EUROPRIS

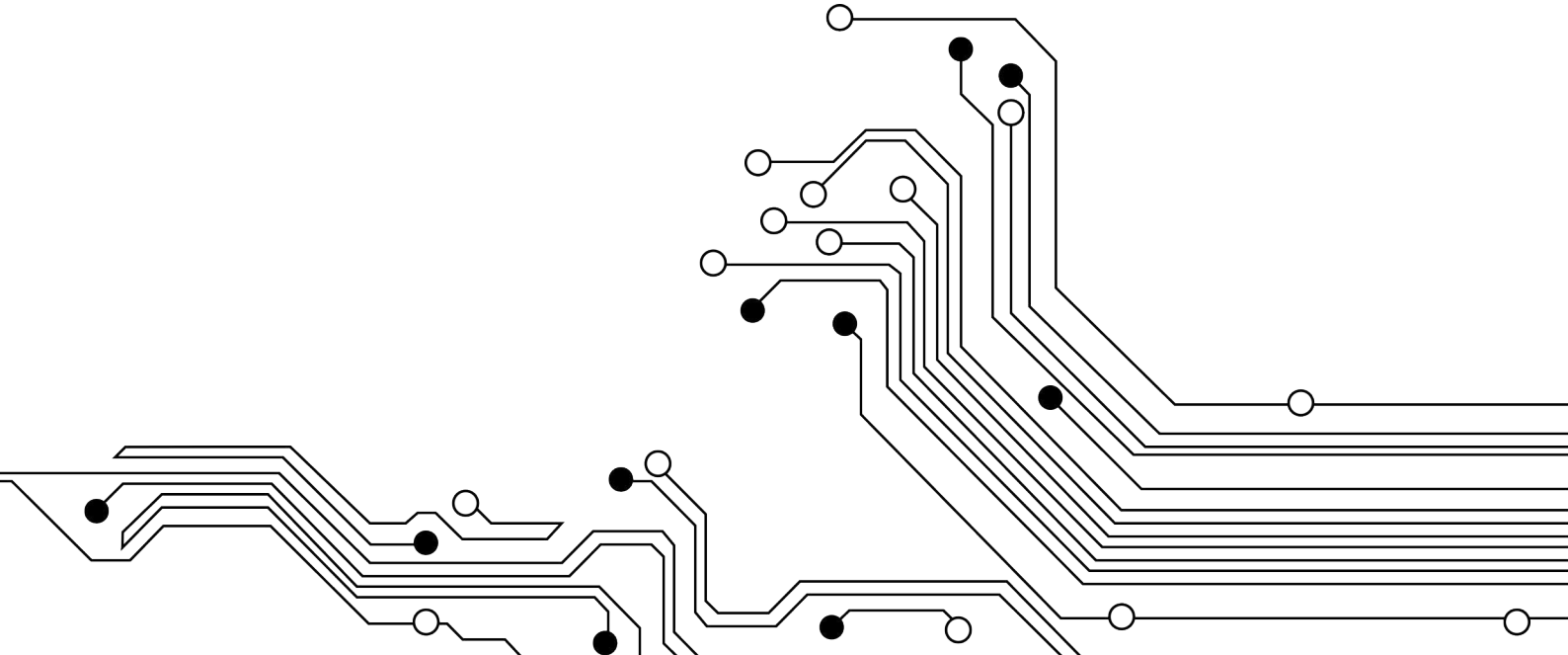
ICT in PRISONS

EuroPris Expert Group

Cloud and Data Protection in Offender Digital Services

Case study

By:
Tuuli Siiskonen, Criminal Sanctions Agency Finland
Pierre Wilderiane, Belgian Prison Service



Cloud and Data Protection in Offender Digital Services

Case study

Presented by Criminal Sanctions Agency Finland and Prison Services Belgium

Federal Public Service
Justice

SITUATION

Cloud access is becoming more and more a regular thing for many software companies and therefore for most of the programs we are working with nowadays. It brings a lot of opportunities for everyone and change our view on data access and data sharing.
With that reality in mind, the prisons have to renew their programs and even their network.

