Workshop on Data Protection in International Organizations

Co-hosted by the European Data Protection Supervisor and the UN World Food Programme

12 - 13 May 2022
International Data Transfers to IOs: Current Status & Ways Forward

- European Commission
- European External Action Service (EEAS)
- ITU
- European Patent Office

**Moderator:** Policy and Consultation Unit, EDPS
INTERNATIONAL ORGANISATIONS
DATA PROTECTION WORKSHOP
ORGANISED BY WFP – EDPS
12-13 May 2022

Presentation by

European Union
EXTERNAL ACTION

Co-
DPO Network of the European Union Institutions [EUIs]
Intervention held together with
European Commission
Setting the scene: Importance of data transfers to IOs

- EUI’s mandate >> strengthening cooperation
- EUI’s projects
  - aiming at implementation of established standards and practices
  - joint events and training activities
- Involvement of IOs >> exchange of data

Examples from various EUIs:

- Transfers of personal data carried out to establish cooperation arrangements with third-country (banking) supervisory authorities for more efficient supervision of internationally active financial groups
- Exchanges of personal data between EUI and IO to increase cooperation between financial supervisory authorities for the stability of the financial system
- EUI–IO colocation agreement - IO hosted by EUI
- Joint platform EUI-IO with information regarding young university graduates accessing to paid traineeships at either the EUI or the IO
EUI specificities and objectives

- EU – an supra-national/international organisation – similar status with IOs
  >> aware of the issues concerning privileges and immunities
- EUIs need tools to cooperate with IOs

Objectives of „the Tool“

- Enabling good cooperation and joint actions to fulfil the mandate of IOs and EUIs
- Allowing exchange of personal data between IOs and EUIs safely and smoothly
- Enabling a rapid but reliable authorisation procedure
- Agreeing on measures which can be implemented in practice

Objectives in working out „the Tool“

- Having all stakeholders on board
- Understanding the different legal frameworks of IOs and EUIs

Addressing the challenges

- Initiative to elaborate an appropriate tool
INTERNATIONAL TRANSFER (ITR) WORKING GROUP OF DPOs of European Institutions (EUs)

Members: DPOs of EEAS, EUIPO, EC, F4E, EMA, SRB, EFSA, FRONTEX, ECA
Observers: DPOs Court of Justice, EACEA

DPO NETWORK INITIATIVE

With the objective of looking for an instrument
- EUI DPOs ITR WORKING GROUP sharing views and best practices among WG members
- Emphasis on the cooperation with our supervisor and the European Commission

TOOL << mechanism provided under our DP framework
Considering the importance and features of the cooperation with various IOs

Useful instrument
= Template to be used by EUIs for different types of cooperation

PROCESS
Elaboration of the tool - in close cooperation with the EC and the EDPS and with strong involvement of IOs = future guarantee for a work-in-practice solution

TIMELINE

<table>
<thead>
<tr>
<th>Year</th>
<th>Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019</td>
<td>Concept, Elaboration, Submission of draft AA to EDPS &amp; Review meeting with EDPS</td>
</tr>
<tr>
<td>2020</td>
<td>Submission of revised AA to EDPS w/EDPS guidelines &amp; EDPS recommendations</td>
</tr>
<tr>
<td>2021</td>
<td>IO - EDPS Transfer TASK FORCE Workshop Meeting Exchange/IO comments</td>
</tr>
<tr>
<td>2022</td>
<td>Revised AA taking into account IOs and EDPS standpoints</td>
</tr>
</tbody>
</table>
STATE-OF-PLAY

OUTPUT: MODEL AA for IOs

Draft administrative arrangement for the transfer of personal data between
Name of EU institution/body or agency

AND

Name of International Organization


ONGOING WORK

- Draft shared with ITR Task Force
- Detailed comments from several IOs

WG - working on a revised draft, taking into account written comments received and Task Force discussions

