSJ	19
I. Brief Historical Review and Reasons for Data Protection	19
II. Council of Europe: Art. 8 ECHR, Convention No. 108 and Recommendation R (87) 15	22
1. Data Protection Guarantees of Article 8 ECHR	25
2. Data Protection Elements and Restrictions with Regard to Articles 5, 6, 10 and 13 ECHR	84
3. Convention No. 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data	92
4. Recommendation No. R (87) 15 Regulating the Use of Personal Data in the Police Sector	96
5. Conclusion: Towards Basic ECHR Principles for Security-Related Data Processing	103
III. European Union Standards	106
1. Main Data Protection Instruments in the AFSJ and Their Scope	107
2. EU Data Protection Principles in the AFSJ	127
3. Conclusion: Data Protection Rules in the AFSJ are Still a Patchwork	171

B AFSJ Actors in the Light of the European Data

Protection Standard	175
I Brief Background Information	176
II European Agencies and OLAF	177
1. Europol	177
2. Eurojust	214
3. OLAF	226
4. Frontex	246
5. Joint Situation Centre of the Council	253
6. European Judicial Network	254
7. Conclusion: Fragmented Data Protection Framework Versus Increasing Powers of the AFSJ Agencies and OLAF	256
III Data Processing in European Information Exchange Systems	259
1. The Schengen Information System	260
2. The Visa Information System	280
3. The Customs Information System	292
4. Eurodac	304
5. Proposal for an Agency Managing Large IT Systems (SIS II, VIS and Eurodac) from a Data Protection Point of View	314
6. Conclusion: Stagnating Data Protection Framework in Contrast to Increasing Functionalities of the EU Information Systems	318

C Cooperation and Data Exchange of the AFSJ Actors and Their Compliance with the European Data

Protection Standard	321
I Inter-Agency Data Exchange and OLAF	322
1. Europol-Eurojust	322
2. Europol-OLAF	330
3. Europol-Frontex	333
4. Eurojust-OLAF	338
5. Eurojust-Frontex	342
6. Conclusion: Unsatisfactory Data Protection Framework in AFSJ Inter-Agency Information-Sharing	342
II Data Exchange Between AFSJ Agencies and Europe's Information Systems: SIS, CIS, VIS and Eurodac	344
1. Europol-SIS II Access	344
2. Europol-VIS Access	348
3. Europol-CIS Access	357
4. Europol-Eurodac Access	360
5. Eurojust-SIS II Access	366

6. Eurojust-CIS Access	368
7. Conclusion: Unbalanced Interests – Law Enforcement Access and Respect of Data Protection Principles	368
D Perspectives and Suggestions for Improvement	371
I. Key Findings	372
II. Lawfulness of the Expanding AFSJ Functionalities	379
III. Limits of Preemptive Storing and Law Enforcement Access to Databases of a Non Law Enforcement Nature	381
1. Pre-Emptive Storing in View of the Case-Law	382
2. No Coherent Solution by the European Court of Justice for Law Enforcement Access	389
IV. Reforming the Supervisory Structure and Creating a General Notification Duty	393
1. The Need for a Central Supervisory Authority	394
2. Upgrading the Rights of the Supervisory Body to Guarantee Effective Protection	396
3. Towards a General Notification Duty	398
V. Aligning the Data Processing Framework in the AFSJ: Improvement Suggestions	398
1. Procedural Requirements and Legal Basis	400
2. Catalogue of Stored Data	400
3. Avoiding Unclear Terms and Harmonising Key Terms	401
4. Framing the Access Conditions	401
5. Improving the Protection of Victims, Witnesses and Persons Whose Data are Pre-Emptively Entered in Security Related Databases	402
6. Individual Rights	404
7. Notification	405
8. Control of Data Recording and Binding Security Rules	406
9. Improving the Protection and the Transparency of Information Originating from Private Parties or Third States	407
10. Common Rules on the Relations to Third Parties	407
11. Managing the Time-Limits	408
12. Dual Control: Introducing an Internal DPO	409
13. Improving the Decision Making and Introducing Sunset and Review Provisions	409
VI. Towards Harmonised Data Protection Principles for Intra-AFSJ Information Exchange	410
1. Restricting the Purpose of Transfer	411
2. Defining Unclear Legal Terms	411
3. Designating the Accessing Actors and Authorities	413
4. Harmonising the Access Procedure	413

