International law enforcement information exchange in an evolving data protection landscape

Meeting of EU Heads of Single Point of Contact (SPOC)
Department of Criminology, Criminal Law and Social Law | UGent
Ghent | 3 July 2018

Prof. Dr. Gert Vermeulen
t. +32 9 264 69 43
f. +32 9 264 84 94
Gert.Vermeulen@UGent.be

GHENT UNIVERSITY

FACULTY OF LAW AND CRIMINOLOGY

IRCP Institute for International Research on Criminal Policy
Ghent University

Structure

disclosure slide | background

SPOC Guidelines & Strengthening (relevant excerpts)

an evolving data protection landscape

- overview
- CJEU standard setting (background)
- LED as point of departure, sometimes connecting to non-LED context
- non-LED instruments (punctual issues)

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

Disclosure slide | background

full-time academic

- international criminal law, EU criminal and JHA policy, cross-border police and judicial cooperation in criminal matters
- [other]

with data protection background

- BE: Privacy commissioner Belgian DPA
- EU: member SCG SIS II, Eurodac, VIS, CIS, Europol Cooperation Board, BTLE (Borders, Travel, Law Enforcement subgroup EDPB)
- CoE: T-PD expert (Consultative Committee Convention 108 + 2nd Protocol)
- ICDPPC: expert group enforcement cooperation

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

EIXM | SPOC Guidelines

Resources (1.2)

- multi-agency organisation, composed of staff coming from/belonging to different services and/or Ministries including criminal police, public order police, border guards, customs, and judicial authorities

Availability of national databases and networks (2)

- Subject to data protection rules and the authorisation level of respective staff members, the SPOC has access, direct or at request from competent authorities, to the broadest range of relevant national databases and in any case to all those databases available to the authorities represented in the SPOC. This covers in particular law enforcement databases, identity documents database, vehicle registration, national visa database, immigration office database, prisoners database, DNA databases, fingerprint databases, information exchange with the national liaison officers, border control database, trade register, ANPR etc.
- Ideally, all members of the SPOC have access to all of these databases, if necessary on a hit/no hit only basis; if this is not possible, all databases are accessible to the unit on a 24/7 basis, where necessary via on-call duty officers
- The SPOC has arrangements for indirect (e.g. on a hit/no hit basis) but quick, effective and efficient access to relevant databases of other authorities or bodies, where appropriate subject to judicial approval. This applies to records of companies providing electricity, water, phone and other communication supplies

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

SPOC Guidelines | International infoex

General rules for international communications (3.2)

- A request is sent through one channel only (in principle)

Specific rules for the choice of channel (3.3)

- Possible cooperation channels:
  - bilateral and regional liaison officers
  - SIRENE Bureau
  - Europol (ENU, liaison officers at Europol)
  - Interpol (NCB, liaison officers at Interpol)
  - jointly staffed units in border regions, in particular PCCCs
  - direct contacts between concerned authorities
  - coordination units for Naples II/ Anti-Fraud Information System (AFIS)/CIS/FIDE/FIU
- Proposed criteria for use of channels:
  - Europol | EU reach and its mandate (terrorism, serious and organised crime, 2 or more MS concerned) | Contributions to AWF, EMPACT projects, analysis, JITs | Exchange of classified information (up to EU RESTRICTED) | Exchange under Swedish Framework Decision (SIENA form/UMF) | Urgency
  - Interpol | Exchange of information with EU Member States and third countries | Alerts (wanted/missing persons, arrest warrants, extraditions) | Verification of persons identity/documents | 24/7 availability and urgency | impact LED?
  - SIRENE | SIS alerts | Cross border surveillance | 24/7 availability and urgency
  - Bilateral/regional channels | Exchange of classified information (depends of concluded bilateral agreements) | Urgency, trust | status existing agreements post-LED?
  - PCCC | Local reach and exchange of information about crimes committed in the border area | direct access to national databases and in PCCCs or during joint actions? (e.g. Benelux 2018)
  - Naples II/AFIS/CIS/FIDE/FIU | Specific information exchange/ legal assistance

