 ISBN: 9789073592421

IPS Paper

Planning for privacy and confidentiality

Author: Mr Baldur Kubo

Coauthors: Triin Siil

Submission ID: 1436

Reference Number: 1436

Brief Description

The availability of unprecedented amounts of digital data, combined with increasing awareness by citizens and companies about the value of their data, call statistical institutions to adopt stronger mechanisms to ensure privacy and transparency of the statistical production process in order to preserve public acceptance and trust.

Some novel
technologies that have emerged recently at the intersection between the fields of cryptography, distributed systems and computer science, are instrumental to achieve this goal.

The family of so-called Privacy Enhancing Technologies
(e.g.

Secure Multiparty Computation, Homomorphic Encryption and Trusted Execution Environment) open new possibilities in terms of how “data” and “computation” are handled and controlled within and across organisations.

With
these technologies, governance policies can be enforced technologically without necessarily relying on a single point of trust.

These technologies have reached maturity and are already moving from laboratories to real-world applications.

An increasing number of statistical institutions have started to pioneer possible applications of these technologies in explorative or pilot projects around different use-cases.

The goal of this session is to provide a stage
for such pioneering activities, share early experiences and lessons learned, discuss what we can (or can not) expect from these technologies and exchange views as to how the adoption of these technologies impacts (or is impacted by) organisational aspects, business processes and legislation.

The session will consist of 4 speakers reporting on
experimental and pilot projects leveraging PET for statistics, including one speaker from the UN PET Lab.

The session
will be divided in two parts, with a series of brief presentations by the speakers followed by a panel discussion between the speakers.

Abstract

Modern data sources, e.g. mobile location, retail, financial transactions data, created by the population living their daily lives, provide opportunities for fast and accurate official statistics. Such secondary use of data could provide population, tourism, economic statistics on country or regional level while reducing response burden of primary sources of statistical information.

But would it be feasible financially and security wise, to fit all that data into a national statistics organization?

Cloud services offer a way to create economic data processing pipelines, be they private clouds offered by a governmental organization or public clouds by private sector.
But how could the data owners and citizens be sure, that all the data is secure and the principles of data protection legislation: data minimization, confidentiality, privacy, transparency and avoidance of misuse are kept, when they give away the control of their data?

Based on the project done by Eurostat and Cybernetica we will discuss how privacy enhancing technologies like secure multiparty computation, trusted execution environments and homomorphic encryption provide statistical offices the ability to plan efficient production processes capable of analysing the volumes of new data sources while providing technical guarantees and cryptographic proofs to data owners, data subjects and data protection agencies.
We will discuss how the stakeholders can work together to notice the threats to data and how to mitigate the risks with technical controls, even when data is being processed outside the organization.