COMMENTS OF THE INTERPOL DATA PROTECTION OFFICE (IDPO) ON THE DRAFT PRACTICAL GUIDE ON THE USE OF PERSONAL DATA IN THE POLICE SECTOR – COUNCIL OF EUROPE CONSULTATIVE COMMITTEE OF CONVENTION 108

GENERAL COMMENTS

The INTERPOL Data Protection Office (IDPO) praises the work of the Council of Europe Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD) on the draft practical guide on the use of personal data in the police sector.

IDPO recalls that the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) has, since its opening for signature in 1981, acted as a basis for the adoption of the first data protection rules at INTERPOL in 1982 and several updates since, including INTERPOL's Rules on the Processing of Data (RPD), a new code with over 135 detailed binding provisions adopted in 2011 and a new Statute adopted in 2016 for the Commission for the Control of INTERPOL's files, INTERPOL's independent Oversight Board.

Furthermore, Recommendation 87(15) regulating the use of personal data in the police sector has similarly been of great value within the law enforcement community over the last three decades. Due to its continued application, IDPO appreciates the regular evaluation of Recommendation 87(15) as well as the initiative to develop a draft practical guide looking at the implementation of the Recommendation at a more operational level.

During the T-PD Bureau meetings held in 2016, IDPO provided comments on an early version of the draft guide and noted the inclusion of those comments in the later versions.

IDPO welcomes the modern light the guide shines upon the practical interpretation of Recommendation 87(15), as the document provides comprehensive guidance for the implementation of data protection principles and safeguards taking into account important technological developments, such as big data analytics, impacting the manner by which data is being processed by law enforcement agencies today.

INTERNATIONAL TRANSFERS & APPROPRIATE SAFEGUARDS

Bearing in mind the increasingly global and fast paced nature of today's crime landscape, the need for enhanced international police cooperation cannot be understated. Following the wave of terror

attacks over the last few years, the UN Security Council reiterated the need for stronger international cooperation in the fight against terrorism, inter alia, by intensifying and accelerating the exchange of operational information (S/RES/2178 (2014)) as well as information about foreign terrorist fighters and other individual terrorists and terrorist organizations, including biometric and biographic information (S/RES/2322 (2016)).

Regarding international data transfers, the guide is clear that this should only take place to countries that provide an appropriate level of protection. IDPO appreciates mention in the practical draft guide of INTERPOL's channels to ensure a legally justified international data transfer with appropriate safeguards in place.

COMMENTS ON SPECIFIC SECTIONS OF THE PRACTICAL DRAFT GUIDE

IDPO noted that most of its comments have already been addressed in the latest draft version (rev6) of the practical guide, for instance expanding the scope of application to predictive policing which has been developing as an important area of today's police work. IDPO wishes to address the following additional comments relating to specific sections:

-Section 2, par.3: collection of data and use of data:

"*If police collect personal data it must fit into the legislative framework and should always be in connection with on-going investigations. "*

This seems to be narrower than the scope set out in point 1 (scope) which has clearly been expanded in the amendments. These amendments are appreciated as they provide a more realistic representation of the diverse missions of LEAs. It is important to ensure that the rest of the document is consistent with these amendments.

-**Section 2, par.4: collection of data and use of data:**

"*Police should apply the data –minimisation principle at all stages of the processing"*

Whereas this is an important data protection principle, one could question how this is/will remain compatible with big data analysis where the importance or correlation between certain data may only become apparent after analyses have taken place on sufficiently large data sets, e.g. when dealing with cyber security.

-**Section 12, first line: communication of data by the police to private parties**

"*There may be occasions when, under strict conditions, the police can communicate data domestically to private bodies"*

As situations can occur where regional and international police bodies may as well, under very strict conditions, communicate data to private bodies, it is suggested either to delete the word "domestically" or to include a similar paragraph in the section 13 on international transfer. Additionally, it would not harm to add "very strict conditions" instead of "strict conditions" taking into consideration the risks inherent to such transfers.

-**Section 13, par.4 on international transfer (p.11-Rev6):**

"An appropriate level of data protection should *always* be guaranteed if data are to be transferred to countries not participating in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)."

It seems rather restrictive and strongly worded to include the "always" in the above statement, as situations can be foreseen in which the risk to the security of individuals will outweigh the risk to the rights of the data subject, e.g. imminent terror attack - transferring the name and image of the suspect to police in another country without appropriate safeguards.

It is therefore suggested to delete the word “always”.

INTERPOL DATA PROTECTION OFFICE

16/07/2017