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

SPOC Strengthening

- single registration number, unique for the involved cooperation channel & relating folder
- “Before being distributed to the operating agencies, the data contained in each request which arrives at the SPOC, should undergo an automated cross-check against national and international databases available at the SPOC” | lawfulness, purpose, legitimacy?
- CMS: “Ideally, the national case management systems should be (inter)connected to SIS/SIRENE and Interpol, as well as to Europol via SIENA” | interconnection, seriously?

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

An evolving data protection landscape

overview

- from Directive 95/46 to GDPR (Regulation 2016/679)
- from FD 2008 to Law Enforcement Directive 2016/680 (LED)
- from Europol 2009 Decision to Europol 2016 Regulation
- from SIS II 2006 Regulation/2007 Decision to 3 SIS II recast Regulations (border checks, return, police and judicial cooperation) from Regulation 45/2001 to Recast Regulation 45/2001
- 2 proposed Interoperability Regulations (borders and visa respectively police and judicial cooperation, asylum, migration)
- (ECRIS and) ECRIS-TCN
- CJEU standard setting

approach

- CJEU standard setting (mere background)
- LED | point of departure, sometimes connecting to non-LED context
- ECRIS and ECRIS-TCN
- non-LED instruments (punctual issues)

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

CJEU standard setting

invalidating both EU & US generalised data retention practices

- 2014 Digital Rights Ireland (invalidating EU Data Retention Directive)
- 2015 Schrems v Data Protection Commissioner (invalidating Safe Harbour)
- 2016 Digital Rights Ireland/*Quadrature du Net* and Others v Commission (actions for annulment of Privacy Shield)
- 2016 Tele2 Sverige AB (data retention ePrivacy Directive)
- October 2017 Irish High Court (Schrems *bis,* SCC, preliminary ruling)
  - distinction mass/bulk *searching* (targeted, not indiscriminate), but involving the collection of non-relevant data, i.e. bulk *acquisition, collection or retention* = mass indiscriminate processing (Upstream)

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

LED | Scoping and relation to GDPR

replaces FD 2008 (which was limited essentially to onward transfers)

application: processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security

- excluded from scope: Europol, Eurodac, SIS II, VIS, ECRIS, ECRIS-TCN, EES, ETIAS, Prüm, …
- competent authorities: FIUs, PIUS, 'mixed' LE authorities, SPOCs …?
  - (Article 3(7)) (recital 11) […] may include […] also any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of this Directive. Where such a body or entity processes personal data for purposes other than for the purposes of this Directive, Regulation (EU) 2016/679 applies. […]
- criminal offences: inclusive of administrative offences? | SPOCs?
  - (recital 13) […] should be an autonomous concept of Union law as interpreted by the Court of Justice
- public security: not national security; quid public order/safety and administrative policing? | quid SPOCs? (on the same page? intelligence services data (regulated in Article 36 SIS II Decision; otherwise?), mixed treaties (Benelux 2018, …), administrative authorities, …)
  - (recital 12) […] include the exercise of authority by taking coercive measures such as police activities at demonstrations, major sporting events and riots. They also include maintaining law and order as a task conferred on the police or other law-enforcement authorities where necessary to safeguard against and prevent threats to public security and to fundamental interests of the society protected by law which may lead to a criminal offence

rest: GDPR | typically referred to as superior for data protection (quod non, e.g. no indirect exercise of data subject rights) | quid SPOCs? (data re borders, asylum, return …)

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

LED | Data processing | principles

principles

- (a) processed lawfully and fairly (including specification of objectives, data and purposes); (b) collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes (including duty to inform recipient authority of specific conditions); (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; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay; (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed; (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
- no processing by the same or another controller for other purposes unless authorized and necessary and proportionate in accordance with Union or MS law