5. Coordinating the Access Conditions	414
6. Data Protection and Data Security Rules	415
7. Follow-Up of the Transferred Data	416
8. Cooperation Between Data Protection Authorities	418
9. Penalties in Case of Misuse	418
10. Access Right, Correction, Deletion and Notification	418
11. Keeping of Records	420
12. Implementing Effective Monitoring and Evaluation	420
13. Specific Rules Concerning Europol and Eurojust and JIT Cooperation	421
VII. The Important Impact of the Lisbon Treaty	422
Concluding Remarks	424
Documents	429
I. Conventions, Treaties, Acts and Related Documents	429
II. Council of Europe	430
III. EU Related Documents	431
Table of Cases	449
I. ECtHR Cases and Decisions of the Commission of the Council of Europe	449
II. EU Cases	453
Bibliography	457

Introduction

Information exchange in the European Union (EU) constitutes an essential part of the different policies of the EU. In many policy fields, information sharing is crucial for decision making and does not necessarily include the exchange of personal information.¹ However, in certain fields, information exchange contains personal data and therefore affects the rights of individuals. In areas related to law enforcement and judicial cooperation, such as the Area of Freedom, Security and Justice (AFSJ), horizontal information sharing, including the exchange of personal data, has become an essential tool in the internal security policy of the EU. The process of European integration and communitarisation has considerably supported the establishment of Union bodies, agencies and information systems in this area.² Traditional national law enforcement and judicial structures are complemented by horizontal EU arrangements increasingly governed by a network type of governance.³ Personal data are therefore not only exchanged between Member States and with third states, but also between EU bodies. Analysing the information exchange taking place at EU level between the relevant EU actors is therefore a challenging task.

Post 9/11 policy concepts, such as the Hague programme and the Stockholm programme promote an enhanced cooperation and coordination of law enforcement agencies and other agencies within the AFSJ.⁴ Under their influence, formerly not related policy areas, such as the prevention of crime and immigration, are linked

¹ Compare Hofmann et al. (2011). Chap. 12, pp. 411–490.

² Mitsilegas (2009), p. 161.

³ Den Boer et al. (2008).

⁴ On this subject: The Hague Programme: strengthening freedom, security and justice in the European Union, Council doc. 16054/04 of 13 December 2004, point 2.5, p. 25, in the following: The Hague Programme, Council doc. 16054/04 of 13 December 2004; The Stockholm Programme – An open and secure Europe serving and protection the citizen, Council doc. 17024/09 of 2 December 2009, adopted by the Council on 10/11 December 2009, point 4.1, pp. 35/36, in the following: The Stockholm Programme, Council doc. 17024/09 of 2 December 2009.

and lead to an intensive cooperation between AFSJ actors of a completely different legal nature, vested with different powers.⁵ In absence of a unified approach to data protection in judicial and criminal matters⁶ and without being limited by the former pillar constraints, legally and structurally different bodies, equipped with different tasks, exchange and transfer personal data within and outside the EU. The result is that data collected for one specific purpose may be transferred and used for other purposes completely unrelated to the original collection. This ever increasing cooperation at multiple levels touches upon different data protection regimes. While information and personal data exchange has been identified as a priority in this field, data protection guarantees risk to be undermined by this practice.⁷ The central question of this research is therefore “Does the EU internal data exchange comply with its own data protection standards?”.

This research examines the inter-agency cooperation between AFSJ actors such as Europol, Eurojust or Frontex as well as the Commission’s anti-fraud unit, OLAF, which led to the conclusion of agreements providing for mutual information exchange in recent years.⁸ In addition, the access of law enforcement and judicial agencies to data stored in the European information systems, such as the Customs- (CIS), the Schengen- (SIS) or the Visa Information System (VIS) and Eurodac occupies an increasingly important place in the AFSJ. It is therefore analysed in detail.

When considering the increasing cooperation between the mentioned AFSJ actors, tensions between the rights of individuals and security interests⁹ are bound to occur. The current development in the AFSJ calls for maximum cooperation in terms of data exchange between the actors involved, the rules regulating such exchanges however vary to a great extent and are far from being harmonised. Questions relating to the coherence and the respect of data protection rules within this cooperation network of the AFSJ actors seem to be pushed into the background. This unbalanced situation can have a profound impact on the rights of individuals.

