36th International Conference of Data Protection and Privacy Commissioners

Resolution
Big Data

Proposer

- Norwegian Data Protection Authority

Co-sponsors

- Dutch Data Protection Authority, the Netherlands
- Federal Commissioner for Data Protection and Freedom of Information (Germany)
- Federal Data Protection and Information Commissioner (Switzerland)
- Office of the Data Protection Ombudsman (Finland)
- Italian Data Protection Authority
- Office of the Information Commissioner (UK)
- Estonian Data Protection Inspectorate
- Danish Data Protection Agency
- Swedish Data Inspection Board
- Office of the Privacy Commissioner of Canada
- Berlin Data Protection Commissioner
- Spanish Data Protection Agency

It is often recognized that the ability to store and analyse vast quantities of data may prove beneficial to society. Big Data may be used, for example, to predict the spread of epidemics, uncover serious side effects of medicines and combat pollution in large cities. Some of these uses do not implicate personal information; however, Big Data may also be utilised in ways that raise important concerns with regard to the privacy of the individuals and civil rights, protections against discriminatory outcomes and infringements of the right to equal treatment.

Big Data entails a new way of looking at data, revealing information which may have been previously difficult to extract or otherwise obscured. To a large extent, Big Data involves the reuse of data. The value of the data may be linked to its ability to make predictions about future actions or events. Big Data can be perceived to challenge key privacy principles, in particular the principles of purpose limitation and data minimisation.

The protection provided by these privacy principles is more important than ever at a time when an increasing amount of information is collected about us. The principles provide the foundation for safeguards against extensive profiling in an ever increasing array of new contexts. A watering down of key privacy principles, in combination with more extensive use of Big Data, is likely to have adverse consequences for the protection of privacy and other fundamental rights.

Members of the International Conference and other stakeholders, including, for example,

the International Working Group on Data Protection in Telecommunications (IWGDPT, a.k.a. "Berlin Group"), have considered data protection and privacy issues relating to Big Data. Privacy concerns relating to the use of profiling have been raised by the International Conference in the Uruguay Declaration on Profiling of 2012 and in the Warsaw Resolution on Profiling of 2013. To further encourage efforts to help reduce risks associated with the use of Big Data

the 36th International Conference of Data Protection and Privacy Commissioners calls upon all parties making use of Big Data:

- To respect the principle of purpose specification.
- To limit the amount of data collected and stored to the level that is necessary for the intended lawful purpose.
- To obtain, where appropriate, a valid consent from the data subjects in connection with use of personal data for analysis and profiling purposes.
- To be transparent about which data is collected, how the data is processed, for which purposes it will be used and whether or not the data will be distributed to third parties.
- To give individuals appropriate access to the data collected about them and also access to information and decisions made about them. Individuals should also be informed of the sources of the various personal data and, where appropriate, be entitled to correct their information, and to be given effective tools to control their information.
- To give individuals access, where appropriate, to information about the key inputs and the decision-making criteria (algorithms) that have been used as a basis for development of the profile. Such information should be presented in a clear and understandable format.
- To carry out a privacy impact assessment, especially where the big data analytics involves novel or unexpected uses of personal data.
- To develop and use Big Data technologies according to the principles of Privacy by Design.
- To consider where anonymous data will improve privacy protection. Anonymisation may help in mitigating the privacy risks associated with big data analysis, but only if the anonymisation is engineered and managed appropriately. The optimal solution for anonymising the data should be decided on a case-by-case basis, possibly using a combination of techniques.

- To exercise great care, and act in compliance with applicable data protection legislation, when sharing or publishing pseudonymised, or otherwise indirectly identifiable, data sets. If the data contains sufficient detail that is, may be linked to other data sets or, contains personal data, access should be limited and carefully controlled.
- To demonstrate that decisions around the use of Big Data are fair, transparent and accountable. In connection with the use of data for profiling purposes, both profiles and the underlying algorithms require continuous assessment. This necessitates regular reviews to verify if the results from the profiling are responsible, fair and ethical and compatible with and proportionate to the purpose for which the profiles are being used. Injustice for individuals due to fully automated false positive or false negative results should be avoided and a manual assessment of outcomes with significant effects to individuals should always be available.