A few Belgian examples in the cloud management:

a. Obviously the first that comes in mind is the "PrisonCloud" program. It's actually running in two prisons and the installation in a third one is actually on his way. This piece of software allows a lot of things for the inmates : phonecalls, watching television, video on demand, buying things from the prison shop, communicate with the prison staff, working with a virtual pc, having a restricted access on the internet, e-learning,…
All the data's are on specific servers (on site and in the data center of the firm). That piece of software authorizes a lot of things that are very useful for the authorities (managing white and black lists for communications, recording some communications,…), for the inmates (E-learning, virtual pc,…) or for the two parts (handling the prison shop, communication between staff and prisonners,…).
This new system brings new possibilities but also new questions :
- Who has access to the data's (only the prison staff or also the firm staff ?)
- Where are the personal data's of the prisoners ? (prison server ?Firm servers ? Firm data center (in or out EU?)
- What about the links between Justice network and the "outside world" (in concrete : is there security risks ? how to handle them ?)

b. A second example is the new sidissuite software which was created two years ago. This program is there to handle the whole incarceration process of every inmates from incarceration to the final liberation. This program is only there for the administration but not only the penitentiary administration, it's there for every partners in the penal process. It brings a lot of possibilities and interactions between services :
i. the courts can upload documents of information such as the dates of the trial,…
ii. the police from all the country can check the system to be sure that the person they are controlling is not an escape prisoner or someone who must be in prison
iii. the service in charge of the prisoner's transportation who can manage the scheduled transfers
iv. the probation services can access the prisoner history or scheduled activities to manage their own follow up of the prisoner

As such, this program is not a cloud program, but it brings some of the important questions such as : who has access to these informations and under which authorities or boundaries

c. The third example is the medical program. It is also an issue because it is actually in a renewing/replacement process : the actual program has no link with the outside world but what about the new one ? the medical programs needs contacts with the hospitals for the importations of results such has x-rays, scans, blood analysis, etc.

That problem of regular exchange of information's brings the idea that there's maybe a need of having a specific network between the prisons and the hospitals for a secure exchange of informations.

That solution is not there only for the medical exchanges,in fact that's a way we are handling things in Belgium : making a specific network for the inmates and bring to it a lot of possibilities (in the near future VOIP telephony and videoconferencing). It's a lot easier to handle the security breaches and risk's and it's also easier to make possible new opportunities without specific risk for the Justice network.

These few examples to illustrate a few of the problems mentioned above :
- The benefits of the system should be there for everyone
- The access to data's must be organised and needs a specific legislation
- The security breaches has to be localized and handled

RISE CRIMINAL SANCTIONS AGENCY

SITUATION

Federal Prison Services of Belgium has been successfully using cloud platform based digital services solution in its prisons. In Finland, Criminal Sanctions Agency has been adopting offender prepaid payment card service that relies on Software as a Service model and runs on top of infrastructure that is run in Infrastructure as a Service mode. These are all typical use cases of Cloud service models and cloud technologies.

Adopting the cloud technologies may not be the biggest change that is entering gradually prison services but considering the service models in relation to general government ICT service models approach may bring about new kind of frame of reference in ICT services portfolio management. This development has consequences in ICT service management and procurement and this in conjunction with latest developments in European data protection legislation. On 8 April 2016 the Council adopted the Regulation and the Directive. And on 14 April 2016 the Regulation and the Directive were adopted by the European Parliament. The new European Union Data Protection legislation is being enforced as of now but allowing for 2 year transition period to get processes and agreements and ICT services within the Prison Services and within partners of Prison Services aligned. In Finland the Prison Services has implemented Prepaid Payment Card service for the Offenders where cards function in controlled manner both inside and outside the prisons. The Service is based on SaaS offering by United Kingdom based Prepaid Financial Services Ltd. In Belgium, the Prison Services has implemented PrisonCloud platform to offer digital services for the Offenders.

Business problem to be addressed:

- How cloud-based Software-as-a-Service service models change ICT services management in prison services.
- Benefits of cloud based services in prisons in practice.
- How to live with security and privacy requirements from procurement to running systems in production
- How to comply with the requirements of national and european privacy legislation on technical level
- How to prepare in advance with changing data protection legislation and keep ICT service procurement and development moving

Task Data Protection and privacy-supporting security requirements in service life cycle management

It is safe to say that most Prison Services act as registrar and the often specific legislation defines e.g. which registers it is responsible for, what is considered to be personal data, who has access to personal data, to whom the Prison Service is entitled to hand over such data and what are the data retention periods. These points for one set the basic requirements for those measures and actions that are taken while authorities review internally and externally code of conduct and goodness of data protection. This activity can be turned into processes and tangible technical tools needed to carry out the activity.

