Communications services and law enforcement assistance

Neil Brown
neil@neilzone.co.uk | http://neilzone.co.uk

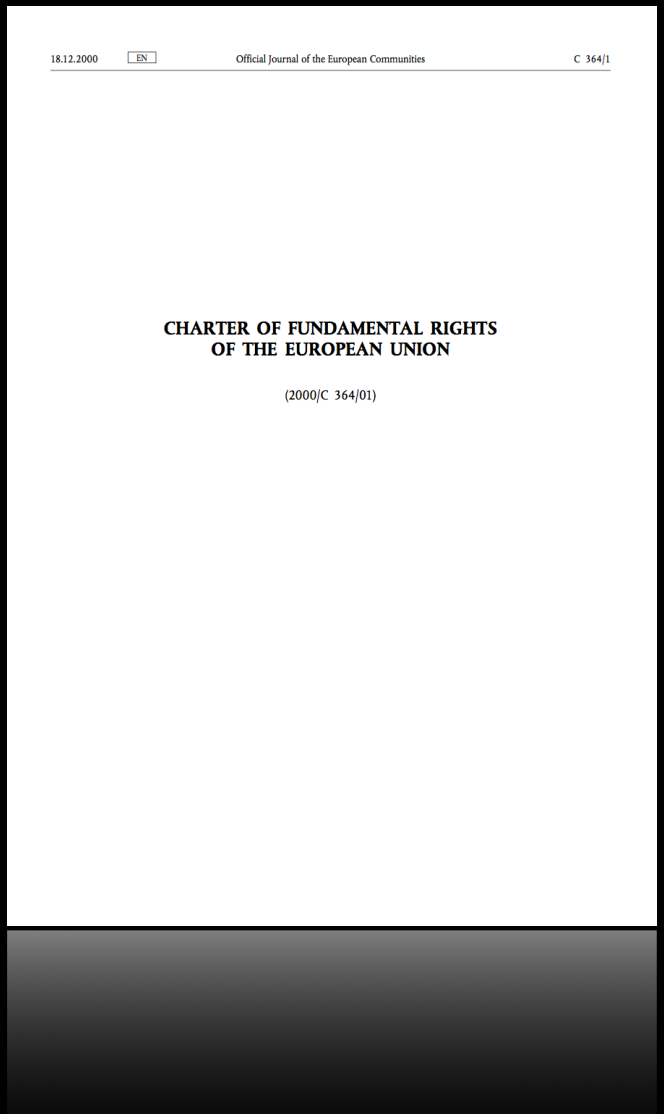
What we will cover

Fundamental rights

Confidentiality of communications

10 different bases of assistance

Fundamental rights



18.12.2000 EN Official Journal of the European Communities C 364/1

CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION

(2000/C 364/01)

Art. 7: respect for private life

Everyone has the right to respect for his or her private and family life, home and communications.

Art. 8: protection of personal data

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.

Art. 11: freedom of expression and information

1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.

2. The freedom and pluralism of the media shall be respected.

Confidentiality of communications

"Member States shall ensure the confidentiality of communications and the related traffic data by means of PCN and PECS through national legislation"

Confidentiality of communications

"In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except where legally authorised to do so in accordance with Article 15(1)."

Confidentiality of communications

"In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except where legally authorised to do so in accordance with Article 15(1)."

1: Interception

Part 1, Chapter 1, RIPA 2000

Generally prohibited

Interception of a communication in the course of transmission by:

- modifying or interfering with telecoms system;
- monitoring transmissions; or
- monitoring transmissions by wireless telegraphy

so as to make communication available while being transmitted to a person other than sender or recipient.

“Interception” includes

Recording for later access

“Stored communications” (*Coulson*)

“Interception” excludes

Broadcasts for general reception

Conduct in respect of traffic data, or necessary to identify traffic data

Criminal offences

Intentional unlawful interception on public or private networks

Conviction on indictment: 2 years' imprisonment and/or fine

Administrative penalty

Unintentional interception on public system, not an attempt to implement a warrant

IOCCO can impose penalty up to £50,000

Two types of lawful interception

Warranted interception

Non-warranted lawful interception

Warranted interception

Administrative, not judicial, process

Sought by permitted person (s6(1))

Any principal SoS, but usually HS, FS, DS, SoS NI or CSfJ in Scotland

Necessity and proportionality (s5)

National security

Preventing or detecting serious crime

Economic well being of UK, relevant to national security

Serious crime MLAT

Two types of warrant

s8(1): named person or single set of premises, schedule of identification factors

s8(4): external communications (s20), no requirement to name

Duration of warrants

Generally three months (s9(6)(c))

National security: six months (s9(6)(a))

Can be renewed at any point (s9(1)(b))

Must be cancelled if no longer needed (s9(3))

Duty to assist

Duty to take all reasonably practicable steps (s11(5)) as are notified for giving effect to the warrant (s11(4))

Enforceable via injunction (s11(8))

Criminal offence: "knowingly failing to comply" (s11(7))

Secrecy of warranted interception

Pretty much everything secret

Includes “existence of warrant”

Criminal offence of breach of secrecy (five years on indictment)

Maintenance of capability

Obligations to ensure can provide assistance (s12(1))

Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002

Duty to comply, enforceable via injunction

2: Data retention

Data Retention and Investigatory Powers Act 2014

Data Retention Regulations 2014

“Retention notices”

Served by SoS (s1(1))

Retention, not generation

Public providers only

Duty to comply

Duty to comply (Reg. 12(1))

Enforceable via injunction (Reg. 12(2))

What data?

