DATA TALKS NOVEMBER 2017: *GDPR AND DATA IMMUNITIES*

The third session of the Data Talks series focused on the European Union's General Data Protection Regulation (GDPR) which will enter into force in May 2018, and how it will affect transfers and management of personal data within and across international organisations (IOs). The session also looked into the diplomatic immunities that may apply to IOs in relation to data.

The moderator, Ms Barbara Rosen Jacobson, programme manager at DiploFoundation, began by summarising the finding of a questionnaire that was distributed among IOs in Geneva. The questionnaire showed that although most respondents had been aware of the GDPR for more than half a year, not all organisations were dealing with the new regulation. the reason is most likely either due to the limited amount of personal data collected and processed by the organisation, or due to a lack of awareness on how the GDPR applies to IOs. The respondents identified a large number of departments within IOs where the GDPR is addressed, including information technology, legal, and human resources departments.

The discussion was opened with a presentation by Mr Massimo Marelli, head of the Data Protection Office at the International Committee of the Red Cross (ICRC) in Geneva, who focused on the implications and possible impact of recent regulatory developments in the EU (GDPR) and Council of Europe (Modernised Convention 108). These are mainly of relevance when transfers of personal data are envisaged from entities subject to these instruments, and third countries and IOs. Chapter V of the GDPR provides for specific requirements to ensure that whenever personal data processed under the 'jurisdiction' of the GDPR leaves the EU to third countries or international organisations, the protection under the GDPR is not compromised by making such transfers subject to specific conditions.

International organisations & data protection regulations

Marelli explained that the GDPR's definition of an IO is very broad as it identifies 'an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries'. The definition of an IO is equally broad in the Council of Europe's Convention 108 ('Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data'). Convention 108 could be acceded to by IOs (and countries outside of the Council of Europe). Conditions for accession, and'considerations about the complexities involved in analysing the adequacy of an IO's 'jurisdiction' are developed in the draft questionnaire to be used by the Convention 108's expert committee (T-PD). Besides the GDPR and Convention 108, resolutions at the international level could provide guidance, such as UNGA resolution 45/95 and the Resolutions of the International Conference of Privacy and Data Protection Commissioners.

The ICRC's current data protection regulatory framework is based on the Headquarters Agreement (HA,1993), and the ICRC Rules on Personal Data Protection, which establish a mechanism allowing individuals to challenge ICRC staff decisions in data protection cases and obtain an effective remedy. In addition, the ICRC together with the Brussels Privacy Hub has released a Handbook on Data Protection in Humanitarian Action, providing data protection guidelines for humanitarian organisations.

Data transfers between international organisations and other entities

Marelli explained that, according to the GDPR, transfers of personal data of EU citizens to IOs can take place after an *adequacy decision* by the European Commission, which would decide that the organisation ensures an adequate level of protection. So far, no IO under scrutiny has passed this test. Yet, data transfers are still possible if they are subject to appropriate safeguards (article 46) or for important reasons of public interest (article 49). These definitions give rise to grey areas, and it remains to be seen how practice develops.

The GDPR does not regulate transfers within organisations, as it assumes that within organisations, a consistent level of protection is maintained. Yet, what happens when data is outsourced for processing outside an IO? This could give rise to legal complexity, as the immunities of the IO are generally attached to the data – even when it's in the hands of an external processor – yet domestic law could apply to the processor. This scenario would require a case-by-case analysis of the situation considering (i) whether privileges and immunities of the IO apply, (ii) whether inviolability of data was respected and (iii) what the responsibilities of the external processor are under domestic legislation.

Data protection within an international organisation

Mr David Foster, head of Data Privacy Protection at CERN, focused on protection within an IO. CERN processes large amounts of personal data related to the 10 000 data subjects present on the site at any given moment. The or-

ganisation maintains a broad definition of personal data, although there are still grey areas. For example, are IP addresses personal data in every circumstance and how to reduce the cost of managing such personal data while reducing the risks to the data subjects? Middle management in the organisation are held accountable as internal controllers of data, and they need to be made aware of their responsibilities. He further considered practical challenges regarding existing CERN IT services in granting the adequate protection of personal data. In addition, with the increased difficulty to distinguish between the public and private use of IT, what are the obligations to prevent organisations from processing the personal data from employees' devices? To bring more clarity on the status of data management and protection at CERN, Foster's unit is conducting an extensive mapping exercise. Finally, he raised the question how the EU privacy regulations will work with the GDPR to fully address data protection concerns, as it addresses machine-to-machine communication and the handling of metadata, which is something extensively processed in highly complex technical environments.

Mr Viktor Polic, head of Information Security and Assurance Services at the International Labour Organization (ILO), explained the organisational structure related to data protection responsibilities in the ILO. In 1997, the ILO adopted the Code of Practice on the Protection of Worker's Personal Data, addressing the protection of personal information between the employee and the employer. Internal organisational policies and processes have been updated and expanded to cover the protection of personal data in relation to the use of Information and Communication Technologies (ICTs) and the complex hierarchy of management responsibilities for ICT Governance, Risk and Compliance. The most important updated policies are Internal Policy for Information Classification and Personal Data Protection Policy. With these new regulations, the Office of Legal Adviser has assumed a central role in the governance of personal data protection, and the bridge has been established to Polic's information security unit for assessing the adequacy of protection controls in place related to ICTs that store and process personal data, whether managed by the ILO or third-parties, and for response coordination to possible breaches and violations. The ILO manages extensive datasets from external sources used for research, labour policy analysis, labour inspection, development co-operation and many other activities with external subjects. To provide internal services related to financial, human resources, programmatic, and other business processes additional data sets are used within many ICT systems. An example was given for an extensive data set of information security and risk management support system that has been collecting data from all computing devices from the ILO's offices over the last three years. Such big data systems represent a challenge for the practical implementation of data protection regulations if they are not covered with transparent, auditable management practice. He concluded by outlining several additional challenges, such as the security of cloud computing; the legal status of data when it is stored in one jurisdiction and processed in another; and the relation of IOs with the Internet industry, and made references to initiatives where such challenges are currently being addressed, such as the UN Chief Executive Board's High Level Committee on Management ICT network that published Guidelines for risk management when adopting cloud computing services.

International organisations and diplomatic immunities

The following discussion addressed the diplomatic immunities for IOs on their management of data. An example from INTERPOL was highlighted, when a French citizen challenged the organisation's data protection provisions in a French court. The court acknowledged INTERPOL's privileges and immunities but determined it had to check whether the organisation provided an effective remedy before accepting to defer to the organisation's privileges and immunities. These cases raise additional questions: which body is to be addressed if a UN employee is concerned with the protection of his/her data? IOs usually have their own regulations and bodies tackling data protection. However, if such a mechanism is not present or is considered deficient, then it might be possible for courts to decide that they need to step in and provide an effective remedy. Should this scenario arise, a second question would then arise: whose laws should the court apply to provide an effective remedy: would it apply the rules of the IO or resort to domestic legislation?