Cloud Computing: a new approach to securing personal information and addressing new EU regulations

Draft

Special research by Rubos, Inc. team
(We do independent research on security matters in various domains)

Prepared for DeepSec 2012 International Conference
Vienna, Austria

Authors: Rubos, Inc. Team

Presented by Mikhail Utin

Rubos, Inc.
39 Lakeview St.
Sharon, MA 02067
USA

DeepSec GmbH
Weyringergasse 30a/10
1040 Wein
Austria

1. Abstract

Security professionals across the world raise concerns about uncontrolled and insecure outsourcing of personal information to so-called "Cloud Computing Services". Such concerns of the public and legislators are reflected in European Commission Proposal "On the protection of individuals with regards to the processing of personal data and on the free movement of such data" (General Data Protection Regulation - GDPR). However, there is no research yet to explain whether the currently existing "cloud computing" services would be able to address such concerns, and what needs to be done to protect personal information in Internet-based distributed computing services.

"Cloud Computing" term originated as a marketing effort to fix financial gaps associated with Internet Bubble at the beginning of this century. Widely used, and commonly considered as a standard, mixed cloud computing models (Cloud Computing Service Model and Cloud Computing Deployment Model) are basically useless, do not reflect the nature of new Internet-based distributed computing services, and do not help in the analysis of such services' information security. In the past [1], we have identified that only one service really represents the dynamic nature of information processing in such Internet-based distributed environment. We termed it "Dynamic Hosting Service" (DHS).

In this paper, we introduce a new conceptual 9-level Personal Information Protection Security Model (PIP9) and a concept of Delegation of Trust (DoT), which explain information security related legal relationship between distributed nodes and DHS customers. Adding two layers to the standard 7-layer model (currently named as Data Protection and Data Management layers respectfully) we extend currently existing 7-layer security models to address personal information protection in Internet distributed systems. There are certain fundamental concepts in any personal information protecting regulation (e.g. data ownership responsibility, service provider responsibility, data auditing, etc.). Implementation of such concepts will guarantee the safety of personal information moving between distributed service nodes.

We consider the difference between information security implementation in our DHS model and currently used and existing "cloud services" and explain why adequate security in "cloud services" cannot be achieved.

Our analysis of personal information protection regulations (namely EU GDPR, and US NIST 800-53 R4 and HIPAA) made it possible to identify fundamental privacy controls, which we used in following design of the implementation framework. Thus, we proved that high level regulations' requirements can be implemented and will resolve major public concerns over protection of personal information moving across public Internet.

2. Introduction

A five centuries old question "To Be or Not To Be?" in our information overloaded world can be rephrased as "To Share or Not To Share?". It has been inevitably resolved to an unequivocal "To Share" the information. In our case, it is Personal Information (PI) and the way that sharing is realized raises a lot of concerns and is still in discussion.

The first problem is the legal protection of PI, as current laws do not reflect continuously evolving situation, at least in the US.

The second problem is the environment to share PI. Centralized sharing may work in some very limited cases, and even medical information cannot be organized in one "center" for such unions as EU or US. Internet has been invented as an information sharing resource and has been used since for that purpose. However, it has not been designed to serve non-public information such as PI.
The third problem is the implementation of sharing services within Internet. What is currently available as so-called Cloud Computing Services (CCS) is not ready to handle PI neither from legal nor from technology standpoints.
In the following presentation we will summarize our two year research of those problems and discuss one potential solution. However, this is still work in progress and in no way should be considered as giving final and ultimate solution. So, everybody is welcome to participate in the discussion.

2.1. Regulations, technologies and compliance – real life problems - our past research

This is our third presentation on the matters of "Information Security Triangle", not to dissimilar from the Bermuda Triangle, where we are trying to address the following:
- Laws and regulations on Personal Information protection,
- IT and security Technologies
- Real life implementation of the regulations,

These three cornerstones are usually considered as relatively independent, but are, in fact, deeply interconnected, as they affect business and security processes, and finally define security status around the globe.
In our first presentation at DeepSec 2011 [2] we discussed various laws protecting PI in the US, and how required compliance could affect small and mid-size businesses (SMBs). Implementation of compliance with Health Insurance Portability and Accountability Act (HIPAA) Security Rule [3] can easy cost tens of thousands dollars in consulting and implementation fees. However, the highest SMB business risk is associated with US government non-compliance penalties, with could be as high as $1,500,000.
Our second presentation at OWASP AppSec DC 2012 [1] considered the implementation of compliance to HIPAA Security Rule within so-called Cloud Computing Services (CCS) technology. In this presentation we:
- Analyzed well-known models of CCS: Cloud Computing Service Model and Cloud Computing Deployment Model;
- Identified that CCS is nothing more than an extension of well-known Hosting Services, which we named Dynamic Hosting Service (DHS)
- Identified trust relationship within DHS distributed computing environment,
- And, finally, introduced the implementation of HIPAA Security Rule Standards utilizing DHS.

We can summarize that compliance with the regulation in question is almost impossible within CCS:
- CCS do not provide easy to use concept and security model
- Thus, implementation of information protection in the combination of CCS models and corresponding security models is almost impossible due to extreme complexity of such mixture of models and security solutions

- Finally, due to the above, addressing high level law requirements and following implementation is practically impossible both organizationally and technically for any organization, and, in particular, SMBs.

Some of our conclusions are important for this research and the presentation, and will be discussed further below.

2.2. Next step – implementation of PI protecting laws

Based on the research and results discussed in the first two presentations, we can now move to the next step:
- Analysis of proposed EU comprehensive General Data Protection Regulation (GDPR) [4] concerning major privacy security requirements
- Analysis and comparison of privacy security controls as they are proposed in the new US NIST 800-53 Rev.4 Draft [5] with GDPR and old HIPAA [6] Privacy Rule
- Based on our research [1], we propose a new 9-Layer DHS security model, which includes new Privacy Control layer and two additional sub-layers as Data Protection and Data Management
- We consider a possibility of implementing security controls for PI protection utilizing existing CCS and security models; based on our analysis we can conclude that the mixture of CCS models, various security controls, and lack of Privacy Control layer does not permit the utilization of currently known CCS architecture to implement PI protecting processes
- Concentration on simple 9-Layer DHS security model gives us a chance to pinpoint controls for securing PI as we see requirements in GDPR and NIST 800-53 R4
- After such controls are identified, we can develop a framework giving technical background for future real life implementation of GDPR and similar regulations.

3. Regulations for PI protection

Laws protecting PI do exist on both sides of the Atlantic Ocean. They are:
- Directive 95/46/EC of the European Parliament and of the Council and new EU proposal on GDPR [4]; currently existing Directive will be repealed by GDPR
- US HIPAA with Subpart E "Privacy of Individually Identifiable Health Information" [6]
- New NIST 800-53 Rev.4 Draft [5]

Below we consider some details of these three regulations, which are important for our research.

3.1. Overview of regulations

3.1.1. EU experience, future, and details of GDPR

EU experience includes a set of historical events with definite progress and existing timeframe for comprehensive regulation:
- Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regards to the processing of personal data and on the free movement of such data, October 23, 1995. This is most likely to be the first law considering protection of personal information in such very visionary aspect as "free movement of data" while

commercial Internet finally became available in the middle of 1995
- The above Directive has been complemented by Council Framework Decision 2008/977/JHA of November 27, 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters
- Finally, on January 25, 2012 new legal framework consisting of Directive and Regulation of the European Parliament and Council on the protection of individuals with regards to the processing of personal data and on the free movement of such data (General Data Protection Regulation) has been proposed. As it is explained in the regulation [4] "This initiative is the result of the current legal framework for the protection of personal data, which lasted for more than two years and included a high level conference in May 2009 and two phases of public consultation".
The discussion in the EU member states still continues [7]. However, general inclination is to adopt the regulation.