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

LED | Data processing | further rules

time limits for storage and review

distinction between different categories of data subject (suspects, convicts, victims, other (witnesses, informers, contacts, associate) | quid SPOCS?

distinction facts-/personal assessment-based + info about accuracy-completeness-reliability-up-to-date-ness (cfr Europol 4x4 matrix accuracy information & reliability source) | SPOC compliance?

special categories of data ('sensitive' data): broader conception (inclusive of biometric data); only where authorised by law; subject to 'appropriate safeguards for the rights and freedoms of the data subject'

no automated individual decision-making (including profiling)

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

LED | More

data subjects' rights | SPOC-relevance!

- right to information (general + case-specific & limitations) (Article 13)
- right of access & limitations (Article 14-15)
- right to erasure + restriction & limitations (Article 16)
- related communication duties (Article 12)
- NB: above limitations: provided for by law + indirect exercise through DPA only following refusal

controller & processor: responsible for data protection, including by default & by design (CMS!); mandatory records of all processing activities; logging; cooperation duty with DPA; DPIA obligation, sometimes following prior consultation DPA (cfr European Tracking Solution Europol)

data security, data breach notification to DPA and communication to data subject | SPOC readiness?

data protection officer (DPO) | SPOC level or broader?

independent supervisory authorities

remedies, liability and penalties

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

LED | Transfers 3rd countries & organisations | 1

2016 Roadmap

- (35) Ensure that national good practices regarding cooperation with third countries on counterterrorism are shared between Member States; operational practices can benefit from a clear understanding of current information exchange on terrorists between EU Member States and third countries. This action could include ways in which information received from third countries is entered into the SIS upon request, the use of Interpol diffusions and sharing of watch lists, common risk indicators, also taking the advantage of agreements concluded by Europol with third partners
- 2016 Roadmap (39) | Agreement on how information is shared between PIUs and with third countries where possible

LED

- […] transferred to a controller that is an authority competent for the LED-purposes | quid mixed-purpose tranfers?

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

LED | Transfers 3rd countries & organisations | 2

- principle: Commission adequacy assessment required, or appropriate safeguards
  - (recital 71) Transfers not based on such an adequacy decision should be allowed only where appropriate safeguards have been provided in a legally binding instrument which ensures the protection of personal data or where the controller has assessed all the circumstances surrounding the data transfer and, on the basis of that assessment, considers that appropriate safeguards with regard to the protection of personal data exist. Such legally binding instruments could, for example, be legally binding bilateral agreements which have been concluded by the Member States and implemented in their legal order and which could be enforced by their data subjects, ensuring compliance with data protection requirements and the rights of the data subjects, including the right to obtain effective administrative or judicial redress. The controller should be able to take into account cooperation agreements concluded between Europol or Eurojust and third countries which allow for the exchange of personal data when carrying out the assessment of all the circumstances surrounding the data transfer. The controller should be able to also take into account the fact that the transfer of personal data will be subject to confidentiality obligations and the principle of specificity, ensuring that the data will not be processed for other purposes than for the purposes of the transfer. In addition, the controller should take into account that the personal data will not be used to request, hand down or execute a death penalty or any form of cruel and inhuman treatment. While those conditions could be considered to be appropriate safeguards allowing the transfer of data, the controller should be able to require additional safeguards.
  - (recital 72) Where no adequacy decision or appropriate safeguards exist, a transfer or a category of transfers could take place only in specific situations, if necessary to protect the vital interests of the data subject or another person, or to safeguard legitimate interests of the data subject where the law of the Member State transferring the personal data so provides; for the prevention of an immediate and serious threat to the public security of a Member State or a third country; in an individual case for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or in an individual case for the establishment, exercise or defence of legal claims. Those derogations should be interpreted restrictively and should not allow frequent, massive and structural transfers of personal data, or large-scale transfers of data, but should be limited to data strictly necessary. Such transfers should be documented and should be made available to the supervisory authority on request in order to monitor the lawfulness of the transfer.
- bilateral and multilateral treaties: existing (? Quid Umbrella-like agreements), future treaties

SPOCs and non-EU Interpol NCBs?

