Draft agenda for the closed session -
the 32nd international Conference of Data Protection and Privacy Commissioners

Dear friends and colleagues,

As host of the 32nd International Conference of Data Protection and Privacy Commissioners, I am delighted to present to you a partial draft agenda for the closed session for regulators. This year, the closed session will be held after the close of the open conference, on Friday, October 29, between 9am and 1:30pm. As you may know, the closed session provides the formal part of the Conference, where DPAs are accredited and resolutions are debated and voted upon.

The main theme of the open conference is "Privacy: Generations", setting out to explore how **a new generation of technologies** and **a new generation of users** have disrupted the current framework and necessitate **a new generation of governance**. A new generation of governance means not only prospective changes in the legislative framework, but also innovative regulatory strategies and new approaches to enforcement. We therefore suggest that the topic for the closed session will be **"Collaboration between Data Protection Authorities and other Regulatory Bodies"**. Specifically, we would like to discuss potential collaboration between data protection authorities and other regulatory bodies, such as competition authorities, capital market regulators, and consumer protection watchdogs.

The 31st Conference of Data Protection and Privacy Commissioners in Madrid unanimously adopted the "International Standards on the Protection of Privacy with Regard to the Processing of Personal Data". The Standards set forth that privacy and data protection supervisory authorities "shall try to cooperate with each other to

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

achieve a more uniform protection of privacy with regard to the processing of personal data, at both national and international level." Our view is that given the increasingly complex ways personal data are intertwined with business decisions, it is imperative to form a framework for collaboration not only among data protection regulators, but also between data protection regulators and additional regulatory authorities.

We intend to devote **two hours of the closed session** for sharing information and experiences about these themes. We would like to explore and discuss issues such as (a) potential synergies between regulatory mandates, capitalizing on experiences gained by EU and US competition authorities in their review of the Google-Doubleclick merger, or the UK Financial Services Authority fining the Nationwide Building Society in an amount of £1 million for a data security breach; (b) regulatory conflicts, such as data sharing mandated by banking regulators, whistleblowing rules under the Sarbanes-Oxley corporate governance reforms, or data retention requirements – all in tension and potential conflict with data protection law; and (c) frameworks for collaboration among regulators, including in policy making, intelligence, communications and enforcement. [See elaboration in Annex I hereto].

In order to facilitate the discussion, we attach as Annex II a draft questionnaire which will help us assemble different points of view and experiences from DPAs in different regions of the world. We would greatly appreciate your completion of the questionnaire, sharing your thoughts, insights and experiences on the subject. As always, the success of the discussion hinges on your active interest and participation. I therefore ask that you please complete the questionnaire, adding additional questions if you see fit; comment freely on the draft agenda; and send us your feedback no later than September 15. In addition, I invite you to offer to present your work and views on the subject in the closed session. In order to prepare the event, I ask that you please appoint a contact person who will liaise with ILITA staff ahead of the conference. Our contact person for the closed session is Amit Ashkenazi, head of ILITA's legal department (amita@justice.gov.il;+972-3-7634080).

I look forward to hosting you in Jerusalem in October and wish you an enjoyable and peaceful visit to Israel.

Sincerely,
Yoram Hacohen
Head of ILITA

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

Annex I - DRAFT Outline

Collaboration between Data Protection Authorities and other Regulatory Bodies

A. **Synergies.**

- Given the technological, economic, and social changes that have taken place over the past three decades, since the inception of the current data protection framework, personal data have become the key raw material of the information economy. Decisions regarding personal data and their collection, use, transfer, retention and security have permeated strategic business processes including corporate governance, marketing, operations management and finance. They therefore impact areas subject to additional regulatory frameworks, including competition law, consumer protection, telecom regulation, securities regulation and protection of critical infrastructure.
- Data protection regulators would benefit from cooperation with other regulators taking into account such other regulators' legislative mandates, institutional tools and enforcement powers.
- We believe such a multi-thronged approach to regulation can deliver greater benefits to markets, consumers and the economy as a whole. It can also enhance efficiencies to businesses, which are currently confounded by an increasingly perplexing regulatory labyrinth consisting of layers upon layers of sometimes contradictory obligations.
- By harmonizing regulatory requirements and capitalizing on synergies in enforcement powers and regulatory tools, we will ensure regulation is consistent and complementary, and thus easier for businesses to implement and for regulators to enforce.
- Several examples are illustrated below:
- **Protection of the principle of "free, unambiguous and informed consent"**
    - **Consumer protection regulators.** Consumer protection regulators are authorized to scrutinize and restrict the scope of excessively broad provisions in standard form

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

contracts. Such provisions are often included in privacy policies and liability disclaimers pertaining to authorize disproportionate uses or transfers of personal data. In addition, consumer protection regulators are authorized to curtail intrusive behavioral advertising methods, increase transparency and ensure consumer consent is fully informed.

