Importance of Purpose Limitation

- A broad interpretation of the purpose of collection, use and disclosure allows subsequent reuse for different reasons
- Purpose limitation is the first premise of data protection analysis, purpose must be narrow, proportionate

14 February 2017

Peter Kimpian,
Data Protection Unit
of the Council of
Europe

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

Modernised Convention 108 - Article 5 – Legitimacy of data processing and quality of data

1. Data processing shall be proportionate in relation to the legitimate purpose pursued and reflect at all stages of the processing a fair balance between all interests concerned, whether public or private, and the rights and freedoms at stake.

4. Personal data undergoing processing shall be:

a. processed fairly and in a transparent manner;

b. collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is, subject to appropriate safeguards, compatible with those purposes;

c. adequate, relevant and not excessive in relation to the purposes for which they are processed;

d. accurate and, where necessary, kept up to date;

e. preserved in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed.

2. Each Party shall provide that data processing can be carried out on the basis of the free, specific, informed and unambiguous consent of the data subject or of some other legitimate basis laid down by law.

3. Personal data undergoing processing shall be processed lawfully.

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Retail company and consumers' health conditions

EXAMPLES

for purpose specification

Personal data collected by drones – how to narrow down the purpose of processing

Public authorities data processing (ex: immigration vs. law enforcement purposes)

Digital Ireland and Tele2 case on data retention for law enforcement purposes by private companies

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Further examples

WG29 Opinion WP 203 on purpose limitation

"Practical examples to illustrate purpose specification" and "Practical examples to illustrate the compatibility assessment"

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

www.coe.int/dataprotection

dataprotection@coe.int

Peter Kimpian

Data Protection Unit
Human Rights and Rule of Law

CONSEIL DE L'EUROPE - COUNCIL OF EUROPE

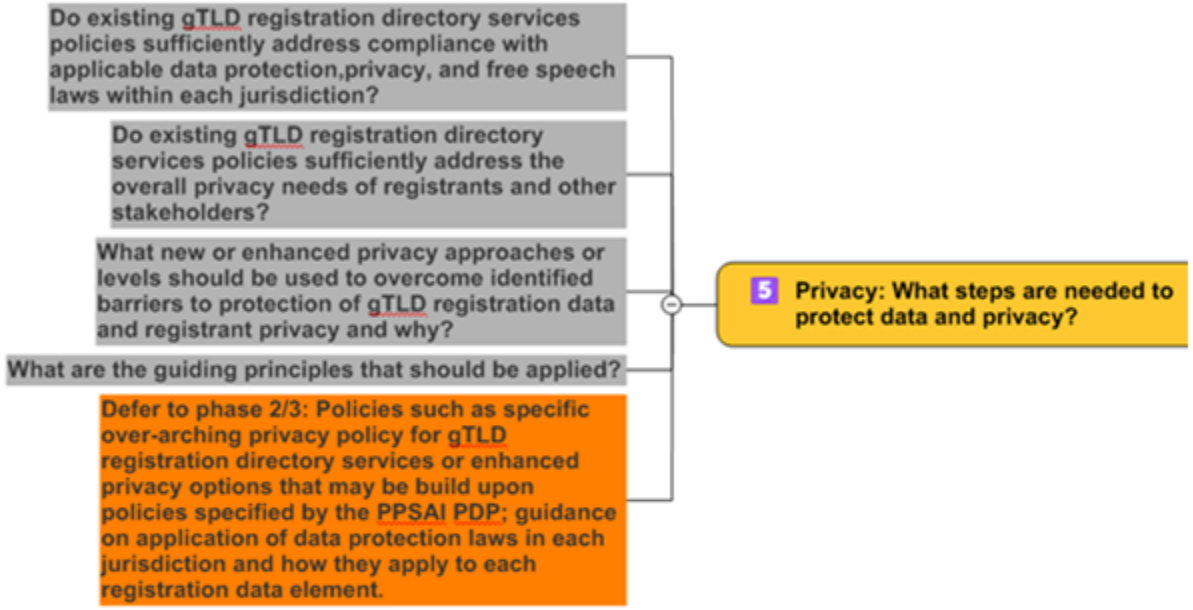
tel : + 33(0) 3 90 21 58 51
Email: peter.kimpian@coe.int

