From: [redacted]

To: [redacted]

CC: [redacted]

Sent at: 02/06/17 15:40:48

Subject: Draft message with the final minutes of the Data protection Workshop

Dear ladies,

We hope everything is going well.
We have prepared a draft message to be sent to all the participants with the minutes that were finalized.

Could you please check the draft of the message and provide your comments if any by Tuesday?

"Dear colleagues,

We would like to thank you for your comments provided to the minutes of the 6th workshop on Data Protection within International Organisations, which took place on 11–12 May at the International Organization for Migration in Geneva. Attached you will find the final version of the minutes of the workshop.

We would like once again to thank you for your participation, your comprehensive contribution to the workshop and we are looking forward to further editions of the workshop.

Sincerely,

Johan Rautenbach, Legal Counsel, International Organization for Migration
Giovanni Buttarelli, European Data Protection Supervisor "

Attached you will see the final version of the minutes to be send on Tuesday.

Thank you and best regards,
[redacted]

[redacted]
Office of the Legal Counsel (LEGLC)
Office of Legal Affairs
International Organization for Migration
17, route des Morillons
P.O. Box 17
CH-1211 Geneva 19, Switzerland
www.iom.int

DATA PROTECTION WITHIN INTERNATIONAL ORGANISATIONS

WORKSHOP
11 – 12 May 2017
IOM 1st floor Conference Room, 17, Route des Morillons, Geneva, Switzerland

SUMMARY

The 6th Workshop on Data Protection within International Organisations, co-hosted by the European Data Protection Supervisor (EDPS) and the International Organization for Migration (IOM), took place in Geneva at the IOM headquarters, on 11 and 12 May 2017.

35 entities, most of them international organisations (IOs), were represented at the event and 77 individual participants, including several newcomers, attended the one-and-a-half-day workshop.

The main topics of discussion were the state of play of data protection policies and their implementation within International Organizations, data protection issues in cloud computing, current practices and challenges of processing health data, the developments in the privacy/ data protection regulatory and policy environment, mainly the EU General Data Protection Regulation (GDPR), including the issue of transfer of personal data to International Organizations.

DAY ONE

Opening remarks – Welcome by IOM and EDPS

Ambassador Laura Thompson, Deputy Director General, IOM

- It is a pleasure for the IOM to co-host this event on data protection. Safeguarding the personal data of individuals, particularly in vulnerable situations, is an essential aspect of the right to privacy which applies to all humans, including migrants. Processing data of migrants is an essential part of IOMs work to fulfil its mandate; the privacy and confidentiality of IOM beneficiaries are of fundamental importance for the IOM.
  IOM applies its internal Data Protection Principles of 2009 when processing personal data of its beneficiaries. Those principles prevent unnecessary and disproportionate interference with the right to privacy.

Giovanni Buttarelli, European Data Protection Supervisor

- The EDPS is glad to support a forum aiming at bringing together international organisations to exchange their experiences and best practices in the field of data protection. It is also an opportunity to share recent developments and discuss current challenges, such as the impact of new technologies for dignity and individual freedom as well as possible solutions.
- Because they are on the front line of the challenges and uncertainty of globalization, international organizations are expected to show leadership in improving data protection standards, and they demonstrated that they do. In particular, the role of DPOs is an essential sign of proactivity of International Organisations in the field of data protection and accountability.
- Since the last workshop in 2015, a “game changer” has happened through the adoption of the GDPR after 3 years of difficult negotiations. The GDPR includes a legal innovation

as compliance with the GDPR has to be clearly demonstrated by data controllers falling under the scope of application.

MORNING SESSION

Session 1: Presentations from Organizations on recent developments

Moderator: Johan Rautenbach, Legal Counsel, IOM

Michela Bonsignorio, Advisor on Protection and Accountability to Affected Populations, Emergency and Transition Unit and DPO a.i., World Food Programme (WFP)

- Adapting to a changing world and to new technologies, WFP leans towards a more cash-based approach instead of providing food and partners with about 70 banking facilities. WPF introduced several new technologies such as a cloud-based solution to store data of beneficiaries and a mobile vulnerability analysis and mapping tool (m-VAM) by which people can be reached by text message and reply.
- This year, WFP issued its Guide to Personal Data Protection and Privacy consisting of five principles, namely: Lawful and fair collection and processing; Specified and legitimate purpose; Data quality; Participation and Accountability; Data Security. WFP expects a stronger accountability and responsibility towards the data subject as outcome.
- The most current challenges are related to the full implementation of the Guide to Personal Data Protection and Privacy, undue data use and disclosure of data by partners, increasing request for data sharing by governments. In order to overcome these challenges, WFP has a people-centered approach, including consulting with people and informing people adequately, setting up mechanisms for complaining, accessing, updating and erasing data as well as strong post distribution monitoring.

