

Workshop on Data Protection in International Organizations

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

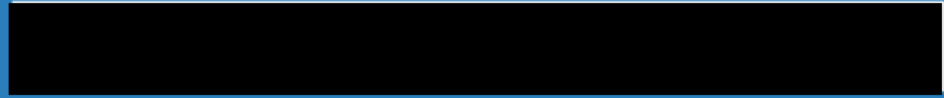
12 – 13 May 2022



International Data Transfers to IOs: Current Status & Ways Forward

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

Moderator: [REDACTED] Policy and
Consultation Unit, EDPS



EEAS

INTERNATIONAL ORGANISATIONS DATA PROTECTION WORKSHOP ORGANISED BY WFP – EDPS

12-13 May 2022

Presentation by [REDACTED]

[REDACTED]



[REDACTED]

Co [REDACTED]



DPO Network of the European Union Institutions [EUIs]

Intervention held together with [REDACTED]

European Commission  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 (EUIs)

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

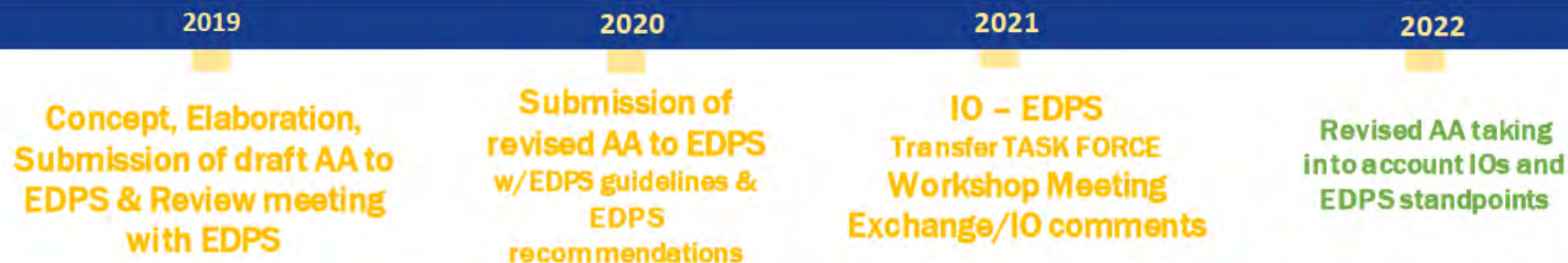
Useful instrument

= 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



OUTPUT: MODEL AA for IOs

Draft administrative arrangement for the transfer of personal data between

Name of EU institution/body/office/agency

AND
Name of International Organisation

Hereinafter individually referred to as 'the Party' or collectively as 'the Parties',

acting in good faith, will apply the safeguards specified in this administrative arrangement ('Administrative Arrangement' or 'AA') to the transfer of personal data between them,

recognizing the importance of the protection of personal data and of having robust protection regimes in place,

having regard to Article 46(3) (b) of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the 'General Data Protection Regulation' or 'GDPR')¹,

having regard to Article 4(3) (b) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Regulation 2018/1725)²,

having regard to the relevant guidelines for the protection of personal data issued by the European Data Protection Board and the European Data Protection Supervisor ('EDPS') in the case of the European institutions, bodies and agencies,

having regard to the need to process personal data to carry out the public mandate and exercise of official authority vested in the Parties, and

having regard to the need to ensure efficient international cooperation between the Parties acting in accordance with their mandates as defined by applicable laws to safeguard individuals, whose data are processed and transferred in the framework of the cooperation between the Parties,

for the purpose of Article 46(3) of Regulation (EU) 2016/679,

and having reached the following understanding:

WHEREAS:

1. The EU institution/body/office/agency _____ (_____) is the EU institution/body/office/agency responsible for the _____
2. The _____ Organisation is an intergovernmental organisation set up pursuant to _____ and responsible for _____
3. Both the EU institution/body/office/agency _____ and _____ the Organisation _____ are _____ in charge of administering _____, managing _____ and mandated to cooperate to fulfil the said task(s);
4. The EU institution/body/office/agency _____ and the Organisation _____ signed in _____ a Memorandum of Understanding (MoU) that establishes the terms and conditions under which they configured mechanisms for mutual cooperation in areas they consider to be a priority;
5. The EU institution/body/office/agency _____ and the Organisation _____ currently cooperate closely in a number of projects and activities, which include _____ and exchange of _____ best practices the main cooperation objective of which is to promote _____
6. The EU institution/body/office/agency _____ and Organisation's _____ respective institutional activities encompass within their scope _____. This objective is carried out through cooperation activities governed _____

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 (REVISED VERSION)

Article 1	Subject-matter and Scope
Article 2	Definitions
Article 3	Personal Data Protection Safeguards <ol style="list-style-type: none">1. Purpose limitation2. Transparency3. Data quality and proportionality4. Storage limitation5. Integrity and confidentiality6. Onward transfers
Article 4	Subject rights and
Article 5	oversight
Article 6	Implementation, revision and termination
Annexes	Information about the parties, transfers, etc.