FUTURE PROSPECT

- Revised version – to be shared
- Changes addressing the complex topics, critical points
- Further round of exchange with IOs

Administrative Arrangement for the transfer of personal data between EUi and IOs
(REVISIED VERSION)

Subject-matter and Scope Definitions

Personal Data Protection Safeguards
1. Purpose limitation
2. Transparency
3. Data quality and proportionality
4. Storage limitation
5. Integrity and confidentiality
6. Onward transfers

subject rights and oversight

Implementation, revision and termination
Information about the parties, transfers, etc.
We took into account

- The requirements for EUIs under EU law
- Legal and regulatory framework (in particular immunities and supervisory structures) of IOs

RESULT - OUTPUT

Formal side
- One set of clauses
- Rapid approval procedure > „Fast track authorisation”
- Commitment on the side of stakeholders

Content side
- Core-data data protection safeguards and individual rights
- Acknowledgement of different legal frameworks
- Oversight and redress mechanisms
Examples of critical points and proposed solutions in revised draft

- References to applicable legal framework
- Purpose limitation
- Transparency

- Onward transfers
- Oversight and redress
Proposed solution – Applicable Legal Framework

- Clarification in the revised AA that each party is subject to its own data protection framework
- Parties to confirm that the relevant data protection safeguards, rights and obligations are provided in their legal frameworks

For EUIs:
EU data protection law

For IOs:
applicable data protection framework (based on founding documents, internal rules, etc.)

Other general references to EU legal framework have been removed (e.g. no longer reference to EU rules for definitions, but definitions to be agreed by the Parties)

Purpose limitation
- Purposes to be included in the AA, possibility to include compatible purposes, such as archiving/scientific research or internal audits/investigations

Transparency
- Both parties’ responsibility; aim at avoiding unreasonable administrative burden
Proposed solution – Onward transfers

**IOs concerns**
- Prior and express authorisation: the consent of the other party might limit the neutrality and independence of the IO
- Possibility for EDPS to request information from a receiving party in case of onward transfer might raise issues jeopardising international organisations immunity
- Concept of public interest

**Proposed solution**
- Information on intended onward transfers to be provided in annex
- Focus on guaranteeing continuity of protection
- With possibility for exceptions in specific situations (e.g. in the interest of/to protect the individual, necessity to fulfil official mandate for important reasons of public interest)
**Proposed solution – Independent oversight and redress**

**IOs concerns**

- The supervisory authorities of most IOs are not “established by law”, but by their own statutes or even by internal regulations or rules
- IOs have their own internal redress bodies with exclusive competence & binding decisions
- No external supervisory authority should be responsible for monitoring the processing of personal data processed by IOs
- Monetary compensation for damages not foreseen

**Proposed solution**

✓ No requirement for supervision by external body (such as national data protection authority) or for redress before (national) judicial fora (courts)
✓ Possibility to rely on independent mechanisms that exist within IOs – functionally independent/autonomous, powers to investigate and take binding remedial measures
✓ Other alternatives also possible, e.g. arbitration to provide redress
Privacy Risk Management in International Organizations

- WFP
- The World Bank
- Interpol
- UNHCR

Moderator: IFRC
Key topics

1. CURRENT STATUS
2. WHAT ARE WE DOING
3. OUR AMBITION
AN APPROACH TO RISK MANAGEMENT
An holistic approach to Risk Management:

2 DIFFERENT TYPES OF RISK MANAGEMENT

- VS THE ORGANIZATION-
- VS FFRR AND FREEDOMS OF AN INDIVIDUAL: harm to the rights and freedoms that a processing operation may cause to data subjects.

Risk management: set of ordered and systematised actions with the purpose of controlling the possible (likelihood) consequences (impacts) that an activity may have on a set of goods or elements (assets) to be protected
A holistic approach to Risk Management:

1. Current Status

- Governance in place: Toolkit
- Accountability on specific function.