3.1.2. US legislative experience in protecting PI
In the US, despite numerous attempts to secure PI by one blanket federal law, there is still no such law as proposed in the EU. For better or worse, all of the attempts either already stalled in various discussions, or are expected to stall [8]. The road to so much needed regulation is covered with bumps and potholes created by lobbies representing commercial interests of various industries. The most common opinion is, as expected, that such law will involve additional compliance expenses, and that it will affect businesses while in recession time.
There are two laws in the US currently in effect, and which we considered in our DeepSec 2011 presentation [2]:
- Federal regulation "Health Insurance Portability and Accountability Act (HIPAA)" requiring protecting personal health related information in its Security Rule (Subpart C) [3] and Subpart E – Privacy of Individually Identifiable Health Information [6], also known as Privacy Rule
- And state of Massachusetts so name "201 CMR 17.00 Standards for the Protection of Personal Information of the Residents of the Commonwealth" [9], which is the extension of Massachusetts General Law Chapter 93H "Security Breaches" [10].
Original HIPAA revision of 1996 had very rudimentary requirements for securing health information in general and no requirements for privacy protection. It took yet another six years until Security Rule and Privacy of Individual Identifiable Health Information appeared as they are known today (it has been revised since that in 2006 and later). So far, these parts of this federal law protect only personal health related information, and, as we mentioned above, there is no a federal law protecting PI that exists and is being used by other industries.
Massachusetts law represents distinctive attempt to be ahead of any federal regulations by enacting security standards [9] in 2009. However, as we discussed in our presentation [2], it by and large remained ignored. The reason is simple – no enforcement. It is the same reason HIPPA security requirements were ignored and not enforced until ARRA/HITECH Act [11] significantly increased penalties and US government started a program of regular preventive audits in 2011.
While US laws do not satisfy current requirements of protecting PI, some help on that matter came in a form of NIST 800-53 R.4 standard. It is not a law, nor, like MA 201 CMR 17.00, is a

mandatory security standard. It is a requirement for US government organizations and agencies to follow it. The rest of the US may consider it as advisory. However, in its new revision it has Appendix J "Privacy Control Catalog: privacy controls, enhancements, and supplemental guidance", which details privacy security controls.

3.2. Comparison of privacy protection requirements

The following is the consideration of three major regulations concerning privacy protection – EU GDPR and two of the US – NIST 800-53 R4 and HIPAA set of standards frequently referred to as a "Privacy Rule".

We only discuss the requirements related to the data movement and operations with data in distributed computing environment like DHS (or known as Cloud Computing services).

3.2.1. GDPR privacy controls

EU proposed regulation is definitely complex and covers great deal of details on Data Subject (a person or an individual), Controller (data owner) and third parties legal matters. We checked its text article by article looking for what relates to privacy protection in distributed computing environment, data movement protection, and other security and privacy requirements.

1. Article 6: Lawfulness of processing:

(a) The data subject has given consent to the processing of their personal data for one or more specific purposes;

2. Article 7: conditions for consent:

(3) The data subject shall have the right to withdraw his or her consent at any time.

3. Article 11: Transparent information and communication:

(1) The controller shall have transparent and easily accessible policies with regard to the processing of personal data and for the exercise of data subjects' rights

4. Article 14: Information to the data subject:

(b) The purposes of the processing for which the personal data are intended, including the contract terms and general conditions

(c) The period for which the personal data will be stored

(d) The existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject

5. Article 15: Right for access for the data subject:

(1) The data subject shall have the right to obtain from the controller at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed.

(a) The purposes of the processing

(c) The recipients or categories of recipients to whom the personal data are to be or have been disclosed, in particular to recipients in third countries

(d) The period for which the personal data will be stored

6. Article 16: Right to Rectification:

The data subject shall have the right to obtain from the controller the rectification of personal data relating to them which are inaccurate

7. Article 17: Right to be forgotten and erasure

(1) The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data
8. Article 23: Data protection by design and by default
9. Article 26: Processor;
(1) Where a processing operation is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organizational measures and procedures…
(2d) Enlist another processor only with the prior permission of the controller
(3) The controller and the processor shall document in writing the controller's instructions and the processor's obligations
10. Article 30: Security of processing:
(1) The controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data
(2) The controller and the processor shall, following an evaluation of the risks, take the measures referred to in paragraph 1 to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorized disclosure, dissemination or access, or alteration of personal data.
11. Article 31: Notification of a personal data breach to the supervisory authority
12. Article 32: Communication of a personal data breach to the data subject
13. Article 33: data processing impact assessment
14. Article 35: Designation of the data protection officer
15. Chapter V: Articles 40 – 45: Transfer of personal data to third countries or international organizations
Conclusion: We did not have any doubt with regard to the thoroughness of the regulation. As it states, it is not tied to any specific technology, but considers electronic processing, storage and transactions. We identified 14 Articles and 23 references within, and one entire Chapter, which, as we see them, are related to DHS utilization for all operations with PI, when Controller, i.e. Data Owner outsources collected PI data to a remote environment such as DHS (or CCS, if you prefer this term). Because of the nature of the document, some controls related to DHS implementation might be missed in our list, so we encourage readers not to consider this list as being carved in stone, but rather as ever developing mechanism to connect the law and its implementation.

3.2.2. NIST 800-53 R.4 privacy protection controls

3.2.2.1. NIST 800-53 R4 as it is

New release of NIST 800-53 standard is a definite break-through, and mostly by inclusion of Appendix J of privacy controls.
One more difference is that NIST tried to address cloud computing in security and privacy controls. Such very difficult task requires considering implementation of each control, and, in general, that is definitely not what NIST does in its standards.
Here is the quote [5, page VII]: "In most instances, with the exception of the new privacy appendix, the new controls and enhancements are *not* labeled specifically as "cloud" or "mobile computing" controls or placed in one section of the catalog." In plain language it means that

entire 800-53 standard does not have controls labeled as "cloud" related, and the Appendix J indeed uses such labels. Unfortunately, in the entire Appendix J "Privacy Control Catalog" the tem "cloud" appears only once in introductory text, and none has been found in Privacy Controls' description. So, this part of NIST's statement is simply incorrect. Concerning that "… are *not* labeled specifically as "cloud"" means a makeup for inability to introduce security and privacy controls related to "cloud computing".
Below, we are fixing NIST's attempt to identify controls in Catalog J, which are applicable to securing PI in DHS.
The standard breaks privacy controls in 8 categories of 25 controls total. In our list of 13 controls we provide the category, the abbreviation for controls, and a short description of how a control works in DHS environment.

3.2.3.2 Analysis of privacy protection controls list
These are abovementioned 8 categories:
AP – Authority and Purpose
AR - Accountability, Audit and Risk Management
DI – Data Quality and Integrity
DM – Data Minimization and Retention
IP – Individual Participation and Redress
SE – Security
TR – Transparency
UL – Use Limitation

It was sometimes difficult to identify whether a control relates to DHS processing implementation. Original NIST description, as we mentioned above, does not contain anything suggesting implementation in a distributed computing environment like DHS.
We added one column to the initial NIST information to identify parties participating in DHS data transition and manipulation - Data Owner (DO) and Service Provider (SP). As expected, both Data Owners and Service Provides are involved in implementation of each of 13 controls.