We took into account

- **The requirements for EIUs 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)**

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**

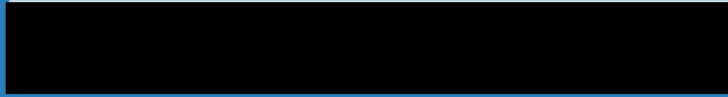
Proposed solution

- ✓ **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

- [REDACTED], WFP
- [REDACTED] The World Bank
- [REDACTED], Interpol
- [REDACTED], UNHCR

Moderator: [REDACTED], IFRC



WFP



World Food Programme

SAVING
LIVES
CHANGING
LIVES



Key topics



1. CURRENT STATUS
2. WHAT ARE WE DOING
3. OUR AMBITION



Global Privacy Office / OED

AN APPROACH TO RISK MANAGEMENT

MAY 2022



World Food Programme

**SAVING
LIVES
CHANGING
LIVES**



World Food Programme

SAVING
LIVES
CHANGING
LIVES

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

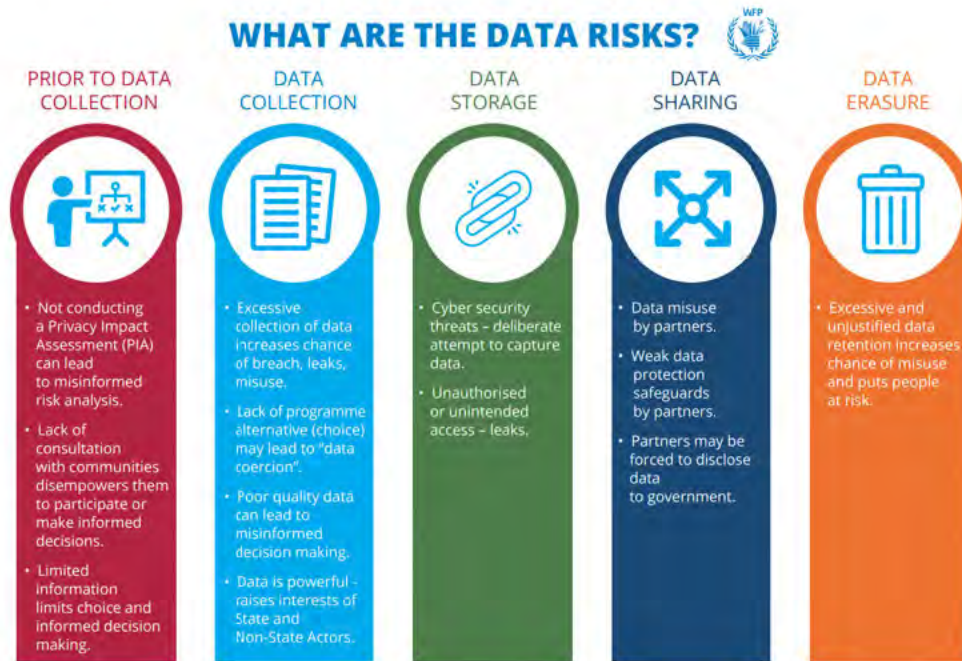


World Food Programme

SAVING
LIVES
CHANGING
LIVES

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) [↗](#)



