

**DATA PROTECTION IN  
EU AND US  
CRIMINAL COOPERATION**

**A Substantive Law Approach to the EU Internal and Transatlantic Cooperation  
in Criminal Matters between Judicial and Law Enforcement Authorities**

**Els De Busser**



**Maklu**

Antwerpen | Apeldoorn | Portland

# Contents

Preface .....	5
Contents .....	7
Alphabetical list of abbreviations and instruments indicated by abridged titles .....	17
General introduction .....	21
A. Background and basic concepts .....	21
1. Privacy and data protection.....	21
2. In criminal matters.....	23
3. International exchange of personal data in criminal matters.....	24
4. Transatlantic relations.....	26
B. Research questions .....	28
C. Relevance .....	29
D. Objective and structure .....	31
1. Threefold structure.....	31
a. First stage: the EU and its data protection standards.....	31
b. Second stage: the EU and its compliance with its data protection standards in the relations between member states and with third states..	33
c. Third stage: the EU and its compliance with its data protection standards in its relations with the US.....	33
2. Limitations.....	34
E. Methodology and sources.....	35
1. Substantive scope.....	35
2. Geographical scope.....	36
3. Historical scope .....	37
Chapter I. EU data protection standards .....	39
A. Personal data in the EU.....	40
1. European definition of personal data .....	40
a. Sources of the definition .....	40
b. EU post factum concept of personal data.....	43
1. Any information.....	44
2. Relating to.....	44
3. An identified or identifiable natural person .....	45
2. Right to a private life in the EU .....	47
a. Merger of the privacy-aspect and the gathering of information .....	47
b. Development of the right to a private life .....	48
1. The right to a private life and the right to data protection.....	48
2. Defining both rights .....	50
c. Lawful derogations to the right to a private life .....	52
1. Legality .....	53
2. Legitimate aim .....	55
3. Necessity and balance of interests .....	56
a. The protection of national security.....	57
b. The protection of health and morals.....	60

4. Sufficiently independent supervision.....	61
3. Personal data protection.....	62
a. Council of Europe data quality standards.....	63
1. Quality standards for personal data.....	64
a. Accurate personal data.....	64
b. Adequate, relevant and proportionate personal data.....	65
2. Quality standards for the processing of personal data.....	66
a. Fair and lawful obtaining and processing of personal data.....	66
b. Purpose limitation and compatibility.....	66
c. Retention of personal data.....	69
3. Lawful derogations from data quality standards.....	70
a. Legality.....	70
b. Necessity.....	70
c. Precise and foreseeable.....	71
d. Proportionate.....	71
b. First pillar data protection by the EC Directive.....	72
1. Background.....	72
2. In the course of an activity.....	74
3. Final purpose.....	76
4. Public security, defence, State security and activities of the State in areas of criminal law.....	77
c. First pillar data protection by subsequent directives.....	77
1. Personal data and electronic communications.....	77
2. Processing and transferring of personal data by the Community institutions and bodies.....	78
d. Data retention directive: first or third pillar?.....	79
4. Conclusion.....	83
B. Personal data in criminal matters in the EU.....	84
1. Council of Europe data protection in criminal proceedings.....	84
a. Scope: defining criminal proceedings.....	84
b. Data quality standards in criminal proceedings.....	85
1. Protection offered by article 6 ECHR.....	86
a. Adversarial element in article 6.....	86
b. Article 6 and the gathering of personal data.....	87
c. Article 6 and the gathering of personal data proactively.....	88
2. Protection offered by article 8 ECHR.....	89
3. Relation between article 6 and article 8 ECHR.....	92
a. Decisive influence of the evidence.....	93
b. Nature of the violation of article 8.....	93
c. Right to challenge the evidence.....	93
c. Fair trial regardless of privacy violation.....	94
2. National implementation of the EC Directive in criminal proceedings..	95
3. Framework Decision on Data Protection in Criminal Matters.....	96
a. In line with the Data Protection Convention.....	97
b. Effect on other data protection provisions.....	98
c. Scope.....	98
1. General.....	98
2. Prevention, detection, investigation, prosecution and execution..	100
3. Transmitted or made available.....	100