ID	Privacy Control	Description	Relates to
AR-1	Governance and Privacy Impact	Governance and Privacy Program (PP): required a PP document and appointed official as Privacy Officer	DO & SP
AR-2	Privacy Impact and Risk Assessment	Requires a document of risk assessment, including risks caused by DHS to DO	DO & SP
AR-3	Privacy Requirements for Contractors and Service providers	Requires identifying roles and responsibilities of service providers; it goes beyond current commonly used service agreements adding privacy to security controls	DO & SP
AR-8	Accounting of Disclosures	Keep an accounting of disclosures (date, nature, purpose, etc.) and retain accounting records for 5 years or lifetime; DO should provide such	DO & SP

		information to the person if requested; the information exists outside of DO premises somewhere in DHS (SP) distributed environment	
DI-2	Data Integrity (DI) and DI Board	The DO should guarantee the data integrity; however, for the data on DHS premises, the SP should guarantee that together with DO	DO & SP
DM-2	Data Retention and Disposal	PI retention time is identified by DO, but retention procedures for all time spectrum, including a maintenance schedule, are implemented by SP; the same applies to the disposal procedures	DO & SP
IP-1	Consent	It is a legal record, which authorizes operations with PI, and should reside within SP services together with PI	DO & SP
IP-2	Individual Access (IA)	This is a right of a person, which is to be implemented via DO access to the person's PI, or directly to SP resources handling PI; such access is required for operations like redress below	DO & SP
IP-3	Redress	Based on the above IA control; it includes all "redress" comprising operations as view, change, delete, etc., plus the dissemination of changes done to PI via SP resources to all users of the individual's PI either in the same DHS or in others; the record of PI users should be kept together with PI on SP resource	DO & SP
SE-1	Inventory of Personal Identifiable Information	DO should establish, maintain and update an inventory of programs and systems using PI; the same applies to the SP, where PI actually resides and the programs and systems run; SP should maintain such inventory for all its DOs	DO & DP
SE-2	Privacy Incident Response	Required are Privacy Incident Response Plan and, and according to it, Response Team; both organizational requirements are applicable to both DO and SP; however PI incidents should be investigated by SP, reported to DO, and DO should take care of reporting to persons and organizations according to applicable regulations	DO & SP
TR-3	Dissemination of Privacy Program Information	It is applicable to both DO and SP privacy programs which required by AR-1 control; programs should be made available to all individuals and organizations associated with both DO and SP operations	DO & SP
UL-2	Information Sharing	DO shares information as follows: - entering in agreements with SPs describing covered PI and purposes PI may be used - monitoring, audit and train staff on authorized use of PI	DO & SP

		- evaluates new instances of sharing PI with SPs Monitoring and audit pertains to such security controls as log management, audit trail records, etc.; such controls are usually implemented as Security Information and Event Management System functioning on SP premises; both DO and SP should be aware of security control information originated by monitoring and auditing systems	

Table 1: NIST 800-53 R4 privacy controls

3.2.2.2. NIST privacy controls conclusion:
1. It was finally possible to identify the group of 13 privacy controls, which should be used in DHS PI protection implementation.
2. Looking through the above list, we can see that some controls are related to "legal" or "compliance" group and others are "data", or say "technical" controls. We will discuss that in our privacy protection model below.
3. We see that each of 13 controls involves both Data Owner and Service Provider reflecting the fact that security is shared responsibility, and that "outsourcing" to DHS (or CCS if you prefer using this term) does not mean outsourcing the responsibility and participation in all processes. Outsourcing implementation requires having on both sides highly interconnected documents and processes.

3.2.3 HIPAA 45 CFR 164 Subpart E – Privacy of Individually Identifiable Health Information

This is a set of 15 standards, which has been written around 2006 with focus on a legal side of the procedures and documents reflecting US healthcare system, and completely independent of the technology. We identified just three standards that could be related to electronic PI processing with a possibility of residing in DHS infrastructure. Next to each standard is a reference to the associated control in NIST 800-53 R4 standards from the table above:
- 164.524 - Access to individuals to protected health information (IP-2)
- 164.526 – Amendment of protected health information (IP-3)
- 164.528 - Accounting of disclosures of protected health information (AR-8)

Conclusion: NIST set of PI protection controls in p. 3.2.2 supersedes old HIPAA standards as it relates to the controls implementation in DHS. To become useful, HIPAA set of controls should be reviewed considering electronic data storage, processing and transaction, including legal part of the requirements as well.

3.2.4 Correlation of EU GDPR and NIST privacy protection controls
The table below represents a correlation matrix between NIST 800-35 R.4 privacy controls and EU GDPR. While NIST gives us more concrete set of controls, it is important to identify if our list of NIST controls correlates with GDPR propositions which, in most cases, are very general. GDPR list is taken from p.3.2.1.

NIST ID	NIST Privacy Control	GDPR Article	GDPR Control

AR-1	Governance and Privacy Impact	11(1) 30(1) 35	The controller shall have transparent and easily accessible policies with regard to the processing of personal data and for the exercise of data subjects' rights. The controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks. Designation of the data protection officer.
AR-2	Privacy Impact and Risk Assessment	30(2)	The controller and the processor shall, following an evaluation of the risks, take the measures referred to in paragraph 1 to protect personal data.
AR-3	Privacy Requirements for Contractors and Service providers	26(1)	Where a processing operation is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organizational measures and procedures.
AR-8	Accounting of Disclosures	14	Information to the data subject.
DI-2	Data Integrity (DI) and DI Board	30(2)	The controller and the processor shall … protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorized disclosure, dissemination or access, or alteration of personal data.
DM-2	Data Retention and Disposal	14(c) 15(1d)	The period for which the personal data will be stored. The period for which the personal data will be stored.
IP-1	Consent	6(a), 7(3)	The data subject has given consent to the processing. The data subject shall have the right to withdraw his or her consent.
IP-2	Individual Access	14(d)	The existence of the right to request an individual access from the controller.
IP-3	Redress	14(d) 16 17	Rectification or erasure of the personal data concerning the data subject. Right to rectification. Right to be forgotten and erasure.
SE-1	Inventory of Personal Identifiable Information	23 33	Data protection by design and by default. Data processing impact assessment.

SE-2	Privacy Incident Response	31 32	Notification of a personal data breach to the supervisory authority. Communication of a personal data breach to the data subject.
TR-3	Dissemination of Privacy Program Information	11	Transparent information and communication.
UL-2	Information Sharing	14(b) 15(1a) 15(1c) 26(2d) 26(3) 40 - 45	The purposes of the processing for which the personal data are intended, including the contract terms and general conditions. The purpose of the processing. The recipients or categories of recipients. Enlist another processor only with the prior permission of the controller. The controller and the processor shall document in writing the controller's instructions and the processor's obligations. Transfer of personal data to other countries or international organizations.

Table 2: Comparison of NIST 800-53 and GDPR privacy controls

Conclusion: We see here that NIST list very well correlates with GDPR requirements, while in some cases we've seen multiple instances of EU regulation requirements corresponding to one NIST control. That, of course, was expected and relates to general nature of GDPR, its legal structure, and the purpose of the document. In a few cases we used entire GDPR chapter reference instead of pointing to a particular article, that is, again, because of the nature of the document.

3.2.5 Conclusion to the comparison of privacy protection regulations

We considered three regulations as providing a background for the identification of privacy protection controls in DHS distributed computing environment. Each document has its own purpose, and is not aligned with our goal. However, our analysis has shown that there is a very strong correlation between privacy controls. In fact, NIST standards supersede old HIPAA, and represent concrete outcome of EU GDPR general requirements. Thus, in the following consideration of the implementation of privacy controls in DHS environment, we will refer to the NIST list (p.3.2.3.2) as a basis for PI protection controls set.