Privacy Impact Assessment

What is a PIA and available tools

- What is a PIA?
- Data Protection Toolkit - Toolkit to operationalise beneficiaries’ personal data protection
- Data Protection Toolkit - Toolkit to operationalise beneficiaries’ personal data protection (ES)
- Data Protection Toolkit - Toolkit to operationalise beneficiaries’ personal data protection (FR)
A holistic approach to Risk Management:

1. Current Status

Global Privacy Office
A holistic approach to Risk Management:

1. Current Status

**CHALLENGES**

- Reactive exercise
- Focused on Beneficiaries
- Lack of capacity
- Lengthy process
- Down to top
- Time consuming
- Lack of effective control and follow up
- Lack of holistic risk visibility

**OPPORTUNITIES**

- Proactive
- Focused on all impacted domains
- Streamline capacity
- Shorter process
- Top-down exercise
- Consistent application
- World risk map
- Accountability
- Consistent approach to risk management
An wholistic approach to Risk Management:

2. What are we doing

- Automation through dedicated software
  - PIA & Register of processing

- Embedding specific controls
  - TEC Procurement process
  - Due Diligence Process for Private partnerships

- Creating ad hoc solutions
  - Data Protection Kit for Emergencies
  - Contract templates

"Business as usual until we have something better to offer"
A holistic approach to Risk Management

3. Our ambition: where do we want to go

- Integrated Risk matrix
- Automated Accountability
- World Risk map
- Prove of concept: Governance
- Integrated risk management within the rest of risk management processes of the organization
Thank you!
Data Privacy at the World Bank

2022 Data Protection Workshop for International Organisations

Presented by [Redacted]

World Bank
Personal Data Privacy Compliance

- World Bank Group Policy on Personal Data Privacy
  - Seven high level principles applied on a risk-based approach that govern the use of all personal data
  - Accountable to Data Subjects via:
    - Requests for Information
    - Calls for Review
- Decentralized implementation along three lines of defense:
  - Business Units
  - DPO
  - GIA
Accountability and Privacy Management Operations

subhead about Q3 growth and cumulative growth comparison goes here
Training, Awareness and Engagement

subhead about the Q3 growth and cumulative growth comparison goes here

- Learning Events (roundtables, open office hours, speaking engagements, etc.)
  - Cumulative +139
- Website Engagement
  - For internal and external websites.
  - Cumulative +11,406
- Privacy Training Sessions
  - Ongoing digitization of paper records
- Focal Point Interactions (onboarding, training, T1s, etc.)
  - Cumulative +173
- Q3 growth +23
- Q3 growth +5,014
- Q3 growth +14
- Q3 growth +65
Thank you.

Questions and Comments?

Email: Privacy@worldbank.org
INTERPOL
Privacy Risk Management in International Organizations

12-13 May 2022, DP workshop co-hosted by the EDPS and WFP
INTERPOL’s MANDATE:

"To ensure and promote the widest possible mutual assistance between all criminal police authorities within the limits of the laws existing in the different countries and in the spirit of the “Universal Declaration of Human Rights”"

Art.2 Constitution
Resolution on "Privacy of Information" - INTERPOL General Assembly 1974

RESOLUTION No. AGO/44/RES/1

TO BE CLASSIFIED AS FOLLOWS:
1 copy in the CHRONOLOGICAL SERIES:
year 1974
1 copy in the SUBJECT SERIES:
Readings: General rules governing international co-operation between police departments or agencies carrying out police duties.
1 copy in the SUBJECT SERIES:
Readings: Human Rights - Protection of privacy.