World Food Programme

SAVING LIVES
CHANGING LIVES

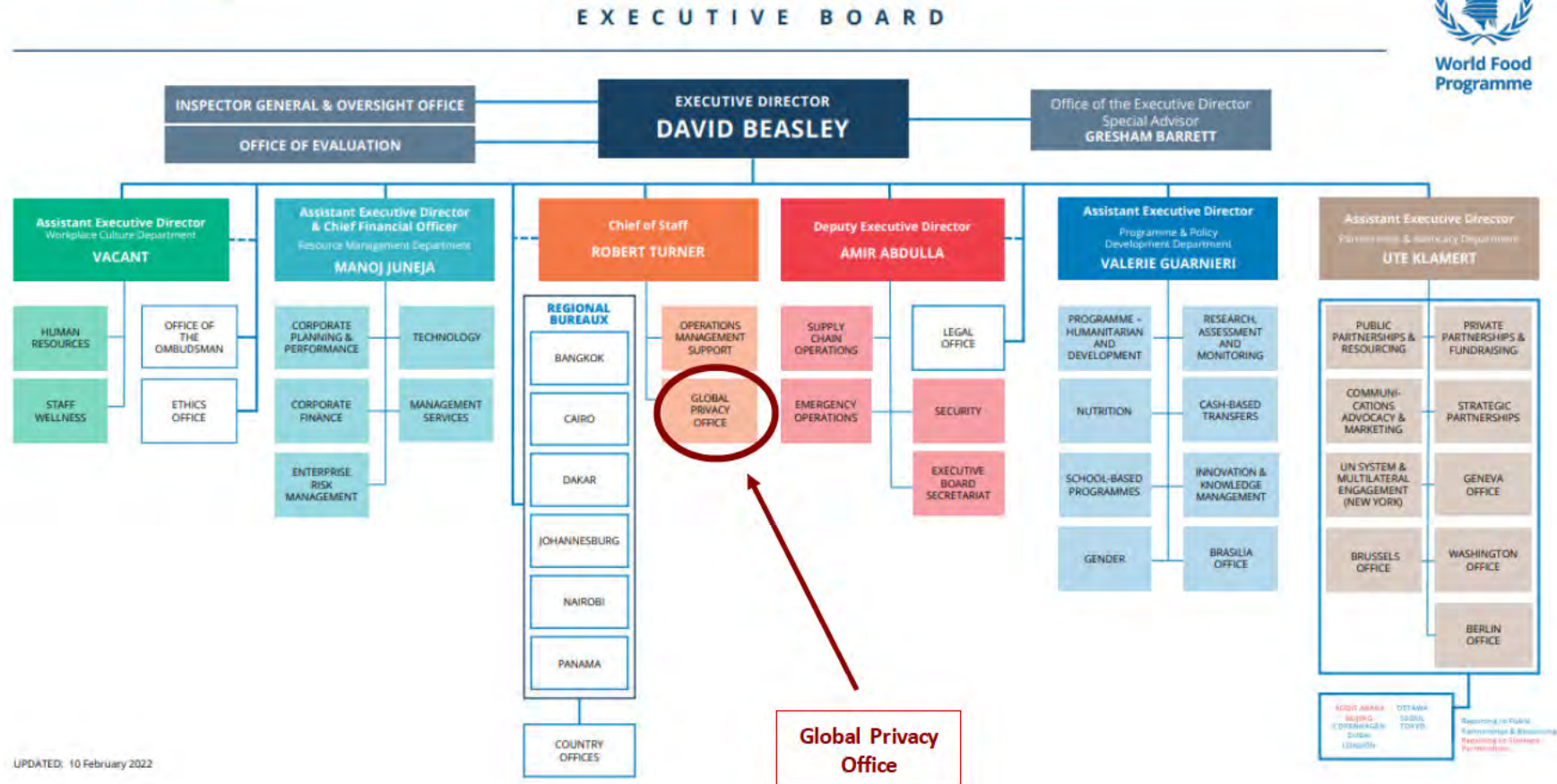
A holistic approach to Risk Management:

1. Current Status

WFP Organigram



World Food Programme



UPDATED: 10 February 2022



World Food Programme

SAVING
LIVES
CHANGING
LIVES

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

AUTOMATION

OPORTUNITIES

- Proactive
- Focused on all impacted d.
- Streamline capacity
- Shorter process
- Top-down exercise
- Consistent application
- World risk map
- Accountability
- Consistent approach to risk management



World Food Programme

An wholistic approach to Risk Management:

2. What are we doing



*“ Business as usual
until we have something
better to offer”*

- **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

SAVING
LIVES
CHANGING
LIVES



World Food
Programme

SAVING
LIVES
CHANGING
LIVES

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



World Food
Programme

Thank you!