Mila Romanoff, Legal and Privacy Specialist, UN Global Pulse, presenting on the UN Privacy Policy Group – *by video conference*

- UN Global Pulse (UNGP) is an innovation initiative of the Executive Office of the UN Secretary-General which aims to accelerate discovery, development and adoption of data science innovation for sustainable development and humanitarian action. Building on the revised version of the Guidelines for the Regulation of Computerized Personal Data Files adopted by UN GA Resolution 45/95, UNGP developed Data Privacy and Data Protection Principles.
- Challenges relating to data protection surface in different contexts and scenarios, and include the fragmentation of data protection regulatory landscapes, efficient and sustainable data sharing, outdated policies due to the speed of development of new technologies and lack of clear guidance.
- The UN Privacy Policy Group includes over 25 UN offices/funds/programmes as members and several observers. It has been operating since September 2016 with the aim to facilitate dialogue within UN system on data privacy and data protection, increase knowledge and to develop a common approach on data privacy. Currently the group is working on unified data protection principles and definitions to be concluded at the end of the year.

Jean-Philippe Walter, Deputy Commissioner of the Swiss Federal Data Protection Authority and Information Commissioner, presenting on the Privacy and Humanitarian Action Working Group (PHAWG)

- The PHAWG was established following the Resolution on Privacy and International Humanitarian Action adopted in the 37th International Conference of Data Protection and Privacy Commissioners in October 2015. The PHAWG consists at the moment of 10 Data Protection Authorities (DPAs) and 2 linguistic networks.
- The PHAWG is part of the Data Protection in Humanitarian Action project, run jointly by the BPH and the ICRC, whose objectives are to explore the relationship between data protection laws and humanitarian action, to understand the impact of new technologies on data protection in the humanitarian sector and to formulate appropriate guidance. A series of 6 thematic workshops were organized throughout the year 2016 which were used as a basis for the development of a Handbook on Data Protection and Humanitarian Action, publication expected Q3 2017.

Updates of Organizations from the floor and interventions

- ICRC and BPH thanked participants who participated in the thematic workshops related to the Data Protection on Humanitarian Action project and for the written comments submitted to the draft of the Handbook on Data Protection and Humanitarian Action.
- ITU expressed an open invitation to the participants to join its internal Focus Group on Data Processing and Management focusing on supporting Smart Cities and Communities by promoting the establishment of trust-based data management frameworks
- ILO noted the overlap and confusion between data protection and intellectual property.
- The Council of Europe mentioned that it is in the process of modernizing its Personal Data Protection Convention, "Convention 108", and that the fact that the number of its member states is increasing is leading to the possible interpretation that the convention represents a global standard. International organizations will also be able to join the modernized Convention 108.
- ICRC mentioned that it will soon launch a study on Humanitarian Metadata Surveillance and the implications to generate data in a conflict environment. ICRC further stated that its ICRC Data Protection Commission is set up to provide an effective remedy to data subjects, in light of the ICRC's privileges and immunities, which is in the process of developing its Rules of Functioning. The ICRC also mentioned the workshop on Mobile Health and data protection organized in February 2017 jointly with the EDPS and the Swiss Data Protection Authority.
- Eurojust outlined challenges in the interaction with IOs and governmental agencies to receive data related to trafficking in persons and international crimes and proposed that the working group should also discuss the issue of data sharing with law enforcement agencies.
- IOM mentioned that it participated in the 38th International Privacy Conference in Marrakech in October 2016 and proposed that other IO could also apply for observership and participate. IOM also mentioned that it had just adopted a Migration Data Governance Policy.

- Multiple participants raised questions related to the feasibility of obtaining informed and voluntary/free consent in humanitarian situations and participants agreed that it remains a challenge. EDPS proposed to focus on alternative legal grounds to consent as outlined in the GDPR. The ICRC mentioned that the difficulties of using consent as a legal basis and the possible alternatives are discussed in detail in the forthcoming Handbook on Data Protection and Humanitarian Action.