TEXT OF RESOLUTION

NOTING the concern of many countries with the privacy of the individual with regard to criminal justice information;

NOTING, in addition, that the development of international crime requires an exchange of information on an international basis;

The INTERPOL General Assembly, meeting in Cannes from 19th to 25th September 1974 at its 43rd session:

URGES that in exchanging information the INTERPOL NCIs and the general secretariats take into account the privacy of the individual and strictly confine the availability of the information to official law enforcement and criminal justice agencies.
40 years of data protection at INTERPOL

- **1982**: Decision to create the Commission for the Control of INTERPOL’s Files (CCF)
- **1984**: Adoption of the Rules on International Police Cooperation and on Internal Control of INTERPOL’s Archives
- **1987**: Rules on the Deletion of Police Information Held by the General Secretariat
- **1990**: Rules Governing the Database of Selected Information and Direct Access by National Central Bureaus to that Database
- **2001**: Rules Governing Access by an Intergovernmental Organization to the INTERPOL Telecommunications Network and Databases
- **2003**: Rules on the Processing of Information for the Purposes of International Police Cooperation
- **2005**: Rules on the Control of Information and Access to INTERPOL’s Files
- **2007**: Implementing Rules for the Rules on the Processing of Information for the Purposes of International Police Cooperation
- **2012**: INTERPOL’s Rules on the Processing of Data (RPD)
- **2014**: Amendments to the RPD
- **2016**: New statute of the CCF
- **2018**: Amendments to the RPD
- **2019**: Working group tasked by the General Assembly to review the RPD
- **2021**: Decision processing personal data for administrative purposes
From legal framework to effective management and implementation.
UNHCR
Data Protection and Privacy Risk Management: UNHCR example

May 2022
Overview: UNHCR Context

- Privacy and Data protection = protection of refugees and other forcibly displaced
- Data maturity in the organization and risk appetite across very diverse contexts across the globe
- Balance between UNHCR’s mandate and functions and the fundamental rights and freedoms of data subjects in relation to processing of their personal data.
- Driven by 7 years of implementation of UNHCR’s Policy on the Protection of Personal Data of Persons of Concern, revision is underway, and will change the policy landscape and governance and accountability framework.
- Approach: integration of data protection and privacy risk management into existing organization design, driven by enabling the refugee/ forcibly displaced individual/ stateless to have agency over his/ her data.

1. Governance
2. Technical considerations
3. Risk management
1. Governance
(integration of data protection and privacy risks into the existing Governance framework and Enterprise Risk Management instruments)

- Takes decisions in respect of strategic and annual planning
- Resource allocation within the region, based inter alia on risks in relation to (personal) data
- Identifies, prioritizes and integrates into multi-year strategy risks associated with data protection and privacy, along other operational risks.

- Identifies data as a strategic asset and establishes data privacy and protection as an opportunity to demonstrate the paramount nature of data subjects’ rights
- Acts as “second line of defence” in supporting managing the risks at the operational level.
- Identifies risks associated with data protection and privacy, along other operational risks.
2. Technical considerations
Expanding reliance on technology as impact of COVID19 pandemic

• Example: data security and data protection risk-based guidance

Authorized Tools for Online Communication and Document Exchange with Persons of Concern

- Secure 1-1 Communications
  - Signal
  - WhatsApp (*)
- Pre-registration/Verification interviews with PoC
  - [communication with more than 2 (1-1) parties]
  - [collection of limited personal data elements]
  - Signal (if only mobile phone)
  - WebEx (if all participants have email)
  - MS Teams (I) (if all participants have email)
  - WhatsApp (*)

Authorized Tools for Online Communication and Document Exchange with PoCs

- Sensitive Registration/Case Management Interviews with PoCs
  - [Communication with more than 2 (1-1) parties]
  - Signal (if only mobile phone)
  - WebEx (if all participants have email)
  - MS Teams (I) (if all participants have email)

- Sharing Documents with PoCs
  - SFS (if all parties have email)
  - Signal (if only mobile phone)
  - WhatsApp (I) (if only mobile phone)

Explanatory Notes:
(*) = WhatsApp is a permissible alternative to Signal if necessary to communicate with an existing user of WhatsApp, and risk is accepted by the Data Controller.

SFS = Secure File Sharing platform for one-way sharing of files from UNHCR to a third party. The platform requires sharing a hyperlink to the PoC via email.