SAVING
LIVES
CHANGING
LIVES



World Bank

Data Privacy at the World Bank

2022 Data Protection Workshop for International Organisations

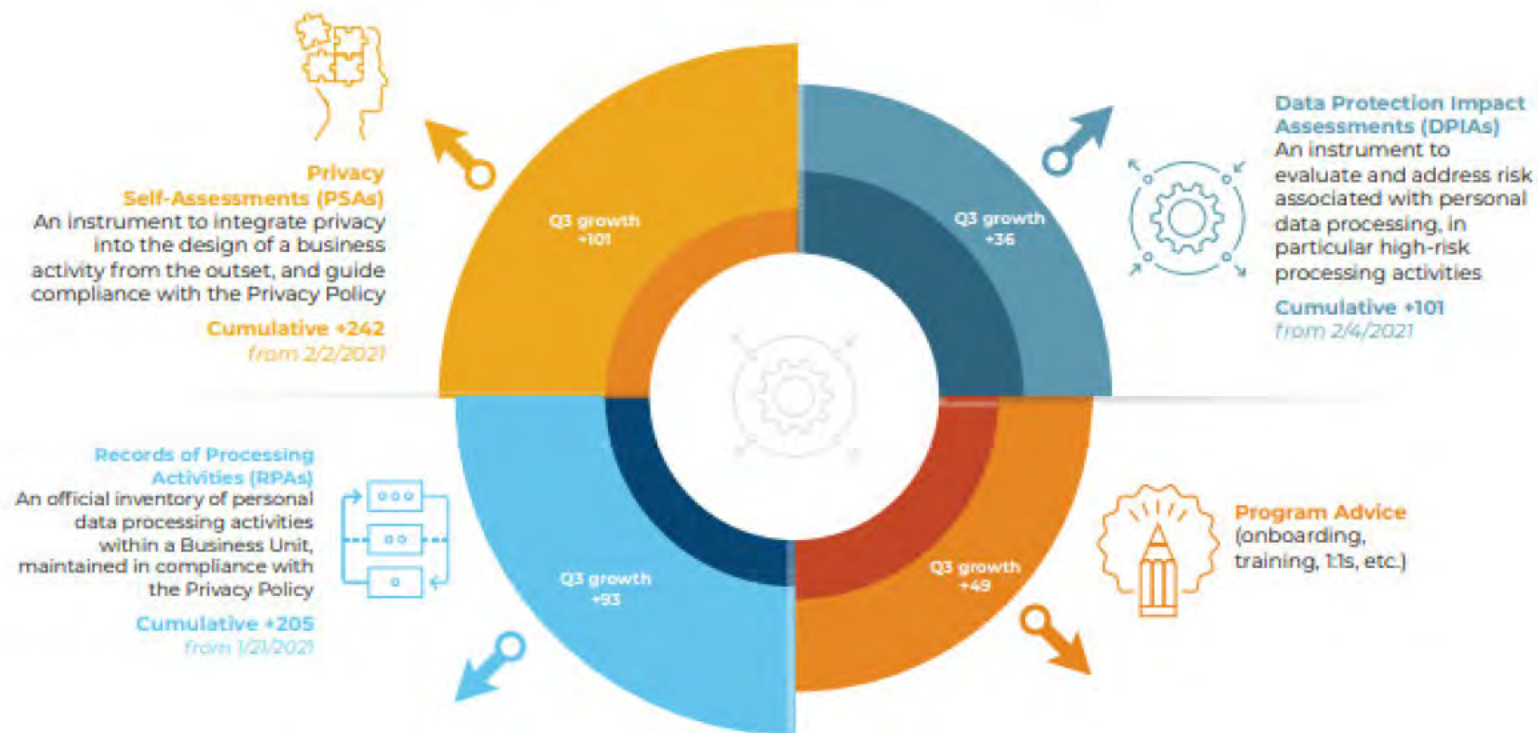
Presented by [REDACTED]
[REDACTED]
[REDACTED] World Bank

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



Thank you.

Questions and Comments?

Email: Privacy@worldbank.org



INTERPOL



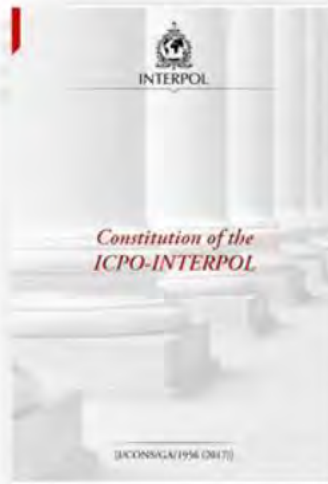
Privacy Risk Management in International Organizations

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



THE UNIVERSAL DECLARATION OF HUMAN RIGHTS

Adopted by the General Assembly of the United Nations in 1948, the Universal Declaration states fundamental rights and freedoms to which all human beings are entitled.

We are all born free and equal.
Everyone is entitled to these rights no matter your race, religion, sex, language, or nationality.
Everyone has the right to life, freedom, and safety.
No one can take away any of your rights.

1 No one has the right to hold you in slavery.

2 No one has the right to torture you.

3 You have a right to be recognized everywhere as a person before the law.

4 We are all equal before the law and are entitled to equal protection of the law.

5 You have the right to seek legal help if your rights are violated.

6 No one has the right to wrongly imprison you or force you to leave your country.

7 You have a right to a fair public trial.

8 Everyone is innocent until proven guilty.

9 You have the right to privacy. No one can interfere with your reputation, family, home, or correspondence.

10 You have the right to travel.

11 You have the right to seek asylum in another country if you are persecuted in your own.

12 Everyone has the right to a nationality.

13 All consenting adults have the right to marry and to start a family.

14 You have the right to own property.

15 Everyone has the right to belong to a religion.

16 You have the right to think and voice your opinions freely.

17 Everyone has the right to gather as a peaceful assembly.

18 You have the right to participate in the governance of your country, either directly or by helping to choose representatives in free and genuine elections.