4. Cloud Computing Services as they are and new security and privacy protection model for Dynamic Hosting Service

The above laws guaranteeing free movement and protection of PI, are written to be technology independent, but with new information technologies in mind. For instance, GDPR [4] refers to them and considers as a foundation for free PI movement and sharing. What kinds of technology did we get during last thirty years? There are: LAN, WAN, Internet,

WLAN/WiFi, datacenter, hosting, and finally Cloud Computing. The latter is considered as a universal distributed computing environment, which basically replaces whatever we had before. Based on the opinion of CCS providers and numerous institutions, including US government, such services are the only one possible technology for free data movement and sharing. We need to return to our analysis of that assumption, which we did for OWASP Appsec DC 2012 [1].
Then we can proceed with proposing a new security model for protecting of PI in a distributed computing environment.

4.1. Cloud Computing misconceptions.

4.1.1. Terminology

How we name a technology is going to profoundly impact its life. That is exactly what happened with "Cloud" Computing (CC). We know Analog Computing, which was the beginning of computing, next - Digital, Multiprocessor, Mainframe, etc., and each identifies which computational method is being used. So far, a "cloud" cannot compute, it is neither a means nor a method of computation.
Current Wikipedia definition of Cloud Computing is "*… the delivery of computing as a service rather than a product…*". That points to the essence of CC: it is a service delivering data to a computational point and back to the user in a dynamic manner, i.e. moving computation point between various resources like datacenters.
The history of CC Services (CCS) goes back to the Internet Bubble, which required a lot of datacenters hosting a rapidly growing number of web sites. After the Bubble has burst, such datacenters became useless, or used just for a fraction of their power, and Amazon.com in 2006 came up with the idea of hosting applications in the same way as web hosting. But what is the difference between hosting http protocol application, or any other? Thus, new marketing label "Cloud Computing" has been designed to sell old hosting service to customers under new marketing label.
Cloud Computing as pure marketing term has been used in the same way as Intranet. Old product is on sale under completely new and sophisticated label to attract customers and financing.

4.1.2. Models

However, just renaming is not enough. Marketing campaign works well if there is some sort of a science behind it. And CCS got two well-known models: Deployment Model and Service Model. There are three NIST-800 (144. 145 and 146) publications [12, 13, 14] considering such models, and seemingly an infinite number of all kinds of other related publications as well. We decided to do some analysis of these models to clarify what they are.

4.1.2.1. CC Service Model

Descriptions of Service Models (SM) could be found, for instance, in Wikipedia [15], NIST publications [12, 13, 14], and other sources. However, we simply see that:
1. "Infrastructure as Service" (IaaS) – quote: "providers offer computers, as physical or more often as virtual machines, and other resources" it is well-known to us as Hosting Service, nothing more, nothing less

2. "Platform as a Service – PaaS" is actually an Application Programming Interface (API) to a hosting service, which may include runtime environment, databases, development tools, etc.
3. "Software as a Service – SaaS" is an application hosting environment consisting of various applications – email, office productivity, games, etc.
Considering that CC services in question have dynamic nature (service can move between infrastructure nodes), we can view "Cloud Computing" as simply Dynamic Hosting Service utilizing the terminology ("Dynamic" and "Hosting Service") which has been used way before the cloud computing initiative.
The following table represents an interpretation of Service Models in simple and understandable hosting services terms:

CC SM	As Hosting Service	Corresponding Dynamic Hosting Service
IaaS	Hosting Service	Dynamic Hosting Service (DHS)
PaaS	API Hosting Service	Dynamic API Hosting Service (DAPIHS)
SaaS	Application Hosting Service	Dynamic Application Hosting Service (DAHS)

Table 3: Relationship between CC Service Model and Hosting Services

We used **old** terminology to describe the evolution of hosting services. Here we show that there is no need to invent and use "CC Service Model"; all processes can be more easily explained using traditional "Hosting Service" term, and its extensions.

4.1.1.2. CC Deployment Model
Service Model has been discussed, and helped us to confirm again that CC is a **service** – it is about **data** freely moving across organizational borders. Then, why do we need "Deployment Model" (DM) which is about **computing resources** and provides no explanation of how **data** moves or the exact meaning of **service** to the customer.
The following is the consideration of essence of each of the existing models referenced in NIST 800-144 [12].
There are so far four DMs:
1. "Public Cloud" – quote: "*...It is owned and operated by a cloud provider delivering cloud service to customers*". Basically, "owned and operated by a provider" implies Hosting Service infrastructure, or as we used to say "Hosting Service" or "Outsourced Hosting". Therefore, we are making a reference to a service again, meaning that there is a supporting infrastructure. However, do we really need a new model of "Public Cloud" to explain what we know since year 2000 as "Hosting Service"?
2. "Private Cloud" – quote: "... *is operated exclusively for a single organization. It may be managed by the organization or by a third party, and may be hosted within the organization's data center or outside of it.*" If Private Cloud is comprised from customer's equipment – it is just well known "Local Network" or organization's "Wide Area Network". If two kind of networks – LAN and WAN – are operated by an external entity, it is called "outsourcing". So, again we can easy explain new "Private Cloud" in old and easily understood terms – LAN, WAN, or Outsourced Infrastructure (LAN, WAN, etc.) and such well

established terms are much easier to comprehend and to use than "Private Cloud"
3. "Community Cloud" – quote: "… *the infrastructure and computational resources are exclusive to two or more organizations that have common privacy, security, and regulatory considerations, rather than a single organization.*" This definition is vague in a legal context. Two pictures NIST provides [12, Fig.5 and Fig.6, pp. 4-10 – 4-12] do not help to identify legal relationship either. If a "community" comprising organizations connect to a cloud on one-to-one basis (i.e. each having separate agreement with a provider) then it is just discussed above "public cloud", i.e. Hosting Service. If NIST is trying to explain that a "community" has only one agreement with a provider, then it is legally incorrect. A "community" is not a legal entity and cannot sign an agreement, unless organizations within form such entity legally. In this case, we again see one-to-one relationship, and "public cloud" – Hosting Service. So far, since Roman time, there was no legal practice of signing service agreement by a vaguely defined "community" with a service provider. Such act should be done by each legal entity individually.
4. "Hybrid Cloud" – it is a composition: "*… more complex than the other deployment models, since they involve a composition of two or more clouds (private, community, or public). Each member remains a unique entity, but is bound to the others through standardized or proprietary technology that enables application and data portability among them.*" As far as services are concerned, this model is a composition of LAN/WAN (private cloud), and a hosting service (public cloud). "Community", as we discussed above, is either a hosting service or cannot legally exist. The Table 4 below summarizes our consideration of "Deployment Models"

CC DM	What is it concerning services?
Public Cloud	Hosting Service
Private Cloud	LAN, or WAN, or Outsourced Infrastructure (LAN, WAN, etc.)
Community Cloud	Legal Nonsense or Hosting Service
Hybrid Cloud	Interconnected LAN, or WAN, or Hosting Service, or Legal Nonsense

Table 4: Interpretation of CC Deployment Model in well-known components and services

We do not think that "Deployment Model" will help in any way in consideration of free movement of data, basically between LAN/WAN (Data Owner) and a hosting application service. In short – it is useless.

