Warsaw declaration
on the "appification" of society

35th INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY COMMISSIONERS
PRIVACY: A COMPASS IN TURBULENT WORLD
Warsaw, 23-26 September 2013

Warsaw, Poland - 24 September 2013

Nowadays, mobile applications (apps) are ubiquitous. On our smart phones and tablets, in cars, in and around the house: a growing number of items have user interfaces connected to the internet. Currently, over 6 million apps are available in both the public and private sector. This number is growing by over 30.000 a day. Apps are making many parts of our day-to-day lives more easy and more fun. At the same time, apps also collect large amounts of personal data. This allows for continuous digital monitoring, often without the users being aware that this happens and what their data are used for.

App developers are often unaware of the privacy implications of their work and unfamiliar with concepts like privacy by design and default. The main operating systems and app platforms do offer some privacy settings, but do not allow for full control by the users to protect their personal data and verify what information is collected for which purpose.

During their 35th International Conference held on 23 and 24 September 2013 in Warsaw, the data protection and privacy commissioners discussed the "appification" of society, the challenges posed by the increased use of mobile apps, as well as possible ways to address these.

Various reports published by the data protection community on mobile apps in the past years, including but not limited to the European Union's Article 29 Data Protection Working Party's *Opinion on apps on smart devices*, the Privacy Commissioner of Canada's *Guidance for mobile app developers,* the United States Federal Trade Commission's staff report *Mobile privacy disclosures: building trust through transparency* as well as the International Working Group on Data Protection in Telecommunication's 2012 *Sopot Memorandum*, give valuable guidance on how to deal with the relation between apps and privacy.

The commissioners expressed their clear commitment to ensure users are offered a better privacy experience and plan to address various actors in both the public and the private sector with regard to their roles and responsibilities.

It is essential that **users** are and will remain in charge of their own data. They should be able to decide what information to share with whom and for what purposes. To this end, clear and intelligible information should be available - including within an app - about data collections taking place before the actual collection starts. Users should be given the option to allow access to specific information like location data or address book entries on a case-by-case basis. Most importantly, apps should be developed on the basis of surprise minimisation: no hidden features, nor unverifiable background data collection.

App developers are drivers of the growth in the digital economy and bring ease to our day-to-day lives. At the same time, they need to ensure compliance with existing privacy and data protection rules around the globe. In order to achieve this goal and at the same time maintain a positive user experience, privacy should be taken into account at the very start of the

development of an app. In this way, privacy can also provide a competitive advantage by increasing user trust. Developers need to make a clear decision on what information is necessary for the performance of the app and ensure no additional personal data is collected without informed user consent. This also applies when third party code or plug ins are used by app developers, for example from ad networks. Developers at all times need to be aware what they offer to and request from their users.

The responsibility for privacy does not rest with app developers alone. **Providers of operating systems** should bear responsibility for their platforms. Admittedly, these actors are increasingly taking up their responsibility by offering general privacy settings on mobile devices. However, these are insufficiently granular to offer full user control for all meaningful aspects of individual data collection. As platform providers create and maintain the framework in which apps are used, they are best positioned to guarantee data protection and bear special responsibility towards the users. In this respect, commitment of the industry to privacy seals or other enforceable certification schemes is to be encouraged.

Although the primary responsibility for user privacy lies with the app industry, **privacy and data protection commissioners** can and should raise awareness of these issues amongst the actors of the app industry as well as with app users, the general public. In particular, engagement with providers of operating systems should be sought in an endeavour to ensure the essentials of data protection are put in place in their platforms. It is not our task to spoil the fun apps can offer to their users, but misuse of personal data has to be prevented. If encouraging a better privacy practice does not resort to sufficient effect, the commissioners will be ready to enforce the legislation in a global effort to reclaim user control.

The privacy and data protection commissioners around the world intend to use the coming year to make serious steps in improving privacy and data protection in this area and will revisit the subject during their 36th Conference in Mauritius.

Wojciech Rafał Wiewiórowski
Generalny Inspektor Ochrony
Danych Osobowych

Jacob Kohnstamm
Chairman of the Executive
Committee of the International
Conference