19 You have the right to social security and are entitled to economic, social, and cultural help from your government.

20 Every adult has the right to a job, a fair wage, and membership in a trade union.

21 You have the right to leisure and rest from work.

22 Everyone has the right to an adequate standard of living for themselves and their family.

23 Everyone has the right to an education.

24 Everyone has the right to freely participate in the culture and scientific advancement of their community, and their intellectual property as artist or scientist should be protected.

25 We are all entitled to a social order in which we may enjoy these rights.

26 Everyone's rights and freedoms should be protected unless they choose; the rights and freedoms of others.

27 No State, group, or person can use this Declaration to deny the rights and freedoms of others.

This is a simplified version of the UDHR. For the complete text, visit www.un.org

Resolution on “ Privacy of Information” - INTERPOL General Assembly 1974

<p>RESOLUTION No. AGN/43/RES/1</p> <p><u>SUBJECT:</u></p> <p>PRIVACY OF INFORMATION</p>	<p>TO BE CLASSIFIED AS FOLLOWS:</p> <p>1 copy in the CHRONOLOGICAL SERIES: year 1974</p> <p>1 copy in the SUBJECT SERIES:</p> <p>Heading: General rules governing international co-operation between police departments or agencies carrying out police duties.</p> <p>1 copy in the SUBJECT SERIES:</p> <p>Heading: Human Rights - Protection of privacy.</p>
---	--

TEXT OF RESOLUTION

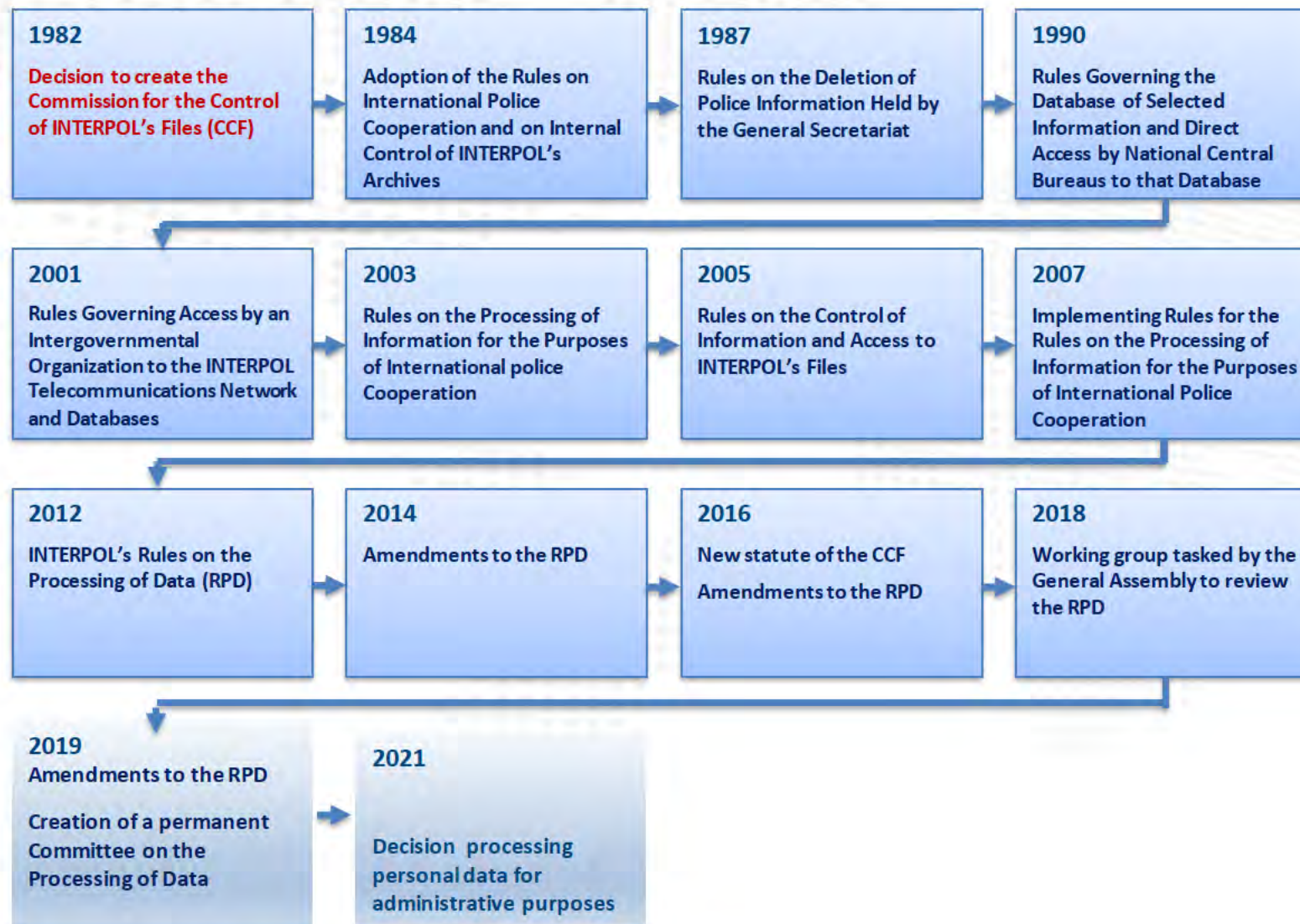
NOTING the concern of many countries with the privacy of the individual with regard to criminal justice information;

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

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

URGES that in exchanging information the ICPO-INTERPOL NCBs and the General Secretariat 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





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

UNHCR Summary:

- Operations in 166 countries
- 100 mln persons in need
- 20 mln persons in UNHCR registry
- 20,000 employees
- US\$ 9 billion budget in 2021



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.