Additionally, this legislation as all national legislation follows developments in EU legislation, like the EU Data Protection Reform. The legislation changes may occur at any time and hence having some visibility on upcoming changes helps. It isn't always possible to have visibility of several years ahead as the case law changes like the Schrems case (judgement ECLI:EU:C:2015:650) made very clear. The EU Court of Justice ruling made Safe Harbor arrangement between EU and United States inadequate forcing ongoing e.g. procurement processes to review the options and requirements for data location set out in the procurement process. For example, if a service provider has been asked to comply to whole tender without possibility to negotiate after having been chosen to be the provider, this arrangement may be binding to other parties as well. In worst case, the procurement may have to be relaunched at the final stages.

This kind of event can be avoided by planning ahead and keeping in mind what are the practical means to answer following two basic questions. Firstly, have you required that the personal data must stay located within EU and secondly, if it isn't possible to keep all personal data within EU, what are the reasons of the service provider to render personal data to be handled outside of EU, e.g. to United States. The EUCJ ruling on Schrems case was a game changer for ongoing operations as well. Many authorities and private companies had to consider either starting moving personal data handling to EU area or considering negotiating bilateral model clauses that would ensure same level of data protection as EU considers adequate. EU is in process of negotiating processor for Safe Harbor, the EU-U.S. Privacy Shield and time will tell how it works in practice. One of the reasons for Data Protection Reform is to support the birth of European Digital market where data protection rules are the same regardless of which European country a company or a citizen is in. It's the same European Digital Market where public sector is functioning.

ACTION Implementation of data protection and privacy-supporting security requirements in systems

The difference between private and public clouds doesn't come into play in deciding if one should keep offenders' personal data within the national borders. Private and public clouds are rather measure of commitment to putting resources in ICT technology and ICT management. Private cloud means more commitment on building and maintaining the infrastructure and networks and additionally Offender Management Agency must take care that one of the following service models is implemented in the private cloud.

Government is responsible of protecting personal data of the Offenders. This can be done by supporting European Digital Market development and using service providers that comply on European Union legislation and requiring that personal data must stay within EU borders. The jurisdiction of the service provider and the location of data must be known and predictable at all times.

Cloud technologies are offered in form of IaaS (Infrastructure as a Service) on top of which the business process providing applications can be put or cloud technology may run behind a SaaS service (Software as a Service) that implements business processes like prepaid payment card management service, email and such. In Finland IaaS and PaaS are the service models used but it would be possible to use PaaS (Platform as a Service) as well. All of these service models can be implemented in private cloud and in public cloud.

The digital services' technical environments should rather be considered as cyber range than a corporate server or network environment as the digital services must be resilient enough to stand potential intrusive misuse attempts and those should protect consequent users from intended or unintended attacks that might put personal data at risk of data breach, impersonation or criminal activities.

As the offering for Offenders digital services widens the sortiment to software being used, rented or run in Prison Service, the attack surface on software vulnerabilities changes. Finding and patching security vulnerabilities that could be used to breach data protection should be taken into account formally. Frequently run vulnerability scanners on software and server environments and the findings mitigated in reasonable time are a good start.

RESULT

Robust and manageable digital services for Offenders can full well be based on cloud technologies. It is the service models and the national and european legislation or even global markets that set the limits where public sector ICT service management can or cannot go.

NOTES

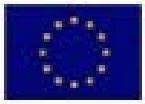
About EuroPris

The European Organisation of Prison and Correctional Services (EuroPris) is a non- political, non-governmental organisation that was founded at the end of 2011 and officially registered in the Netherlands.

EuroPris speaks for the views of prison practitioners in Europe. Membership is open to public institutions or organisations in the Council of Europe region, which provide prison or correctional services on a legal or statutory basis. .

EuroPris brings together practitioners in the prisoners´ arena with the specific intention of promoting ethical and rights-based imprisonment, exchanging information and providing expert assistance to support this agenda. The organisation exists to improve co-operation among European Prison and Correctional Services, with the aim of improving the lives of prisoners and their families, enhancing public safety and security; reducing re-offending; and advancing professionalism in the corrections' field.

Supported by the Justice Programme of the European Union



The European Organisation of Prison and Correctional Services (EuroPris),
PO Box 13635,
2501 EP, Den Haag,
Netherlands

_____

Waterside Building,
Quai de Willebroeck 33,
1000 Brussels,
Belgium

http://www.europris.org

EUROPRIS

Promoting Professional Prison Practice

www.europris.org