MS Teams (I) = Corporate tool that supports communication with external party(ies). However, participants’ email addresses cannot be hidden.

Signal = Recommended standard for secure communication. Since Dec 2020, Signal supports both audio and video (limited to 5 participants) group calls.

• Operational needs
• Preferences of Data subject (refugees and other forcibly displaced)
• Risk-based considerations
3. Context, risk appetite and resource allocation (Example of life-saving emergencies)

Balance between UNHCR’s mandate and functions and the fundamental rights and freedoms of data subjects in relation to processing of their personal data:

- Humanitarian emergencies and need for life-saving assistance: Ukraine, Afghanistan, Ethiopia, Mozambique, Cameroon
- **Context-driven** (presence of lawful authorities, Govt’s policy, national legislation, partner/NGOs presence and ability to deliver services)
- **Sensitive** personal data processing (e.g. biometrics, details of circumstances of flight, etc)

Rapid risk assessment

- Security
- Protection of refugees/ forcibly displaced
- Data protection and privacy
- InfoSec
- Reputational
- Financial
Digital Transformation and Data Protection: An Oxymoron?

- European Commission
- Maastricht University
- EDPS

Moderator: WFP
European Commission
Data protection aspects in Blockchains

European Commission
EU 'gold standard' for blockchain:

- Environmental sustainability
- Data protection
- Digital Identity
- Cybersecurity
- Interoperability
Global blockchain market share by sector

Data protection

• Does data envisaged to be on the blockchain contain personal data?
• Principles of fairness, lawfulness, transparency, purpose limitation, data minimization, accuracy, storage limitation
• “Miners” and the concepts of controller, joint controller and processor
• Data subject rights
Digital Transformation and Data Protection: an Oxymoron?
The challenges of cloud

EDPS - WFP Conference on Data Protection within International Organisations
12-13 May 2022

(Supervision and Enforcement Unit at the EDPS)
WHERE ARE THE CHALLENGES?

- IO: Your regulatory framework, privileges & immunities, tasks
- PROCESSING: Processing itself, control
- REQUIREMENTS: Your needs, legal, technical requirements
- CLOUD SERVICES: Different service models, capabilities
- PROVIDER: Provider itself, subcontractors, general practices, legal obligations
- PROCUREMENT: Organisation, selection
- SAFEGUARDS: Contract & other measures, checks & audits
WHAT ARE THE CHALLENGES and how to approach them?

- **WHO ARE YOU, WHAT DO YOU DO, WHY DO YOU DO IT** – Know yourself
- **WHAT DO YOU WANT** – Know enough from the start about your use case
- **WHO DOES WHAT** – Clarify roles and responsibilities
- **WHO IS ACCOUNTABLE** – Take informed decisions to be in control
- **HOW TO GO TO CLOUD** – Have a comprehensive data protection strategy
WHAT ARE THE CHALLENGES and how to approach them?

➢ WHAT ARE YOU GETTING INTO – Carry out risk assessments

➢ WHEN & WHERE TO INCLUDE DATA PROTECTION –
  Embed data protection principles and safeguards in procurement, processing & all that supports it

➢ HOW TO SELECT THE RIGHT SERVICE & PROVIDER – Impose requirements during procurement

➢ HOW TO GET THE RIGHT TERMS & CONDITIONS – Be in control, get informed & take action
WHAT CAN GO WRONG?

- your data may be processed for further incompatible purposes
- your data will end up in unknown locations, with unknown sub-processors
- security of processing compromised
- onward transfers to further third parties
- unauthorized access – including foreign public authorities
- unilateral amendments – applicable law, substantial conditions change
- other law, foreign jurisdiction applicable – not providing for equivalent level of protection for people as you would under your rules
- unauthorized access to your premises, access to confidential data

You are responsible for the processing
Petra Candellier
Head of Complaints and Litigation, Supervision & Enforcement, EDPS