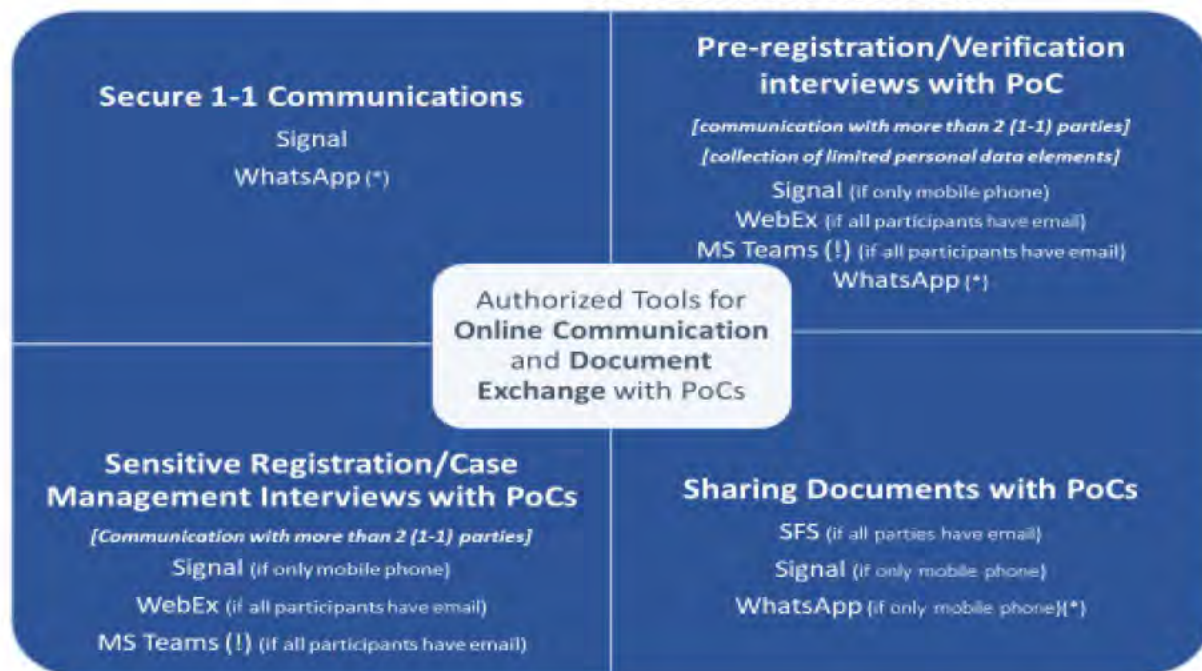
- Identifies **data as a strategic asset** and establishes data privacy and protection as an opportunity to demonstrate the paramount nature of **data subjects' rights**
- Acts as “second line of defence” in supporting managing the risks at the operational level.
- Identifies risks associated with data 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



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 (!) – Corporate tool that supports communication with external party(ies). However, participants' email addresses cannot be hidden.

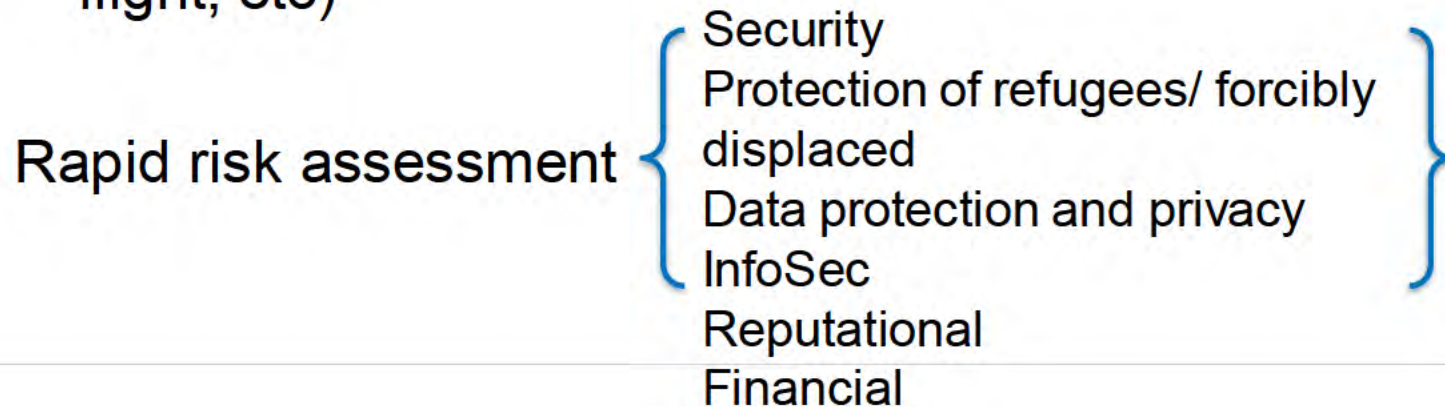
Signal – [Recommended](#) standard for secure communication. Since Dec 2020, Signal supports both audio and video (limited to 5 participants) group calls.