Thank you for your attention

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

For "thin data" only -- Do existing gTLD RDS policies sufficiently address compliance with applicable data protection, privacy, and free speech laws about purpose? If not, what requirements might those laws place on RDS policies regarding purposes associated with "thin data"?

4. Charter Question: Privacy



FOCUS OF INITIAL DELIBERATION WILL REMAIN "THIN DATA" & POTENTIAL PURPOSES FOR "THIN DATA" SUCH AS

- Domain Name Control
- Technical Issue Resolution
- Domain Name Certification
- Business DN Purchase or Sale
- Academic/Public Interest DNS Research
- Regulatory and Contractual Enforcement
- Criminal Investigation & DNS Abuse Mitigation
- Legal Actions
- Individual Internet Use

Note: Additional work on definitions will be needed to clarify purpose for collection vs. purpose for disclosure/use, as well as who/what is collecting registration data.

Sources:
KeyConceptsDeliberation-WorkingDraft-24January2017.pdf
GNSO PDP on Thick WHOIS Final Report page 10

See also related materials:

Intro Presentations by Kimpian and Perrin:
Kimpian_pdp_rds_2_2_17.pdf

PDP WG Links and Summaries to Privacy-Related Input Documents:
https://community.icann.org/download/attachments/56986791/RDSPrivacy-InputsAndSummaries-24May2016.pdf

Example of Thin WHOIS record:

Domain Name: CNN.COM
Registrar: CSC CORPORATE DOMAINS, INC.
WHOIS Server: whois.corporatedomains.com
Referral URL: http://www.cscglobal.com
Name Server: NS1.TIMEWARNER.NET
Name Server: NS3.TIMEWARNER.NET
Name Server: NS5.TIMEWARNER.NET
Status: clientTransferProhibited
Updated Date: 04-feb-2010
Creation Date: 22-sep-1993
Expiration Date: 21-sep-20184

Example of a ccTLD Registry policy statement related to the purpose of WHOIS*

.eu -- Excerpted from https://eurid.eu/en/other-infomation/whois-policy/

Section 2. WHOIS Look-Up Facility

2.1. Introduction

The Public Policy Rules require the Registry to provide a WHOIS look-up facility where, by typing in a .eu Domain Name in one of the available scripts, information about the administrative and the technical contact administering the Domain Name can be found.

When a Domain Name is registered the information relating to that registration sits in a WHOIS database in compliance with the rules set out below. The information collected includes Registrant contact information, the Registrar involved and details of the name servers to which the Registry delegates authority for the Domain Name and is further set out in Section 2.4. hereof.

By going to the Website of the Registry and typing in the Domain Name in the WHOIS look-up facility, information about that name and the Registrant can be accessed in accordance with the rules set out below.

When registering a Domain Name, the Registrant is required to accept the Registry's Terms and Conditions which authorises the Registry to make some personal data accessible on its web site, along with some other technical data, in order to guarantee the transparency of the domain name system towards the public.

2.2. Purpose

The purpose of the WHOIS database, as set forth in the first paragraph of Article 16 of Commission Regulation (EC) No 874/2004 of 28 April 2004 is to provide reasonably accurate and up to date information about the technical and administrative points of contact administering the domain names.

If the Registry is holding false, incorrect or outdated information, the Registrant will not be contactable and may lose the name. By deliberately submitting inaccurate information, the Registrant would also be in breach of the Terms and Conditions which could also lead to loss of the Domain Name.

* Note: Example given here for illustration only; no assumption is made regarding compliance with applicable laws.