d. Quality standards for personal data.....	102
e. Quality standards for the processing of personal data.....	103
1. Purpose limitation.....	103
2. Data retention.....	105
f. Supervisory authority.....	106
4. Conclusion.....	107
C. Trans-border flows of personal data from the EU.....	110
1. Data protection in trans-border flows from the EU: adequacy requirement.....	110
a. The Data Protection Convention and its Additional Protocol.....	111
b. EC first pillar instruments.....	113
1. Regulating the trans-border flow of data.....	113
2. Safe Harbour compromise.....	114
3. Adequacy requirement.....	116
2. Data protection in trans-border flows from the EU in criminal matters.....	117
a. Functional criterion.....	117
b. Consent.....	118
c. Adequacy requirement.....	119
d. Effects of the Framework Decision on Data Protection in Criminal Matters.....	121
3. Conclusion.....	122
D. Conclusion: and the rules are ... there are different rules.....	123
 Chapter II. Instruments in cooperation in criminal matters in the EU.....	 127
A. Applicable instruments between the EU member states.....	128
1. Quality control in line with the Council of Europe principles.....	128
a. Data Protection Convention.....	128
b. Recommendation R(87)15.....	129
c. Quality standards of personal data and of the processing of personal data.....	130
2. Quality of personal data.....	131
a. Accuracy of personal data.....	131
1. Degree of accuracy and reliability.....	131
2. Blocking instead of deleting.....	134
b. Judicial cooperation.....	136
1. Mutual assistance in criminal matters.....	136
2. Prüm instruments.....	137
3. Eurojust.....	137
a. Eurojust Decision.....	138
b. Rules of procedure on the processing of personal data.....	139
c. Law enforcement cooperation.....	141
1. In line with the Data Protection Convention and Recommendation R(87)15.....	141
2. Europol.....	142
a. Europol Convention.....	143
b. Changes in the data protection framework by the Europol Decision.....	143

3. Schengen law enforcement cooperation.....	144
3. Quality of the processing of personal data.....	145
a. Judicial cooperation .....	145
1. Purpose limitation .....	145
a. Strict purpose limitation .....	145
i. Eurojust’s own data protection rules.....	145
ii. Criminal records instruments.....	146
b. Widening purposes towards purpose deviation.....	148
i. EU mutual assistance in criminal matters.....	148
ii. Framework Decision on Data Protection in Criminal Matters .....	152
iii. Transfer to private parties.....	153
iv. The Schengen Information System and its inconsistencies .	155
v. Judicial authorities’ cooperation with OLAF.....	158
vi. Eurojust’s cooperation with OLAF.....	159
2. Data retention.....	160
a. Data retention directive .....	161
i. Legal bases.....	161
ii. The essential objective of the data retention directive .....	163
iii. Data retention for as long as necessary.....	165
b. Framework Decision on Data Protection in Criminal Matters..	166
c. Prüm Convention .....	167
d. Data storage by Eurojust.....	168
b. Law enforcement cooperation.....	169
1. Purpose limitation .....	169
a. For police use only unless consent.....	169
b. For other purposes with consent .....	170
i. Prüm Convention and its integration in the EU .....	170
ii. Framework decision on simplifying the exchange of information and intelligence .....	173
iii. Europol Information System.....	173
iv. Customs Information System (CIS).....	174
v. Other law enforcement cooperation initiatives .....	174
c. SIS and law enforcement authorities.....	174
d. Interoperability and availability .....	175
e. Second generation SIS (SIS II) .....	177
f. Visa Information System (VIS).....	179
g. Eurodac .....	180
2. Data retention.....	181
4. Supervision .....	182
5. Effects of the Framework Decision on Data Protection in Criminal Matters .....	183
a. First pillar instruments .....	184
1. Unaffected first pillar instruments .....	184
2. Unlisted first pillar instruments.....	185
a. The data retention directive.....	185
b. First pillar instruments governing SIS II.....	186
b. Title VI instruments .....	188
1. Unaffected third pillar instruments .....	188

a. Complete and coherent set of rules more detailed than the framework decision.....	188
i. Should not be affected .....	189
ii. Europol .....	191
iii. Eurojust.....	192
iv. SIS .....	192
v. CIS .....	193
vi. Direct access .....	193
vii. Decision integrating the Prüm Convention .....	194
b. Provisions on use of personal data.....	194
i. Should remain unaffected .....	194
ii. MLA Convention.....	195
iii. European Evidence Warrant .....	196
iv. SIC and the framework decision on simplifying the exchange of information and intelligence between law enforcement authorities.....	196
v. CIS .....	197
vi. Criminal records .....	197
vii. Financial Intelligence Units .....	197
viii. Passenger Name Records data for law enforcement purposes .....	198
2. Unlisted third pillar instruments .....	199
c. Council of Europe instruments.....	200
B. Applicable instruments in cooperation with third states .....	201
1. Judicial cooperation .....	202
2. Law enforcement cooperation.....	204
a. Europol.....	204
b. Transfer of passenger name records to law enforcement authorities of third states .....	206
3. Effects of the Framework Decision on Data Protection in Criminal Matters .....	208
a. Significance of article 26 on relationships with third states .....	208
b. Customs Information System (CIS).....	209
c. Europol and Eurojust's agreements with third states .....	210
d. Member states' agreements with third states .....	211
e. Agreements between the Union and third states .....	213
C. Conclusion .....	213
Chapter III. Cooperation EU – US.....	219
A. US data protection standards.....	220
1. Personal data in the US .....	220
a. American definition of personal data .....	220
b. Right to a private life in the US: reasonable expectation of privacy .....	222
c. Personal data protection .....	225
1. Fourth Amendment protection in non-criminal cases .....	227
2. Fair Information Practice Principles .....	228
a. Background .....	228