AFTERNOON SESSIONS

Session 2: *Data Protection issues in cloud computing*

Moderator: Professor Christopher Kuner, Professor of law and co-chair of the Brussels Privacy Research Hub at the Vrije Universiteit Brussel

Shashank Rai, Senior Strategic Technology Specialist, UN International Computing Center (UNICC)

- The topic of cloud computing was introduced from a technical perspective explaining that a cloud is basically computing services running in a service provider's data center which can be located everywhere in the world leading to the problem that service providers often are uncertain in which data center and therefore in which country a specific data is stored.
- Several threats to data protection were mentioned, such as hacking, (un)intended disclosure of data and the existence of legal frameworks that allow governments to request data from cloud service providers which can be problematic with regard to the P&I enjoyed by IOs.

Ricardo Guilherme Filho, Director, Legal Affairs Directorate, Universal Postal Union (UPU)

- Certain concerns related to cloud computing were highlighted such as data security and reliability, legal and compliance issues due to limited precedents, lack of transparency (including data protection concerns) and lack of international technical standards. The main legal issues for IOs concern IO's privileges and immunities (P&I) and the protection of sensitive data in a cloud.
- It was highlighted that very few IOs have policies on cloud computing, but that as a principle, IOs should not store sensitive data in a cloud. Moreover, clear cloud usage policies should be established in IOs.
- Servers of the cloud service provider as well as service provider should be ideally located in countries where the IO has adequate P&I. Moreover, IOs should engage as a group in negotiations with service provider companies to enhance the chances that P&I and other important principles for IOs would be included in the contract with the service provider, and to minimize the risk of service provider's "take-it-or-leave-it-approach".

Nikos Volanis, Legal Officer, International Telecommunication Unit (ITU)

- Even though there has been an ongoing debate in the UN system on the usage and handling of cloud computing since 2013, there is no common approach at this point of time.
- ITU takes multiple considerations into account when deciding whether data should be stored in a cloud, such as category of personal data, modalities of transmitting and storing the data by the cloud service provider, purpose of processing personal data, way of ensuring the rights of data subject (consent; access; rectification; erasure), and that the outcomes of these consideration are then included in the agreement with the cloud service provider. It is important to ensure that the service provider informs ITU in case of a request to disclose any data in order to ensure that ITU can invoke its P&I towards the authorities.
- The possibility of different types of encryption, such as end-to-end encryption or homomorphic encryption, as well as the opportunity of quantum computing was mentioned.

Session 3: *Processing personal health data: current practices and challenges*

Moderator: Massimo Marelli, Head of Data Protection Office, ICRC

Dr. Teresa Zakaria, Migration Health Emergency Operations Officer, Migration Health Division, Department of Migration Management, IOM

- Challenges to data protection in health operations conducted by IOM are complex and relate, for example, to identification of a person giving a DNA sample for family reunification, to continuity of care for migrants on the move and to health care in emergency situations.
- Attention was particularly drawn to the importance of ensuring continuity of care throughout migration by sharing data for the prevention of, for example, microbial resistance spread of diseases and complications. Ensuring the protection of personal data when deciding to share data in such contexts was especially mentioned.
- Based on the example of the Ebola-outbreak, the challenges of balancing the individual's right to privacy with public health safety considerations was highlighted.

Dr. Abha Saxena, Coordinator, Global Health Ethics, World Health Organization (WHO)

- Personal health data is different from other types of data due to its sensitivity and due to its link to public trust. Personal health data is used by health professionals for treatment and for public health purposes and can be legitimately shared in several situations.
- WHO's core mandate includes data collection, analysis, publication and dissemination. The collaboration on data, data compilation and statistics are built into WHO's Basic Agreements with Member States.
- WHO has developed a position on data use during public health emergency which enumerates certain critical ethical considerations that must be borne in mind in the context of public health emergencies. Moreover, WHO is in the process of drafting a policy that defines the conditions under which health data collected during non-emergencies can be shared by WHO, including through anonymization procedures.

Andrea Iber, Data Protection Officer, European Centre for Disease Prevention and Control (ECDC)

- ECDC's task is to identify, assess and communicate current and emerging threats to human health posed by infectious diseases. In this regard, ECDC operates a number of data basis. ECDC mentions as an example the set-up of a data base to facilitate the collection, analysis and dissemination of surveillance data on a number of infectious diseases (TESSy).
- With regard to the privacy and database design, pseudonimization was ensured by asking Member States to remove/re-code personal identifiers before inclusion of data. Moreover, variables that were not needed for the activities to be carried out were removed. Compliance with applicable data protection legislation for collection and submission of data was an important factor, so was to ensure data quality (accurateness, up-to-date, etc.).
- TESSy data can be used for scientific research upon request. A peer-review group assesses whether research purpose is genuine and the sharing of data is conditional upon signature of a written undertaking.