4.1.3. CC models' consideration conclusion
The goal of our consideration of CCS was to identify if there is any value in this concept, and if its models would help us in the implementation of privacy controls.
1. Cloud Computing Service Model utilizing IaaS, PaaS and SaaS models is an overly sophisticated presentation of a hosting service; our concept of Dynamic Hosting Service and its extensions (DHS->DAPIHS->DAHS) is based on a traditional hosting service model; it is simple and explains interconnection relationship in Internet computing environment as connection between various hosting services and processes transmitting PI.
2. Cloud Computing Deployment Model is irrelevant to the consideration of interconnecting and utilizing PI processes; in fact this model represent only the **infrastructure layer**, which

can be easy explained in the old terms of LAN, WAN, outsources LAN/WAN, and hosting service. In some cases Deployment Model even contradicts legal aspects of service agreements. Our DHS model is very useful, because it represents PI-moving interconnected processes on higher abstraction layer thus avoiding unnecessary details and confusions over infrastructure implementation.

4.2. Is CCS going to help in an implementation of PI protection?

We discussed CC misconception with the purpose of deciding if it could be useful when we move from a list of privacy controls to the implementation. Vague and complex models with no real technical value cannot help is our case. Laws are complex, implementation is complex, and any extra complexity will make the implementation unmanageable.

Do we really need CC Deployment Model representing **infrastructure** layer? How the **infrastructure works** and **secured** is not the concern of **PI protection**, which is implemented by **different protection layers**. The only model we really need is a service level abstraction model like DHS representing distributed hosting **services**. Then **data** utilized by such service, which is PI, will be protected **by other layers of privacy controls**.

Do we need CC Services Model? No, we can easy use DHS or its extensions to explain precisely which service is used. In general, we need only DHS itself, because, according to NIST list (p. 3.2.3.2), the only control concerned about which application and the extension of DHS is used is SE-1 "Inventory of Personal Identifiable Information".

Numerous CCS security models do not include what is our core concern – protection of PI in a form of privacy controls. In most cases they are a derivation of 7-layers OSI model like, for instance, one of the most complex Cloud Computing Security Model depicted below (see Pic.1). While such general model includes components of Cloud Model, Security Control Model and Compliance Model, it completely misses a component of PI Protection. As we see in the picture below, Cloud Model (on the left) does not refer to any privacy protection controls either.

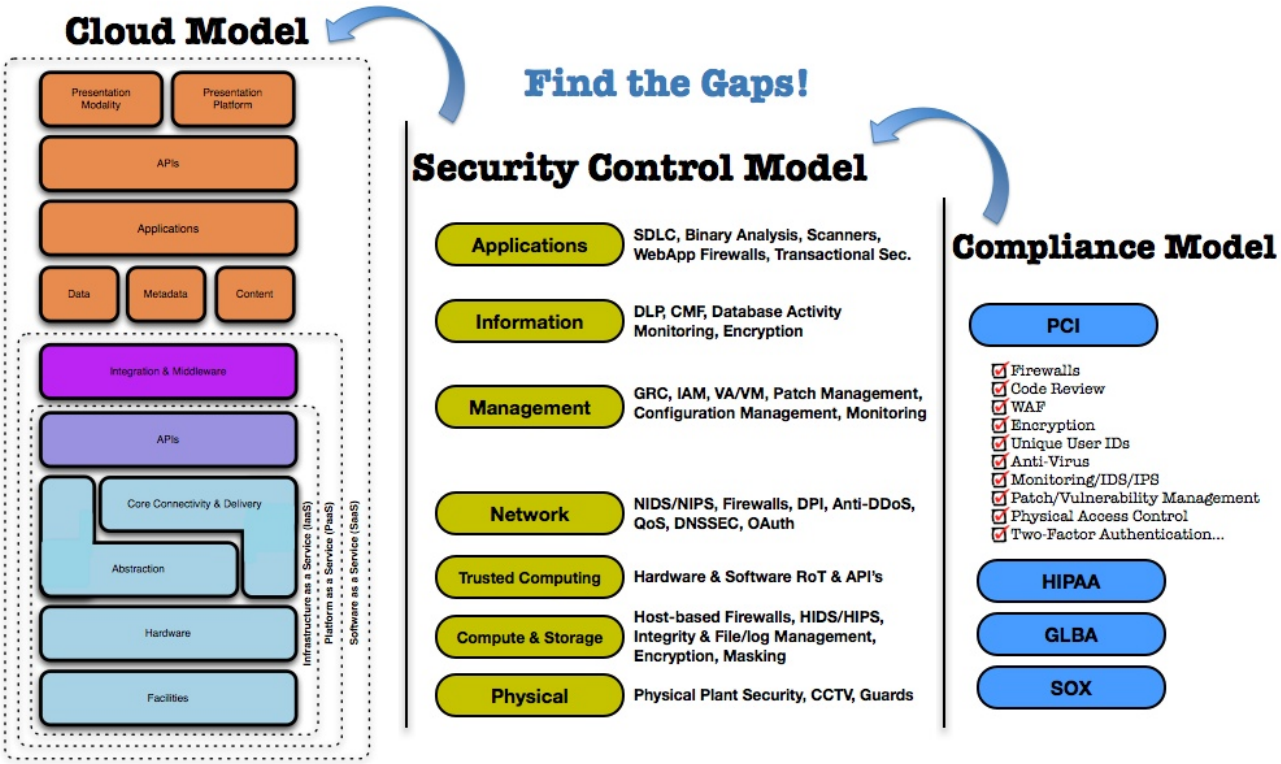
When we talk about Dynamic Hosting Service, we completely understand that such PI concerned service should include PI protection components above regular security controls. The following paragraph explains our PI protection model.

4.3. PI Protection 9-layer Security and Compliance Model (PIP9 Model).

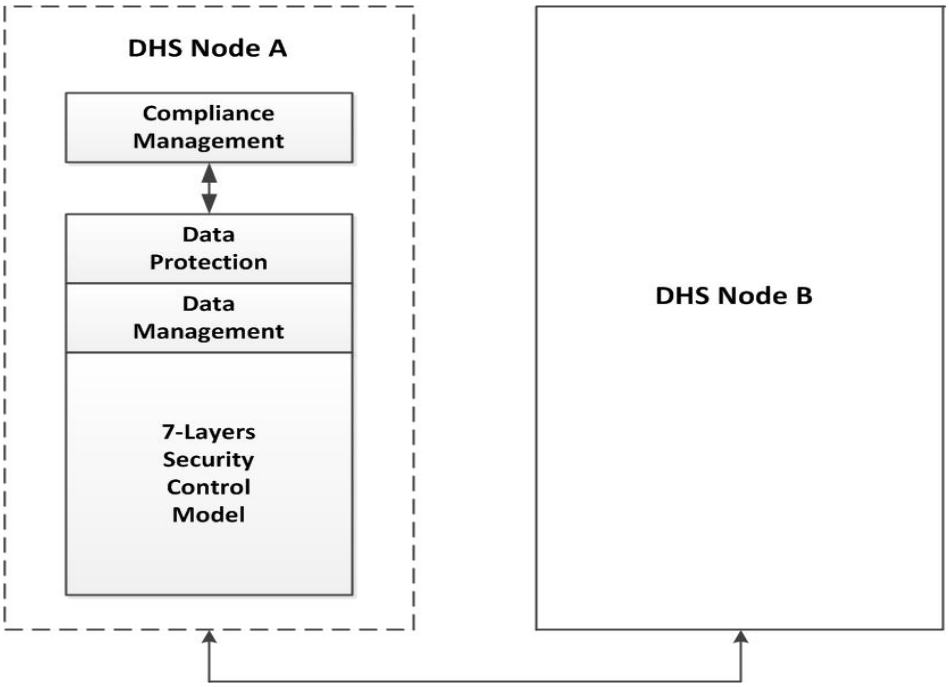
As we have mentioned before, the concept of 7-layer OSI model is used widely as information security model, including CCS [16], but it does not include privacy protection controls. To fill out such conceptual gap we introduce our high level PI Protection 9-layer Security and Compliance Model (PIP9 Model). The model is presented on Pic.2 and shows two communicating DHS nodes. Each node has 7-layers traditional Security Control Model, which protects the node infrastructure. On the top of those 7 layers we added two privacy protection layers of Data Protection (DP) and Data Management (DM), and Compliance Management (CM) layers. DM layer (eighth) provides necessary controls for manipulation and movement of PI. DP layer (ninth) consists of various controls providing confidentiality, integrity and availability of PI.