- 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)



Digital Transformation and Data Protection: An Oxymoron?

- [REDACTED]
- [REDACTED] European Commission
- [REDACTED] Maastricht University
- [REDACTED], EDPS

Moderator: [REDACTED], WFP





European Commission

Data protection aspects in Blockchains

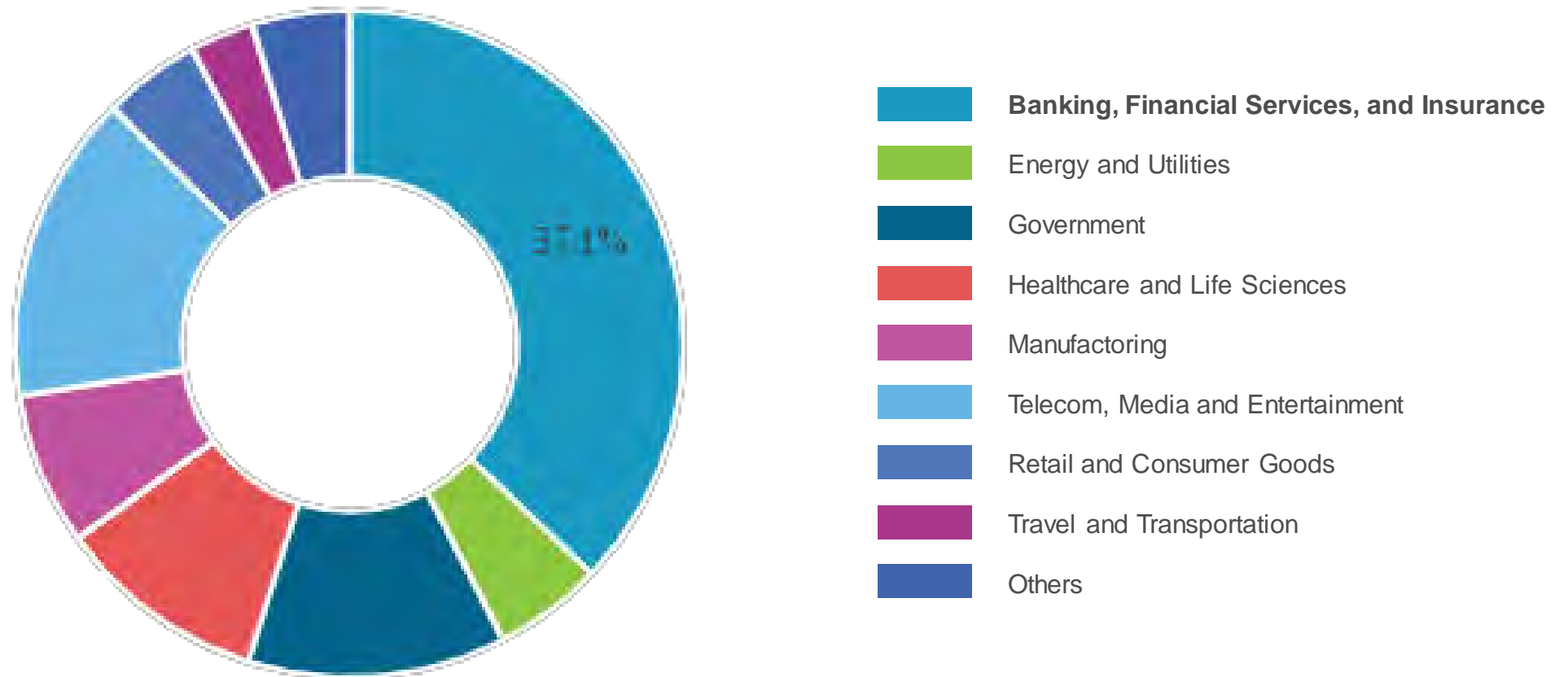


European Commission

EU 'gold standard' for blockchain:

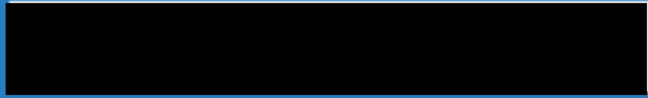
- Environmental sustainability
- Data protection
- Digital Identity
- Cybersecurity
- Interoperability

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



EDPS




Digital Transformation and Data Protection: an Oxymoron?