b. Principles .....	229
i. General requirements .....	229
ii. Public notice requirement .....	231
iii. Rights of individual data subjects .....	232
c. Supervision.....	234
3. Data protection provisions in US Acts.....	235
a. Sectoral legislation on personal data processed by government agencies.....	236
i. Privacy Act .....	236
ii. Federal Records Act .....	240
iii. E-Government Act.....	241
iv. Specific sectoral acts.....	243
b. Sectoral legislation on personal data processed by private companies .....	245
c. Self-regulation.....	247
d. Technologies of privacy.....	248
4. Supervision .....	248
2. Personal data in the US in criminal matters.....	249
a. Constitutional protection of personal data in criminal matters.....	250
1. Fourth Amendment .....	250
a. Personal information .....	251
b. People, not places.....	251
c. Persons protected by the Fourth Amendment .....	251
d. Search .....	252
i. Warrant .....	253
ii. Probable cause .....	253
iii. Supported by Oath or affirmation .....	254
e. Admitting evidence in criminal proceedings.....	255
f. Violating the Fourth Amendment.....	256
i. Suppressing evidence: the exclusionary rule .....	256
ii. Exceptions to the warrant requirement .....	257
iii. Evidence brought forward by private parties.....	260
2. Fifth and Sixth Amendment.....	260
b. Data protection in legal instruments within the US .....	261
1. Records held by the government.....	262
a. Privacy Act and Freedom of Information Act.....	262
i. Accuracy standard and exemptions.....	263
ii. Government use for compatible purposes.....	264
iii. Disclosure of data compiled for law enforcement purposes .....	267
b. E-Government Act .....	268
i. Privacy policies .....	268
ii. Privacy Impact Assessments (PIAs) .....	269
a. PIA of a transfer to law enforcement authorities.....	269
b. PIA of a transfer from law enforcement authorities.....	270
2. Records and objects held by third parties .....	271
a. No reasonable expectation of privacy .....	271
b. Subpoenas .....	272
c. National Security Letters.....	274
3. Interception of communications.....	276

a.	Interception of oral communications.....	277
b.	Electronic surveillance.....	278
i.	Phone numbers and addressees.....	278
ii.	Communications in transmission.....	279
iii.	Stored wire and electronic communications.....	280
iv.	Assistance from telecommunication carriers.....	281
v.	The Foreign Intelligence and Surveillance Act (FISA) and the Patriot Act.....	281
a.	The wall and the windows built into it.....	282
b.	A FISA warrant.....	285
c.	Minimization procedures.....	288
d.	Amendments to FISA by the Patriot Act.....	289
e.	Amendments to FISA by the Protect America Act.....	290
4.	Data retention in the US legal instruments.....	292
5.	Supervision.....	292
3.	Compatibility between the EU and the US in criminal matters?.....	293
a.	Similar definitions.....	294
b.	A common source.....	295
c.	Quality standards.....	296
1.	Quality standards for personal data.....	296
2.	Quality standards for processing of personal data.....	298
a.	Purpose limitation and compatibility of the use of personal data.....	298
i.	Different reasoning.....	298
ii.	Compatibility.....	299
iii.	Purpose deviation.....	300
b.	Retention of personal data.....	301
3.	Supervision.....	302
d.	Conclusion: adequacy of the US data protection standards.....	302
B.	Cooperation between the EU member states and the US.....	303
1.	Exchange of data in the absence of a treaty.....	305
a.	Letters rogatory.....	305
b.	Subpoenas.....	306
c.	'Cop to cop' exchange.....	308
2.	Treaty-based exchange of data.....	309
a.	Multilateral treaties.....	309
1.	Data protection provisions in multilateral treaties.....	310
2.	Complemented by bilateral treaties.....	312
b.	Bilateral treaties.....	313
3.	Adequacy requirement.....	314
C.	Law enforcement cooperation: the Europol – US Agreements.....	316
1.	Relations with third states: adequacy requirement.....	316
2.	Safeguarding data protection standards before negotiations start.....	318
3.	The 2001 Europol – US Agreement on the exchange of non personal data.....	319
4.	The 2002 Supplemental Europol – US Agreement on the exchange of personal data and related information.....	320
a.	Undermining the traditional speciality rule.....	321