- **Competition regulators**. Personal data is increasingly seen as a source of market power. In markets ranging from online advertising and social media to telecoms, health and financial services, aggregated data may yield even greater returns to businesses than their core economic activities. Where one or two companies exert market power, consumer choice is limited and consent rid of meaning. By limiting market power and reducing concentration, competition regulators can tip the scales back in the direction of consumers, thereby increasing transparency and choice.

- **Accountability**
  - **Securities regulators.** The market crashes of 2001 and 2008 have focused the attention of securities regulators on corporate governance structures and the accountability of companies and senior executives. With personal data elevating to become a key business asset, there is a growing understanding that privacy and data protection must be integrated as a critical module into corporate governance schemes. This includes not only IT security, which is already regulated under the U.S. Sarbanes-Oxley Act, but also information management and data protection measures.
- **Information security**
  - **Financial market and health regulators**. The financial and health sector have long been subject to regulation requiring the implementation of information security standards, including standard audits and oversight mechanisms. Nevertheless, significant data security

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

breaches in these sectors highlight the need for effective enforcement and regulatory cooperation.

- **Critical infrastructure watchdogs**. *The Economist* has recently declared that "after land, sea, air and space, warfare has entered the fifth domain: cyberspace." The appointment by U.S. President Barack Obama of a cyber-security tsar and establishment of a new Cyber Command signal the gravity of risk that cyberwarfare poses to global peace and infrastructure. Critical infrastructure watchdogs impose information security requirements to ensure the integrity and safe operations of systems including the electric grid, air traffic control, telecommunications networks and oil pipelines. These requirements should mesh with data protection rules into a seamless network of information management obligations.

B. **Potential conflicts.**

- Data protection law sometimes runs into potential or direct conflict with other regulatory frameworks. Best efforts should be made to eliminate inconsistencies and deliver to businesses a fair and coherent set of requirements.
- Some recurring examples appear below:
  - **Data retention**. Archiving rules and data retention requirements potentially conflict with the data minimization principle underlying data protection laws. Businesses are finding themselves in a quandary facing apparently incompatible requirements mandating data retention on the one hand (*e.g.*, the EU Data Retention Directive; Anti Money Laundering legislation), and data deletion on the other hand.
  - **Whistleblowing rules**. Whistleblowing hotlines, allowing employees to report their concerns anonymously about possible violations by their fellow workers, have been mandated by the Sarbanes Oxley Act, which applies to all companies traded on U.S. stock exchanges. Companies which fail to comply with these rules are subject to heavy sanctions and

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

penalties. Yet the legality of such hotlines has been called into question in Europe, leaving companies to face an intractable problem of apparently having to comply with one set of rules at the expense of violating the other.

- **E-discovery**. The breadth and scope of U.S. e-discovery rules have created a tension with the data protection principles of proportionality and purpose limitation as well as EU restrictions on cross border data transfers. Here too, violation of one set of rules may be detrimental, as illustrated by the well known decision of the United States District Court case of *Zubulake v. UBS*.
- **National databases**. Technological breakthroughs and the rise of digital identity and e-government have increased states' interest in the establishment of massive national databases, such as biometric identity systems, national health records, or financial clearinghouses. These innovations, which serve important and legitimate public interests such as increased security, efficiency, and public health, impose privacy "externalities" which are not always factored in by relevant government agencies. The initiation of a dialogue between and such government agencies and data protection regulators is essential to ensure individual privacy is not scarified in pursuit of additional public interest goals.

C. **Frameworks for collaboration.**

- In order to facilitate collaboration with additional regulatory authorities, a framework needs to be put in place to allow joint policy making sessions, as well as collaboration in intelligence, communications and enforcement. In addition, a conflict resolution mechanism should be put in place to prevent regulatory disputes and forum shopping.

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

Annex II – Short Questionnaire*

I. Have you had any experiences of cooperation or conflict with Other Regulators?

[ ] No

[ ] Yes. If so:

a. Please list Other Regulators with which you have cooperated:

_____

_____

b. Please specify one case illustrating regulatory cooperation (if any)

_____

_____

_____

c. Please specify one case illustrating regulatory conflict (if any)

_____

_____

_____

II. What do you consider to be the three most important considerations in handling regulatory cooperation or conflict with Other Regulators?

I. _____

II. _____

III. _____

* "Other Regulators" in this Questionnaire means competition, consumer protection, securities, banking, health, financial markets, anti money laundering, critical infrastructure, or similar regulatory authorities operating in your jurisdiction, except for data protection authorities.

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

IV. What can a DPA offer to Other Regulators in return for regulatory cooperation?

V. Do you have a coordinating mechanism and/or conflict settlement mechanism (formal or informal) vis-à-vis Other Regulators? Please specify.

VI. What are the areas under your responsibility for which you require and would benefit from regulatory collaboration? (*e.g.*, joint policymaking, complaint handling, intelligence, investigations, enforcement, communications with business and/or consumers, public and press relations?)

VII. Do you support cooperation between different regulatory organizations (e.g., DPAs and securities regulators?)

VIII. Do you think the ICDPPC should approach similar regulatory organizations?

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il