DM layer protocols and processes require various control information data structures, which identify the status and the location of PI in a distributed environment, and we include them

in DM as well.
CM layer is universal and controls compliance with all related regulations and internal policies. Therefore, we place it above DM and DP.
PIP9 PI protection model is represented on Pic. 2, and the Table 5 explains the relationship between NIST 800-53 PI controls and layers of our model.
There are 5 controls composing Compliance Management Layer, 3 of Data Protection, and 5 of Data Management. It should not be a surprise that DP has only three controls. The majority of these 13 controls focus on data management processes and compliance requirements. The latter, in general, delines all controls in DP and DM layers.



Pic. 1: Typical Cloud Computing 7-Layer Security Control Model



Pic.2: PI Protection Security (PIP9) Model

ID	NIST Privacy Control	PI Protection Model
AR-1	Governance and Privacy IWempact	CM
AR-2	Privacy Impact and Risk Assessment	CM
AR-3	Privacy Requirements for Contractors and Service providers	CM
AR-8	Accounting of Disclosures	DM
DI-2	Data Integrity (DI) and DI Board	DP
DM-2	Data Retention and Disposal	DM
IP-1	Consent	DM
IP-2	Individual Access	DP
IP-3	Redress	DM
SE-1	Inventory of Personal Identifiable Information	DM
SE-2	Privacy Incident Response	DP
TR-3	Dissemination of Privacy Program Information	CM
UL-2	Information Sharing	CM

4.4. PIP9 Model conclusion.

Privacy controls are, in fact, information security management processes rather than what we used to see as security controls. Certainly, modern security controls like Vulnerability Management, Security Information and Event Management (SIEM) system, even Malware

Protection, are complex processes as well, but privacy controls are much more of data and documents management rather than data and documents security protection. Even Privacy Incident Response is more of organizing the response and reporting than incident investigation using information security techniques. The latter we already have within 7-layers Security Control Model. Such difference in privacy and security controls is essential, and our model reflects that.

1. We considered CCS as they are well-known through various sources, including three official US Government NIST standards. Unfortunately, market driven approach affected most of the associated industries and security professionals, and NIST's usually balanced position as well. We cannot use vague models and recommendations if we want to address such challenge as EU GDPR. We proposed our simple to understand Dynamic Hosting Services Model that gets right to the point. It includes two extensions for API and application implementation.
2. Our high level presentation of processes in Internet computing environment such as DHS running on interconnected nodes permitted us to introduce a new 9-layer PI Protection and Compliance (PIP9) Model. Such logical and common sense approach is confirmed by easily fitting NIST 800-53 privacy controls in our model.
3. Our DHS and corresponding PIP9 models give us a change to consider a framework of PI protection implementation in Internet computing environment in the following chapter.

5. PI Protection Implementation framework.

Our limits of the implementation are DHS model, PIP9 model, and 13 PI protecting controls from NIST 800-53 R4. We need to stress here that these NIST controls, which we picked up from the original set, address very common EU security community written or verbal concerns over Access, Accounting, Retention, Integrity, Consent, and Redress of PI. Additionally, our list includes Inventory and Incident Response controls.
In our proposed framework we will consider the implementation of three groups of privacy controls, which we identified above, and which correspond to our model layers: Compliance Management, Data Protection and Data Management.
We would like to mention here one fundamental security principal, which is very often forgotten while always being clear in any security regulation: outsourcing of security controls and privacy protection functions from Data Owner to a Service Provider does not mean outsourcing responsibility to control security and privacy. It means that Data Owner should be aware of what is happening and where it happens, have an ability and readiness to act, and being responsible for what happened. That has been mentioned in p.3.2.2.2 as the outcome of analysis of privacy controls, which is presented in NIST Privacy Control table (Table 1).

5.1. Compliance Management (CM)

Compliance Management layer represents the legal part of PI protection implementation, which, according to our PIP9 model, has universal character and is above our DP and DM layers and general security controls (7-layers in our model). Compliance is a general requirement by any regulations including EU GDPR, US HIPAA Security and Privacy Rule,

SOX, PCI DSS, and others. Thus, CM layer identifies corresponding controls and processes.

5.1.1. CM layer implementation

This layer consists of 5 controls as follows.

5.1.1.1. Governance and Privacy Impact

It has two major requirements – Privacy Program (PP) and assignment of Privacy Officer. PP is the main document identifying complete set of privacy controls (13 in our case). Both Data Owner (DO) and service provider (SP) should have a version of PP.

PP should include 13 privacy controls and either be amended by consideration of all 7-layers applicable security controls, or having them considered in an attached security program.

When we talk about multiple DHS providers, which may be distributed around the world, we mean PP compatibility, which in [1] we proposed as Delegation of Trust concept. Service provider guaranties appropriate PI protection level, and in return, the data owner delegate its trust to handle appropriate operations with PI. Logically, service provider's protection level cannot be lower that data owner requires in its PP. We see guarantees as PP at each side and binding service agreement.

Logically simple, but not in practice yet, two-side DoT becomes much more complex when we expect participation of multiple service providers in a "free movement" of PI. Either each DO should have DoT process with each SP (an agreement, a contract and certain legal process as well), or each SP should have similar DoT process with all other SPs, or it should be a certification process, which would simplify DoT to just signing service agreement with any participating service provider. Such provision exists in GDPR in very general form.

EU GDPR resolves that in its Article 39 to the case of "Certification" as "1. The Member States and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors."

From our experience, PP should be a structured document with Policy, Procedures and Guidelines levels specifying each control up to the implementation details in Guidelines. That would guarantee a functional and useful document.

Privacy Officer is a standard requirement in any security or privacy related regulation. This person is responsible for all privacy protection duties and problems.

5.1.1.2. Privacy Impact and Risk Assessment

Both DO and SP should do risk assessment on their side considering all 7-layer security controls and privacy protection controls from the group DP. As we mentioned above in 5.1.1.1, it should be a privacy program and a security program as well. And each should consider associated risks.

There is a specific risk, which should be assessed and addressed in SP's PP. Because SP provides PI protection, and 7-layer security and infrastructure management as well, such services require administrative level access to all system components. Therefore, SP's personnel have unrestricted access to DO PI and other data in processing and transmission. It seems that we pioneered pointing to such risks, which should be assessed together with "internal" risk. The latter is a standard risk assessment practice, which in distributed

environment should be amended by abovementioned "border" risk. From our experience discussing "border" risk with a few internet infrastructure and CCS providers, they never considered such risk as existing, and therefore never assessed it.

5.1.1.3. Privacy requirements for contractors and service providers.
We already discussed that in two paragraphs above - in privacy program and risk assessment paragraphs. Current security and privacy regulation consider both DO and SP equally responsible for security and privacy. SP should have the same or better level of protection as DO, and be responsible for compliance in the same way as DO is.
However, based on our experience, the most of service providers are completely unaware of that and think of themselves as compliant as long as they encrypt data transmission and database! They do not realize that compliance is a complex process addressing both legal and technical sides. And the legal side is usually least addressed.
Delegation of Trust concept is the cornerstone of this control as regulating legal ground of cooperation with contractors and service providers in matters of privacy protection.