Schedule 1 to DRR

NAT/PAT logs: s21, CTSA 2015

Specified per CSP, along with retention period, in each retention notice

Human rights compliant?

C-293/12, *Digital Rights Ireland*

Struck down DRD — but not necessarily all "data retention"?

Wait and see: JR lodged

3: Access to retained data

Part 1, Chapter 11, RIPA 2000

Framework to acquire communications data

Three types: (s21(4))

- Traffic data
- Use data
- Subscriber data

Not content

Disclosure notice

Notice placed on provider (s22(4))

Includes “obtain” (s22(4)(a))

Not just public providers

No inherent limit

Duty to comply

Duty to comply (s22(6)) enforceable via injunction (s22(8))

No right to question notice, but limitation of "reasonably practicable" (s22(7))

Report errors to IOCCO

Urgent oral process

Extremely urgent situations

Still requires authorisation

Written notice within one day

Reportable error if not provided

Access to retained data under other frameworks

Social Security Fraud Act 2001

2001 CHAPTER 11

Salmon and Freshwater Fisheries Act 1975

1975 CHAPTER 51

Mostly prohibited

s1(6) DRIPA, in force 13th April 2015:

s22(4) RIPA

Court order / judicial mandate

"as provided by regulations"

Does not affect SAR (s27(5) DPA 1998))

4: Police powers of access and seizure

Police and Criminal Evidence Act 1984

Production orders

General powers of seizure

Production orders

Non-confidential material (s8(1)): enter, seize and retain

Special procedure (s14): express or implied undertaking of confidence

General powers of seizure

Where lawfully on any premises

Evidence of offence, and necessary to prevent concealment, loss or destruction

Not retained communications data

5: Disclosure of encryption keys

Part III, RIPA 2000

Relatively little written about its use in practice

Disclosure notice (s49)

LEA or IA has protected information

Necessary and proportionate

Access otherwise not reasonably practicable

Cannot be used to obtain key only used for generation of electronic signatures (s49(9))

Broad definition of "key"

"Any key, code, password, algorithm or other data

the use of which allows access to the electronic data; or

facilitates the putting of the data into an intelligible form" (s56(1))

Two types of notice (s50)

General notice

Provide plaintext (i.e. decrypt), or

Provide key

Specific notice (s50(3)(c))

More intrusive

Only satisfied by providing key

Limited to “special circumstances” and where proportionate

Not secret by default

Secrecy provision can be added in some circumstances (s53(3))

Non-specific offences (e.g. impeding an investigation)?

Criminal offences

Knowingly failing to comply (s51)

Tipping off (s54)

Up to five years' imprisonment

Knowingly failing to comply

Presumption that, where someone was in possession of a key, they still are

Unless sufficient evidence otherwise, which cannot be disproved beyond reasonable doubt

6: Directions in the interests of national security

s94, Telecommunications Act 1984

Virtually nothing written about it

What is in scope?

Directions of a general character which appear to SoS to be necessary in interests of national security

Proportionality test

What is in scope?

Public electronic communications networks only

Not secret by default, but provision for secrecy (s94(5))

7: Mobile devices in prisons

Two aspects

Jamming of signals

Disconnection / blacklisting

Jamming of signals

Unauthorised use of wireless telegraphy

Memorandum of Understanding

Prisons (Interference with Wireless Telegraphy) Act 2012

Safeguards: NOMS and Ofcom

Disconnection / blacklisting

Telecommunications Restriction Order (s80(1), Serious Crime Act 2015)

Duty to take "whatever action specified"

No regulations currently in place

8: Suspension of entitlement to operate

SoS can direct Ofcom to remove a provider's entitlement to operate (s132, Communications Act 2003) for an indefinite period

Criminal offence, and civil claims (s133)

9: Interference with wireless telegraphy

Powers to LEAs / IAs, rather than duties on CSPs

Part 3, Police Act 1997

s5, Intelligence Services Act 1994

10: Obligations in state of emergency

Broad powers to compel available under Civil Contingencies Act 2004 (s19(1))

MTPAS (was ACCOLC)

Emergency alerts under PECR (Reg. 16A)

Interception

Data retention

Access to retained data

Police powers of access and seizure

Disclosure of encryption keys

National security

Phones in prisons

Suspension of entitlement

Interfering with wireless telegraphy

Obligations in states of emergency

Neil Brown
neil@neilzone.co.uk | http://neilzone.co.uk