DAY TWO

MORNING SESSION

Session 4: *The role of the Data Protection Officer (DPO)*

Moderator: Michela Bonsignorio, Advisor on Protection and Accountability to Affected Populations and DPO a.i., Emergencies and Transitions Unit, WFP

Petra Candellier, Legal Officer, Supervision and Enforcement, EDPS

- As per the GDPR, the DPO is a key player for ensuring, inter alia, the application of the Regulation in an independent manner. DPOs have investigative powers related to data protection matters.
- The independence of DPOs is crucial. It was noted that many organization do not have a fulltime DPO, but only a part-time DPO (together with legal or IT roles), however, this might entail a conflict of interest as well as confusion due to different reporting lines. To ensure independence, DPOs should ideally be full-time, only focusing on data protection and should not have a temporary contract.
- Important is the principle of accountability which helps in moving data protection from theory to practice. Accountability goes beyond compliance with the rules - it implies a culture change. The GDPR integrates accountability as a principle which requires that organizations put in place appropriate technical and organizational measures and can demonstrate what they did when requested. EDPS launched an Accountability Project in 2015 and developed a specific tool to be shared with EU institutions: a set of questions for staff member dealing with data that relate to data protection management and to organizational policies measures.

Diana Alonso Blas, Data Protection Officer/ Head of the DP service, Eurojust

- Eurojust is not yet under the supervision of EDPS, but this will change soon. The implementation of the GDPR will have a big impact on the protection of data and certainly strengthen the role of DPOs who now have a clear legal basis for their establishment. Eurojust introduced certain procedures to ensure compliance with data protection issues: Weekly checks based on a standard checklist whose outcome is addressed in an internal report for accountability purposes that could be used to start a process in case of non-compliance; monthly time limit reviews; annual compliance report.
- In addition to the DPO, a Joint Supervisory Body (JSB) was introduced as external control mechanism in which members are judges or have an equal level of independence. JSB monitors the correct application of the rules on data protection, can issue binding rulings on appeals by individuals and carries out frequent inspections. Information gather through the compliance procedures highlighted above is shared with the JSB who uses it as input for their own inspections.
- Eurojust has a technical system to store data that does not allow to bend the data protection rules since it applies the rules automatically. In the system it is possible to trace the date data was received, who it was shared with and how long it is stored. The system notifies the DPO automatically.

Caroline Goemans-Dorny, Data Protection Officer, Interpol

- While there is a clear trend of increased data sharing involving IOs, there is a big difference between IOs that have data processing in their core mandate and other IOs that do not.
- It is important to build a trusting environment which requires transparency and accountability. Interpol has introduced its Rules on the Processing of Data in 2016 and it created an independent supervisory board to oversee their compliance.
- The IDPO -introduced in 2016- has a mandate to monitor the lawfulness and compliance of data processing activities; to provide advice and recommendations; to liaise, collaborate and ensure coordination with DPOs at the national level; to examine the

yearly reports of the DPOs at the national level; to provide training and awareness among staff; to liaise with the Commission of the Control of Interpol's Files (CCF) and with DPOs of other institutions and with other bodies; to submit annual report to Executive Committee and Commission for Control of Interpol's files.

Session 5 ***The EU General Data Protection Regulation (GDPR): data transfers to international organizations***

Moderator: Jean-Philippe Walter, Deputy Commissioner of the Swiss Federal Data Protection Authority and Information Commissioner