5.1.1.4. Dissemination of Privacy Program Information
In our Internet era this requirement is pretty simple to implement on both DO and SP side. Privacy programs can be published on a web site hosted by SP for its program or for both DO and SP. They should be maintained and reviewed according to the regulatory requirements, and usually on yearly basis.

5.1.1.5. Information Sharing
Information sharing is permitted only if legal entities – DO and SP - are in formal agreement, which we identified as Delegation of Trust, and which should include at least privacy program at each side and a contract.
Such contract should identify the purpose of PI sharing, basically – services provided by SP. Each service is associated with privacy protection controls, and very likely, with 7-layer security controls as well. Thus, each high level service, for instance, moving PI from one DHS node to another, should have downfall consideration of all controls involved.
Monitoring and audit of authorized use of PI are standard controls, which are technically implemented inside of 7-layer security controls model. Here, on the CM level, we should identify all instances of PI and all of the permitted operations. Considering a possibility of international PI exchange, such permissions on certain operations should include "country permission code", which finally makes a matrix of services, permissions and national limitations.
However, limitations may include other than just "country" matter, and that brings us to complex "matrix of limitations", which should include all variations of possible PI utilization. EU GDPR considers such matter in great details.
Concerning monitoring and audit, such controls are usually implemented as a Security Information and Event Management (SIEM) system. However, not each of SIEM has such standard feature of providing audit trail logs management, which in most cases is a database transactions monitoring and logging system. Where such control is going to be implemented? As we consider DHS multi-node distributed system, then it should be implemented in each DHS node inside 7-layer security controls implementation. However, it

is not only for SP to know what is going on, but DO is responsible for working with SIEM as equally responsible party for security monitoring. We discussed this principle above.
Evaluation of new PI instances before sharing means a complete cascading process of reviewing permitted operations along with implementation of privacy and then security controls. Our abstract PIP9 model describes PI protection layers as independent from 7-layer security controls, but it may not be always the case. For instance, implementation of PI confidentiality via encryption may change from country to country according to national laws.

5.2. Compliance Management conclusion
1. Having internal and service provider's privacy program, security program, and risk assessment is the responsibility of PI data owner.
2. In case of distributed network of DHS providers, Delegation of Trust should be implemented by having either guarantees from all service providers, or an independent certification of providers needs to be implemented.
3. Risk assessment should include data owner internal risk assessment, service provider's assessment, and contained in the provider assessment, there should also be an assessment of risks invoked by the provider's services to the data owner.
4. Our experience shows that service providers are deeply unaware of the meaning of compliance and of the privacy and security requirements, including legal part as above [p. 5.2(1),5.2(2) and 5.2(3)].
5. Each new kind or instance of PI sharing involves complete assessment of privacy controls and, possibly, of security controls as well.
6. Such controls of sharing as monitoring and audit of PI usage involves implementation of complex and costly SIEM-class system at each service provider's premises. It is tough to answer the question of how the data owner will deal with SIEM, and potentially with a few SIEMs if PI moves between distributed DHS.
7. Privacy Officer should be appointed to supervise activities as above [p. 5.2(1) – 5.2(6)] and monitor security status.

5.3. Data Protection (DP)
Per NIST opinion that we share, PI data protection, that is ninth level per our PIP8 model, is to be implemented mostly by utilizing security controls of 7-layer security control model. However, both DO and SP should be aware how to use security controls to protect PI, and what to do in a case of privacy violation.

5.3.1. Data Integrity (DI) and DI Board
Data integrity is enforced by such security controls as access monitoring and, more generally, by utilizing SIEM systems. Responsibility of DO is to be aware of DI requirement, knowing security controls used to monitor data integrity, and what to do in a case of data integrity is violated, i.e. privacy incident, which is considered below.
DI Board is a management body, which handles PI compromise cases, officially handles security and privacy incidents, see p.5.3.3 below. It is usually comprised of company officials.

5.3.2. Individual Access (IA)

Individual access is universal control, which is widely used by Data Management (DM) group for various operations with PI. It is implemented utilizing security controls mechanism such as Access Control List (ACL). PI "free movement" means that a person's PI may travel across Internet independently from the original application and DHS node. In this case it would require transmitting with it an "individual" ACL, rather than the applications "group" ACL. Considering permissions to access for various organizations across EU and beyond, such "individual" ACL can grow and become very complex.

5.3.3. Privacy Incident Response

It is based on security control as well as processes related to incident prevention, response and reporting, which described in great details in NIST 800-61 [17]. The difference with standard incident response is that PI compromise should be reported to government authorities and affected individuals as well. Standard reporting criterion is the number of personal records compromised. Therefore, if security process identified PI records compromise on SP premises, it should be reported to DO Privacy Officer, who will handle the case further together with DI board above (p.5.4.1).

5.4. Data Protection conclusion

1. Data Protection controls are implemented utilizing associated security controls of 7-layer Security Control model. The management of both DO and SP, and involved in resolution of PI compromise, should be aware of regulatory requirements how to handle such incidents, including reporting to authorities and affected individuals.
2. EU GDPR considers various and complex aspects of sharing and access to PI data, and such requirements should be reflected in Individual Access implementation (IP-2 NIST 800-53 R4 control). In case of PI data is moving over Internet between DHS processes, access information (like ACL) should move together with data, and be updated according to changing access requests and permissions.

5.5. Data Management (DM)

This group represents controls responsible for supporting free movement of data between distributed DHS processes. Whether a transfer of data is dictated by internal status of the infrastructure (failure or overload of a node, etc.) or by a requests for data, the transfer functions are implemented by a connection oriented communication protocol. Such protocol provides assurance that DM operation has been finished and the status of PI in distributed nodes infrastructure is always known

DM group of controls guarantee that PI's free movement does not mean uncontrolled release of information. Thus, DM controls should permit accounting of PI movement and therefore knowing the current location of a given PI record, where its copies are, and what is the status of PI (active, deleted, etc.).

Conceptual character of GDPR requires that the access to PI should be implemented on per individual record bases and the transfer of records across multiple nodes rather than collecting all PI records in one central repository. The latter seems impossible to implement considering EU principals of cooperation as well.

Each PI record should have supporting data structures, which we name "descriptors". Such descriptors save and release necessary privacy control information. We already discussed one

of descriptors – ACL – while discussing the access to PI record.
In the following paragraphs we proposed DM implementation according to principals outlined above.

5.5.1. Inventory of Personal Information

NIST quote: "… the organization establishes, maintains and updates an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining or sharing personal identifiable information; the update in this case should be on a change basis; such inventory may contain name and acronym of each system identified, the types of personal identifiable information in that system, classification of level of sensitivity of each type of personal identifiable information as combined in that information system."
Therefore, the following information should be collected and maintained as the system inventory:
- It should be a list of systems and programs operating with PI
- Identification of each system location and name
- Inventory information update should happen immediately (on change basis)
- The inventory should keep all types of PI in each system.

Such inventory collection process can be accomplished, as we described above, via a connection-oriented high level protocol seamlessly delivering very important system information. Another question is where to keep this information. After some analysis we concluded that de-centralized static model will fit NIST identified requirements and our model of distributed DHS nodes. It means that each node is considered as "parent" for PI originally created in it, and will keep and maintain all PI inventory information originated at it. Respectfully, if PI is released from the parent node, all operations as transfers, release, copying, deletion, modification, and involved systems should be registered in parent's inventory, which we named Parent Status Descriptor (PSD).
The following explains how our PSD inventory model works in the implementation of other privacy controls.