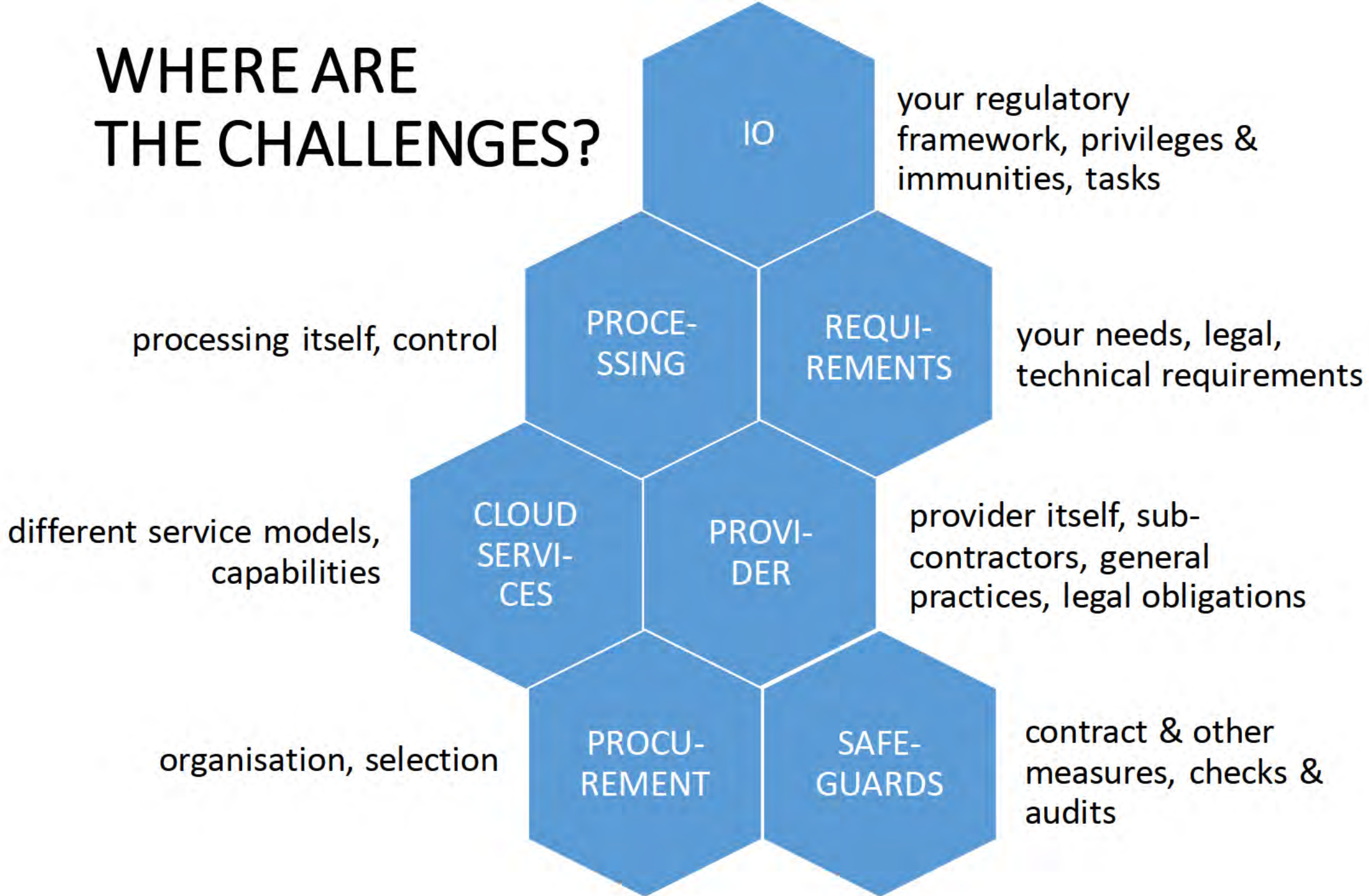
The challenges of cloud

EDPS - WFP Conference on Data Protection within International
Organisations

12-13 May 2022


 (Supervision and
Enforcement Unit at the EDPS)

WHERE ARE THE CHALLENGES?



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



CLOSING REMARKS

[Redacted]

[Redacted]



CLOSING REMARKS

Petra Candellier

Head of Complaints and Litigation, Supervision & Enforcement,
EDPS