Massimo Marelli, Head of Data Protection Office, ICRC

- As recognised in the Resolution of the International Conference of Privacy and Data Protection Commissioners on Privacy and International Humanitarian Action (Amsterdam 2015), and in the Draft Questionnaire for the Evaluation of States and International Organisations of the Council of Europe TPD Committee (Questionnaire), it is crucial for the independence of IO that their P&I are respected. If P&I are not respected and there is pressure to disclose personal data, the independence of the work of the IOs could be compromised and vulnerable people harmed.
- As also set out in the Questionnaire, the importance to have effective remedies to the upholding of P&Is of IOs was emphasized which was linked to the assessment of local courts concerning the upholding of P&Is when IOs are alleged of a violation of a fundamental right, such as the right to privacy.
- With regard to data protection, the ICRC's Rules are aligned with the requirements outlined in the GDPR. It was highlighted that the principles of the GPDR were compatible with enabling entities subject to the GDPR to enable the ICRC's performance of its mandate and that when data is transferred to an IO (to which the GDPR is not applicable), the GDPR foresees additional protections have to be guaranteed to ensure data protection under Chapter V (Transfers). Chapter V of the GDPR includes different bases according to which data can be transferred to IOs, and it is interesting to see the derogations mentioned, as they include "public interest" as a basis for data transfers as well a "legitimate interest", that could be appropriate for IOs to receive data from entities covered by the GDPR.

Lance Bartholomeusz, Head, Legal Affairs Services (LAS), UNHCR

- Data protection is crucial for humanitarian organizations such as UNHCR or IOM especially as the consequences for the data subjects in case of inadequate protection can be life threatening.
- When assessing the applicability of data protection legislation, including the GDPR, to UNHCR, the following legal frameworks need to be taken into account: The UN Charter, the 1946 Convention on the Privileges and Immunities of the United Nations, the 1951 Convention and 1967 Protocol relating to the Status of Refugees, international refugee law, human rights law.
- The UNHCR Data Protection Policy was adopted in 2015 to respond to the challenges arising from (i) new forms of protection activities (e.g. cash assistance by mobile devices) requiring enhanced cooperation between UN agencies and with the private sector; (ii) increased use of biometrics. The UNHCR Data Protection Policy aligns with international data protection principles as reflected in human rights treaties and EU human rights law.
- UNHCR cannot apply different levels of protection to refugees depending on where data is collected and/or processed. It thus applied consistently its internal Data Protection

Policy. Unless otherwise agreed with relevant governments, UNHCR partners must observe national laws when processing data on behalf of UNHCR and transferring data to it: since they are also bound to observe UNHCR Data Protection Policy their processing should be deemed generally in line with EU Data Protection principles.

Bruno Gencarelli, Head, and Ralf Sauer, Deputy Head, International data flows and protection unit, DG Justice and Consumers, European Commission - *by video conference*

- The European Commission thanked the organizers for the possibility to be part of the workshop and wanted to use the opportunity to clarify certain issues related to the GDPR and to engage in an exchange with the participants of the Workshop.
- It was stressed that with regard to data transfers from an entity to which the GDPR is applicable to IOs, the principles of the GDPR are the same or very similar to the ones that are already in force and the GDPR is only ensuring the continuity of the existing rules. The approach taken in the GDPR does not aim to restrict data sharing, but, on the contrary, to broaden the tool box for transfer of data.
- It is crucial to distinguish two different scenarios:
  1. Transfer to IOs by entities subject to EU data protection to which the Directive 95/46/EC and soon GDPR are applicable which means that the transfer needs to comply with the rules regulated therein.
  2. Processing of data by IOs to which P&I apply.
- The European Commission invited participants to engage with it in further discussions on the topic of GDPR and its implications for IOs on a bilateral basis which was welcomed by the participants.

Closing remarks

Sophie Louveaux, Head of Policy and Consultation, EDPS

- EDPS thanked the panel and participants for very interesting presentations, discussions, strong engagements and a lot of fruitful exchanges as well as IOM for hosting the event.
- As a summary, it was noted that new technologies are a trend and that participating organizations, although having different standards, seem to have a common approach on data protection issues. The challenges mentioned during the Workshop's discussions were highlighted such as balancing privacy versus safety as well as public health versus data protection, anonymization of data, informed and voluntary consent, need-to-know-approach and the need of safety with regard to cloud computing services.
  The EDPS welcomes the setting up of the independent control commission recently created for ICRC as independent supervision is a key component of a strong data protection regime.
- EDPS commits to promote and support the work of the network, to act as a facilitator for the Workshop and it is looking for a volunteer organization to organize the Workshop in 2018.

Johan Rautenbach, Legal Counsel, IOM

- IOM thanked the panellists, moderators and all participants for their interest in the workshop, for their active participation throughout the two days and the rich and substantive discussion as well as EDPS for their co-hosting.
- IOM highlighted the value of having so many IOs, including newcomers, in the network and promised to share the participant list with contact details in order to deepen the cooperation.