5.5.2. Consent

Consent is a legal document authorizing disclosure of PI to a list of authorized persons (individuals, organizations, etc.). In our case of electronic PI records, the consent should be in an electronic form as well. The consent record should have at least three parts – consent text, Individual's Record (IR), and Authorized Persons List (APL) who may receive this PI. IR and APL uniquely identify the consent and its scope, and together named as Consent Descriptor (CD). There should be a CD for each PI originated in the node. We do not consider here a case when PI is derived from other PI records, which is more of a legal case than a technical one.
CD is checked when a request for PI is received to identify if requesting party is in APL.
If consent is revoked, CD is changed to reflect this status.

5.5.3. Accounting of disclosures (AD)

Disclosure of PI means its release to an authorized person. Therefore, the following activities should take place:

- Consent verification
- Disclosure to the identified person based on received request
- Registration of the disclosure.

Consent verification is described in p.5.5.2.
Release of PI to authorized party is the transfer to the requesting system (DHS), and is based on the system identification and location (see p.5.5.1). The transfer is done via high level communication protocol, as it is described in p.5.5.1 as well.
Finally, the transfer should be registered in this PI Status Descriptor (PISD), which is a part of inventory PSD. Each transfer adds corresponding record in PISD, thus creating a trail record for the PI.

5.5.4. Data Retention and Disposal (DRD)
DRD is one of cornerstones of PI protection. Disposal of PI is the final operation of data retention, and technically is the same as "deletion". We expect that each type of PI may have different retention period, and thus each type of PI of each individual should have its own PI record.
Data Retention and Disposal Descriptor (DRDD) record should be created synchronously with the PI record. It should contain at least timestamps of creation, change and disposal, and may be next verification date. All this information is saved in DRDD, which is a part of inventory PSD.
There are two major operations in DRD process: retention period verification and disposal. If PI was not released from parent node that is checked in PISD/PSD, then retention period is verified in DRDD, and if it has expired, PI will be disposed. This change of PI status should be registered in PISD/PSD.
If PI has been released to another node, its retention period can be verified locally at its parent node in PISD/PSD. If disposal is required, such request is to be sent to the node holding the PI. When disposal is finished, PI change status will be registered in parent node PISD/PSD.

5.5.5. Redress
This control permits an individual to access his/her PI record and change it. Accordingly, all other released copies should be changed as well and parties using them should be informed of the change.
If the individual's PI is located in the parent DHS node, the redress process involves the following:
- Consent verification, when the individual name and/or ID is checked in the Consent Descriptor
- Verification in inventory Parent Status Descriptor (PSD) that there is only local PI copy
- Changing PI record
- Registration of the change in inventory PSD

All these processes controls were described above.
In case there are copies of individual's PI has in other DHS nodes, the verification in PSD will identify where such copies are located, and a request for change and notification of the change will be sent to PI-sharing parties. After receiving a confirmation from a party, the status of associated record in PSD will be changed.

5.6. Data Management conclusion

1. We considered an implementation of all NIST Data Management privacy controls in our distributed DHS environment. We suggested using a high level connection oriented protocol to transfer PI and control information between nodes.
2. We concluded that both the nature of GDPR and EU states' cooperation principals require decentralized storing of PI and information associated with it, and that can be done utilizing DHS nodes infrastructure.
3. Decentralized PI and control information should reside in each DHS node, which thus is considered as "parent" node for PI originated in it and all PI control information. The latter resides in an information repository called "Parent Status Descriptor".
4. Repository of all control information is an inventory keeping information about DHS distributed infrastructure, and information about all operations with PI and where is has been released. Parent Status Descriptor information is changed upon conclusion of each DM operation.
5. It was possible to design implementation framework utilizing proposed solution for all NIST Data Management group controls, thus proving that all standard operations with PI can be implemented within our models and the framework.

6. The Research Conclusion

1. We have shown that our approach of replacing Cloud Computing services by Dynamic Hosting Service model works. Instead of using sophisticated combination of useless models, we concentrate on one Dynamic Hosting Service high level model, which is simple and easy to use.
2. We analyzed three major regulations concerned with PI protection – EU General Data Protection Regulation, and US NIST 800-53 R4 Privacy Control standards and HIPAA Privacy Rule. We identified that complex and thorough GDBR requirements can be mapped to NIST controls which provide the ground for privacy controls implementation framework.
3. We proposed a new 9-Layer PI Protection Security Model (PIP9), composed of what is considered a standard 7-layer Security Control Model and two additional layers of Data Protection and Data Management representing PI protection. The model also includes a Compliance Management layer.
4. We divided 13 NIST Privacy Controls is three groups corresponding to our PIP9 model, and considered implementation of controls utilizing proposed models and principals. It was possible to develop the implementation framework, which covers our list NIST privacy controls and required operations with PI, thus implementing high level GDPR requirements in our framework.

7. References:

1. Mikhail A. Utin, Daniil Utin. Private Information Protection in Cloud Computing – Laws, Compliance and Cloud Security Misconceptions, OWASP AppSec DC 2011, April, 2012.
2. Mikhail A. Utin, Daniil Utin. US Experience: Laws, Compliance, and Real Life – When everything seems right but simply does not work; DeepSec 2011, Vienna, November, 2011.
3. 45 CFR Subtitle A, Subchapter C, Part 164, Subpart C – Security Standards for the

Protection of Electronic Protected health Information
4. Proposal for a regulation of the European parliament and of the Council on the protection of individuals with regards to the protection of personal data and on the free movement of such data (General Data Protection Regulation); COM(2012) 11 final, Brussels, 25.1.2012
5. National Institute of Standards and Technology (NIST), US Department of Commerce, NIST Special Publication 800-53 Revision 4: Security and Privacy Controls in Federal Information Systems and Organizations, February, 2012.
6. 45 CFR Subtitle A, Subchapter C, Part 164, Subpart E – Privacy of Individually Identifiable Health Information.
7. Review: National Concerns over the proposed EU Data Protection regulation, Infosecurity magazine, August 6, 2012; http://www.infosecurity-magazine.com/view/27399/national-concerns-over-the-proposed-eu-data-protection-regulation/
8. GovTrack.us: S3333 - Data Security and Breach Notification Law http://www.govtrack.us/congress/bills/112/s3333/text
9. Code of Massachusetts Regulations: 201 CMR 17.00: Standards for protection of Personal Information of Residents of the Commonwealth - http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf
10. MGL Chapter 93H – Security Breaches - http://www.malegislature.gov/Laws/GeneralLaws/PartI/TitleXV/Chapter93H
11. Public Law 111-5, February 17, 2009 - http://www.gpo.gov/fdsys/pkg/PLAW-111publ5/pdf/PLAW-111publ5.pdf
12. Guidelines on Security and Privacy in Public Cloud Computing, NIST Special Publication 800-144, December 2011.
13. The NIST Definition of Cloud Computing, NIST Special Publication 800-145, September, 2011.
14. Cloud Computing Synopsis and Recommendations, NIST Special Publication 800-146, May 2012.
15. Wikipedia: Cloud computing - http://en.wikipedia.org/wiki/Infrastructure_as_a_service#Service_models
16. Wikipedia: Cloud computing security model - http://www.google.com/search?q=cloud+computing+security+model&hl=en&tbo=u&rlz=1W1DKUS_en&tbm=isch&source=univ&sa=X&ei=5lWoULnvBPTv0QGB9IHAAw&sqi=2&ved=0CGYQsAQ&biw=1236&bih=564
17. Computer Incident Handling Guide, NIST Special Publication 800-61 R1, March, 2008.

Mikhail A. Utin, CISSP, PhD, Rubos, Inc.
Email: mikhailutin@hotmail.com
Daniil Utin, MS
Email: dan777@gmail.com