b. Adequate level of data protection .....	322
1. Quality standards for personal data .....	323
2. Quality standards for processing of personal data .....	324
a. Purpose limitation .....	325
i. Widened purpose limitation .....	325
ii. Other purposes .....	328
iii. Competent authorities .....	328
iv. No generic restrictions .....	330
v. Lawful derogations from the purpose limitation principle? ..	330
a. Legality .....	331
b. Necessity .....	332
vi. Data retention .....	334
c. Interests of member states providing personal data .....	334
5. Conclusion .....	335
D. Eurojust – US Agreement .....	336
1. No speciality rule .....	336
2. Adequate level of data protection .....	337
a. Quality standards for personal data .....	338
b. Quality standards for processing of personal data .....	339
1. Purpose limitation .....	340
a. Widened purpose limitation .....	340
b. No generic restrictions .....	343
2. Lawful derogations from the purpose limitation principle? .....	343
a. Legality .....	344
b. Necessity .....	344
3. Data retention .....	345
c. Interests of member states providing personal data .....	345
3. Conclusion .....	345
E. Relations EU – US in criminal matters .....	346
1. The 24-38 agreements: a different type of cooperation .....	347
2. EU – US Agreement on mutual legal assistance in criminal matters .....	349
a. The EU-US MLA Agreement and the bilateral written instruments .....	350
b. Adequate level of data protection .....	352
c. No speciality rule .....	353
1. MLA Agreement .....	353
2. Bilateral written instruments .....	354
d. Data protection provisions .....	356
1. Quality of personal data .....	356
2. Quality of processing of personal data .....	357
a. Purpose limitation .....	357
b. Data retention .....	358
3. A special case: the PNR Agreements .....	358
a. Passenger Name Record .....	359
b. Background to the PNR Agreements .....	360
1. US legislation on aviation security .....	360
2. Data needed from EU air carriers .....	363
c. PNR Agreements .....	363
1. Preparations .....	363
2. First pillar legal basis of the 2004 PNR Agreement .....	366

3. Annulment by the ECJ .....	367
4. 2006 Interim PNR Agreement and 2007 PNR Agreement .....	369
d. Data protection issues .....	370
1. Quality of personal data .....	370
a. Push and pull .....	371
b. List of data .....	373
c. Accuracy and relevance of data .....	375
2. Quality of processing of personal data .....	376
a. Purpose limitation .....	376
i. Use of PNR data .....	376
ii. Data sharing .....	378
b. Data retention .....	380
i. Time limits .....	380
ii. Applicable Undertakings .....	382
3. Transfer of PNR data to third states .....	383
e. Compliance with EU data protection standards .....	384
4. SWIFT case .....	384
a. Administrative subpoenas .....	386
b. Data needed from SWIFT .....	387
c. Applicable rules on data protection .....	389
1. Belgian Data Protection Law .....	389
2. Safe Harbour Principles .....	389
d. US Representations .....	390
e. Is SWIFT a data controller or processor? .....	391
f. Data Protection issues .....	393
1. Quality of personal data .....	393
2. Quality of processing of personal data .....	394
a. Purpose limitation .....	394
b. Data retention .....	395
c. Data sharing .....	396
3. Independent oversight .....	397
4. Transfer of data to third states and Safe Harbour .....	398
g. Compliance with EU data protection standards .....	399
5. High Level Contact Group .....	399
a. Common principles .....	400
b. Binding or non binding instrument .....	403
6. The Future Group reports .....	404
7. The Lisbon Treaty and data protection .....	407
8. Conclusions .....	409
 Chapter IV. Conclusions .....	 413
A. Framed inconsistencies within the EU data protection legislation .....	413
1. Widening of existing data protection principles .....	413
2. In a framework of formalized non-compliance with the data protection principles .....	414
3. Double standards in law enforcement and judicial data exchange .....	415
B. An adequate transatlantic bridge? .....	416

1. A consistent widening of existing data protection principles.....	416
2. Structural differences.....	417
3. Can we build a bridge on adequacy? .....	418
C. Future transatlantic relations in criminal matters: building or burning bridges?.....	420
Chapter V. Bibliography.....	423
A. Legal and policy instruments .....	423
B. Jurisprudence .....	457
C. Literature.....	461
D. Other sources .....	473