⁵ Mitsilegas (2009), p. 223.

⁶ Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ 2008, L-350/60, in the following: FDPJ, OJ 2008, L-350/60, represents a first step towards a comprehensive framework in this area; the FDPJ is however very restricted in scope as it is for instance not applicable to the data processing of most of the AFSJ law enforcement agencies, such as Europol and Eurojust, as well as at other AFSJ exchange systems, i.e. the SIS or the CIS; moreover, excluded from the scope is also the internal processing of the Member States in police and criminal matters; the scope and the guarantees of the FDPJ are illustrated in more detail in Chaps. A III 1 c and A III 2.

⁷ To the general necessity to establish an effective data protection framework with regard to former third pillar bodies, see Paeffgen (2006), pp. 63–86, in particular pp. 77–79.

⁸ Compare note from the General Secretariat to the Standing Committee on operational cooperation on internal security (COSI), final report on the cooperation between JHA agencies, Council doc. 8387/10 of 9 April 2010.

⁹ For the understanding and the importance of the term “security” in the EU, see Kotzur (2009); Möstl (2009); Grabenwarter (2009b).

It is worth pointing out that, even though the context in which information is used is changing rapidly, no evaluation or overview of the existing data collection, processing and data-sharing systems, including a thorough assessment of their effectiveness, their possible overlapping effects, proportionality and their respect of data protection rights have thus far been carried out.¹⁰

In the light of these considerations, the data protection rights of the individuals concerned by the increasing AFSJ cooperation play a decisive role. The establishment of a strategic approach for the exchange of information in the AFSJ is urgently needed to balance the rights of individuals against the multiple and still increasing possibilities that personal data will be exchanged by and between AFSJ actors.¹¹ Therefore, analysing the different data protection regimes and the existing arrangements providing for personal data exchange in the AFSJ is an essential in order to detect possible shortcomings in this complex cooperation structure.

I. Brief Background on Data Protection in EU Law

Data protection in EU law constitutes a relatively new individual right encompassed in Article 8 Charter of Fundamental Rights as well as in Article 16 TFEU. It protects against the potential misuse of information by governmental and non-governmental actors.¹² The basic concepts of data protection are included in Article 8 Charter of Fundamental Rights stipulating that:

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

Article 8 (2) Charter of Fundamental Rights includes basic quality standards and individual rights which have to be respected when processing personal data. In addition to the prohibition of data processing for unspecific and undefined purposes, the fairness of the processing and the access to and the rectification of personal data are crucial elements in data protection law. Independent supervision is a further

¹⁰ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Delivering and area of freedom, security and justice for European's citizens – Action Plan implementing the Stockholm Programme, COM(2010) 171 final, in particular p. 6.

¹¹ Ibid.

¹² On the general risks of data processing in databases see Simitis (2006), p. 65, para 10.

important element to make data processing legitimate. These rather broad principles need to be specified in the different contexts of processing.

The current understanding of data protection as a fundamental right under Article 8 Charter of Fundamental Rights is intrinsically linked to the right to private life included in Article 8 European Convention of Human Rights (ECHR).¹³ While private life is a broad term which embraces issues concerning the protection of an individual's personal space which go far beyond data protection¹⁴ such as the right to be let alone¹⁵ or the right to develop personal relationships with each other,¹⁶ the protection of personal data is one important aspect of the right to private life.¹⁷ This historical background is the reason why, prior to the adoption of EU data protection instruments, such as the Data Protection Directive 95/46,¹⁸ Article 16 TFEU and Article 8 Charter of Fundamental Rights, public international law instruments of the Council of Europe played the central role in interpreting data protection principles in the EU context. The first instruments specifying the right to data protection at European level were therefore not EU instruments, but instruments of the OECD and the Council of Europe.

The economic orientated OECD Guidelines of 1980 governing the protection of privacy and trans-border flows of personal data (OECD Guidelines)¹⁹ and the Convention of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention No. 108) were the first

¹³ Both concepts (data protection and private life) are twins but not identical; compare Siemen (2006); De Hert and Schreuders (2001), p. 42; for the coherency between ECHR and Charter of Fundamental Rights see Schneiders (2010), pp. 145–245; Steiner et al. (2006), pp. 115–144.

¹⁴ Kuner (2009), pp. 307–317, in particular p. 309.