- See Article 4 under e) 2015 BE Royal Decree: documented evaluation of the necessity to limit access to data and information in the Interpol information system to certain member states
- See SISII Decision and Recast Regulation (possible direct connection SISII –SLTD and conditionality of an EU-Interpol Agreement following adequacy decision European Commission and where shared data will only be accessible by Interpol members from countries that ensure and adequate level of protection
- LED (recital 25): “Where personal data are transferred from the Union to Interpol, and to countries which have delegated members to Interpol, this Directive, in particular the provisions on international transfers, should apply”

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

ECRIS and ECRIS-TCN

ECRIS

- insert additional information based on criminal records (national databases and ECRIS) with an SIS alert (14.A 2016 Roadmap)
  - even after ESP?
  - quid judicial prerogative criminal records information exchange?

ECRIS-TCN

- COM(2017) 344 final (29 June 2017): Proposal for a regulation (overall compromise text on 12 June 2018, not yet accessible text version): centralized ECRIS-TCN system to identify which MS holds information of TCN, with actual exchange of TCN information through ECRIS (Framework Decision 2009/315/JHA and Decision 2009/316/JHA as amended by the Directive proposed in January 2016), managed by eu-LISA and supervised by EDPS, part of the Interoperability proposals (linked to a ESP, shared biometric matching service and common identity repository) and ETIAS, with access for Europol and Eurojust, also acting as central contact point for 3rd states, as well as for EPPO; also facial images
- quid impact ECRIS-TCN on Article 24.2.a. SIS II Regulation?
- compare with ECRIS and lack of access Europol, national police etc.

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

Non-LED instruments | Punctual issues

Europol 2016 Regulation

- in context of access requests Article 36 (3 month period for Europol to reply, inclusive of consultation with ENU) | rectification-erasure-restriction Article 37: same issue + duty to correct domestically and to inform all parties to which the info concerned has been communicated | SPOC readiness?
- Article 39 new types of processing (prior consultation EDPS) | European Tracking Solution
- (13.C 2016 Roadmap) Examine the possibility for Europol to become a partner in the Prüm framework with a view to enabling the cross matching of DNA, finger prints and vehicle registration data with third countries with which Europol has an operational agreement while fully taking the information owner principle into account (?)
- Upcoming adequacy assessment existing operational agreements 3rd countries & international organisations
- IDMC?

3 SIS II recast Regulations (border checks, return, police/judicial cooperation)

- ready for SISII Return Regulation?
- quid data protection regime re right to access, correction, deletion? (currently: national law; recast: GDPR or national provisions implementing LED; BE: in the mean time?)

Recast Regulation 45/2001 (23 May 2018 agreed in co-decision)

- new lex generalis for LE and judicial agencies, including Eurojust
- Europol & EPPO exempted ony after tough discussions

2 proposed Interoperability Regulations (borders and visa respectively police and judicial cooperation, asylum, migration)

- impact ESP on SPOC functioning?
- inclusive of Article 18.2a cross-referencing data EIS
- 18.2b and c as well in order to establish the Europol IDMC?

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

Q&A

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

www.ircp.org

Contact

Prof. Dr. Gert Vermeulen

t. +32 9 264 69 43
f. +32 9 264 84 94
Gert.Vermeulen@UGent.be

http://www. linkedin.com/in/gert-vermeulen-42b00068

IRCP

Ghent University
Universiteitstraat 4
B – 9000 Ghent

GHENT UNIVERSITY

FACULTY OF LAW AND CRIMINOLOGY

IRCP Institute for International Research on Criminal Policy
Ghent University