

Council of Europe  
Conseil de l'Europe

2 February 2017

Peter Kimpian,  
Data Protection Unit  
of the Council of  
Europe

PDP on Next-  
Generation gTLD  
Registration  
Directory Service  
(RDS)

## Art 12 of the Universal Declaration of Human Rights:

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

## Art 17 of the International Covenant on Civil and Political Rights:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.

## Art 8 of the European Convention on Human Rights:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others



Individuals have to be in control of their personal data (trail of the data)

# Main principles

- Necessity
- Proportionality
- Purpose specification/Purpose limitation

- Adequate, relevant and not excessive in relation to the purposes for which they are stored
- Accurate and, where necessary, kept up to date
- Preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored



- Legitimate aim/purpose
- Lawful and fair means of data processing (ex: online marketing)
- Valid legal basis (law, consent, contract, vital interest of the individual, etc.)

- state security
- public safety
- the monetary interests of the State
- the suppression of criminal offences

## Exemptions

- protecting the data subject or the rights and freedoms of others
- statistical and research purposes

*BUT, processing of personal data for national security, law enforcement etc. purposes can constitute an interference with the right to privacy and to the protection of personal data*

The interference has to be “*provided for by law and has to constitute a necessary measures in a democratic society*” (based on law, necessary and proportionate to the aim pursued)

Same rules  
as for  
processing

Discloser of  
data/Third party  
access to  
data/Further  
data processing

*BUT, here there is a third party  
and a second purpose and it is not  
for the original data controller to  
define the secondary purpose, it  
defines the conditions, the  
procedures etc. under which it can  
disclose personal data if all legal  
requirements met*

*Purpose for  
processing*

≠

*Purpose for  
disclosing*



*New data processing has to  
comply with*

- Legitimate aim/purpose
- Lawful and fair means of data processing
- Valid legal base (law, consent, contract, vital interest of the individual, etc.)
- Adequate, relevant and not excessive in relation to the purposes for which they are stored
- Accurate and, where necessary, kept up to date
- Preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored

# Accountability

*“A personal information controller should be accountable for complying with measures that give effect to the Principles stated above”* - APEC Privacy Framework

*“Each Party shall provide that controllers and, where applicable, processors take all appropriate measures to comply with the obligations of this Convention and be able to demonstrate, in particular to the competent supervisory authority provided for in Article 12bis, that the data processing under their control is in compliance with the provisions of this Convention.”* - Modernised CoE Convention 108

*“A data controller should be accountable for complying with measures which give effect to the principles stated above”* - updated OECD Privacy Framework, 2013

→ So collection of personal data for a specific purpose  
=  
responsibility for the implementation of the privacy and data protection principles for that purpose

*“ The Data Protection Directive requires data controllers to observe a number of principles when they process personal data. These principles not only protect the rights of those about whom the data is collected (“data subjects”) but also reflect good business practices that contribute to reliable and efficient data processing.”* - EU Directive 95/46/EC

*“ The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’)”* - Art 5, GDPR

13<sup>th</sup> March  
2017

!!!

“Privacy  
Summit” –  
ICANN 58

[www.coe.int/dataprotection](http://www.coe.int/dataprotection)

[dataprotection@coe.int](mailto:dataprotection@coe.int)



**Thank you  
for your  
attention**

Peter Kimpian

Data Protection Unit  
Human Rights and Rule of Law

CONSEIL DE L'EUROPE - COUNCIL OF  
EUROPE

tel : + 33(0) 3 90 21 58 51  
Email: [peter.kimpian@coe.int](mailto:peter.kimpian@coe.int)