¹⁵ The first description of the right to privacy was made by Warren and Brandeis in their famous article in the Harvard Law Review in 1890. They described the right as “the right to be let alone”, see Warren and Brandeis (1890).

¹⁶ Compare ECtHR case law: *Niemietz v. Germany*, Application no. 13710/88, of 16 September 1992, para 29.

¹⁷ Compare ECtHR case law: *Z. v Finland*, Application no. 22009/93, judgment of 25 February 1997, para 95; *Peck v. United Kingdom*, Application no. 44647/98, judgment of 28 January 2003, para 78; *L.L. v France*, Application no. 7508/02, judgment of 10 October 2006, para 43; *Biriuk v Lithuania*, Application no. 23373/03, judgment of 25 November 2008, para 39; *I v Finland*, Application no. 20511/03, judgment of 17 July 2008, para 38; *S. and Marper v the United Kingdom*, Application nos. 30562/04 and 30566/04, judgment of 4 December 2008, para 103; *C.C. v. Spain*, Application no. 1425/06, judgment of 6 October 2009, para 31; see also: Breitenmoser (1986), p. 245; (Kugelman 2003) pp. 16–25; Meyer-Ladewig (2006), Article 8, para 11; Moreham (2008).

¹⁸ Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of the individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995, L-281/31, in the following: Directive 95/46 OJ 1995, L-281/31.

¹⁹ OECD Recommendation concerning Guidelines governing the protection of privacy and trans-border flows of personal data of 23 September 1980.

international instruments which included data protection rules in Europe.²⁰ In addition to these first instruments, the interpretation of Article 8 ECHR by the European Court of Human Rights (ECtHR) contributed to the specification of basic data protection principles inherent to the right to private life. The relevant case law of the ECtHR is further detailed in Chap. A.

Due to the former pillar structure, different rules exist in EU law for the protection of personal data. Prior to the adoption of the Lisbon Treaty,²¹ Directive 95/46, Regulation 45/2001²² and Article 286 EC Treaty²³ (now Article 16 TFEU) guaranteed data protection rules in former first pillar matters.²⁴ Excluded from the scope of these instruments was data processing in former second and third pillar matters.²⁵ Data processing in these areas was for a long time exclusively governed by the aforementioned public international law instruments of the Council of Europe.²⁶ In November 2008, the Data Protection Framework Decision 2008/977/JHA on personal data processed for police and judicial cooperation in criminal matters (FDPJ) was finally adopted with the intention of covering data processing in (former) third pillar matters.²⁷ Its scope is however, very restricted and does not cover data processing of Europol and Eurojust,²⁸ nor of the data exchange systems,

²⁰ Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1981, CETS No. 108. In the following: Convention No. 108.

²¹ To the general changes in the different policy areas through the Lisbon Treaty, see Fastenrath and Nowak (2009).

²² European Parliament and Council Regulation (EC) 45/2001 of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ 2001, L-8/1 (referred to as Regulation 45/2001, OJ 2001, L-8/1 in the following).

²³ Brief comments on the scope and the content of Article 286 EC Treaty can be found in Callies and Ruffert (2007), pp. 2332–2334; Léger (2000), pp. 1849–1851; Lenz and Borchardt (2006), pp. 2495–2504.

²⁴ For more details see Chap. A III 1.

²⁵ Article 3 (2) Directive 95/46, OJ 1995, L-281/31 and Chap. A III 1.

²⁶ Convention No. 108, the ECHR standard and in addition Recommendation R (87) 15 of the committee of ministers to member states regulating the use of personal data in the police sector, adopted on 17 September 1987; The importance of the ECHR for the protection of fundamental rights in Europe is underlined by Breitenmoser et al. (2006), pp. 1–385; for a general overview of the Council of Europe see Wittinger (2005).

²⁷ Council 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, OJ 2008, L-350/60 (in the following referred to as FDPJ, OJ 2008, L-350/60), equivalent to Directive 95/46, the processing refers to automatic and non-automatic processing of personal data, Article 2 (a) FDPJ.

²⁸ Europol considers in recital (12) of Council Decision of 6 April 2009 establishing the European Police Office, OJ 2009, L-121/37: “A Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters will be applicable to the transfer of personal data by Member States to Europol. The relevant set of data-protection provisions in this Decision will not be affected by that Framework Decision and this Decision should contain specific provisions on the protection of personal data regulating these