

Privacy in the Cloud Environment



[1]

Dr Kaniz Fatema
COINS summer school 2015

Privacy? Do we care

Some people do, may not to
others' privacy at least their
own...





Mark Zuckerberg in court with neighbour over 'personal privacy deal'




Facebook founder is in dispute

It's sad yet ironic that Zuckerberg has to go through great lengths to protect his privacy. Yesterday news broke that Facebook was removing yet another privacy feature. Soon, even people who wish to remain hidden from Facebook searches will have no choice but to be searchable on the social network.

-Business Insider 11 Oct 22013

He made his fortune by persuading over a billion people to share their lives online, but when it comes to protecting his own privacy Mark Zuckerberg appears to spare no expense: the Facebook founder has reportedly spent \$30m (£18.8m) buying four houses that surround his own home in California.

- TheGuardian 11 Oct 2013

An aerial satellite view of a residential neighborhood. The image shows several large houses with swimming pools, surrounded by dense green trees. Two white callout boxes with black backgrounds and white text point to specific houses. The first box, labeled 'Zuckerberg home', points to a large house with a dark roof and a swimming pool. The second box, labeled 'Voskerician property', points to a house with a light-colored roof and a swimming pool. The text '© Google Street View' is visible in the bottom left corner, and the number '6' is in the bottom right corner.

Zuckerberg home

Voskerician
property

Any real life experience on
privacy threat?

Do you think you are doing
enough to protect your personal
data ?

Time to wake up

Amazing mind reader reveals his 'gift'

<https://www.youtube.com/watch?v=F7pYHN9iC9I>

What does privacy mean to you?



Privacy = secrecy?

[2]

What is privacy?

Privacy is a fundamental human right which was first defined as “**the right to be left alone**” by the United States Supreme Court Justice Louis Brandeis and Samuel Warren [3].

Some other views of privacy are – **the protection of an individual’s independence, integrity, dignity, secrecy, anonymity, solitude, protection against intrusion into an individual’s personal life or affairs** [4].

Professor Roger Clarke [5] has defined the different dimensions of privacy – **Privacy of person**, which is also referred to as 'bodily privacy', is concerned with the integrity of an individual's body such as blood transfusion without consent, compulsory provision of samples of body fluids and body tissue and so on.

Privacy of personal behaviour relates to all aspects of behaviour such as sexual preferences and habits, political activities and religious practices.

Privacy of personal communications relates to privacy of communications using various media without being monitored. This is sometimes referred to as 'interception privacy'

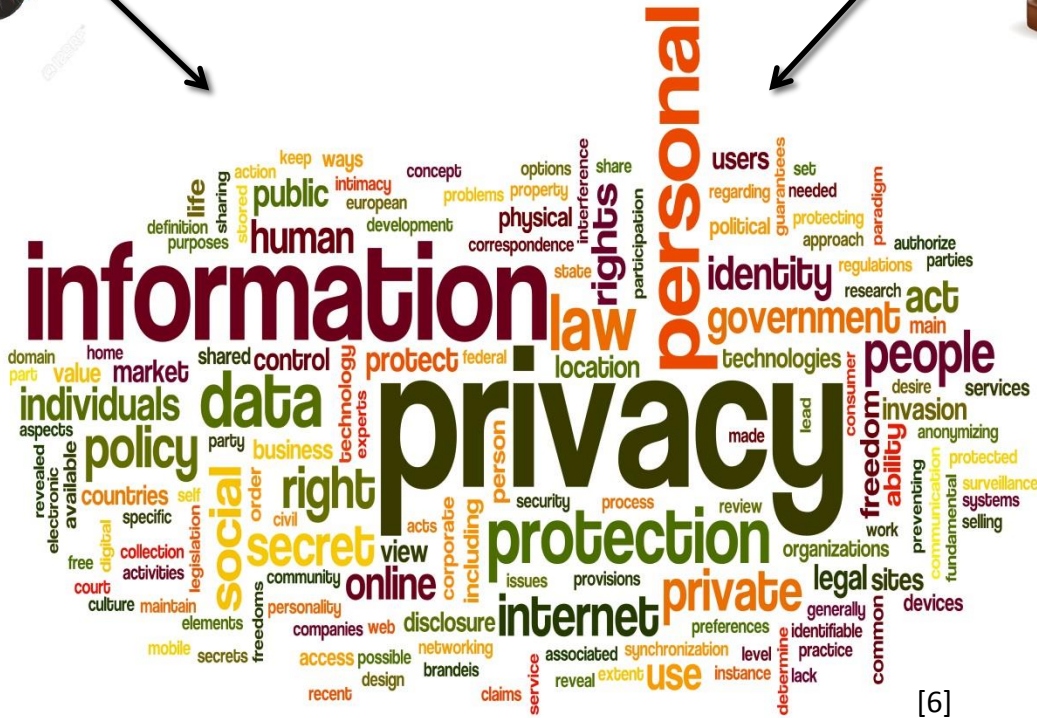
Privacy of personal data is also referred to as 'data privacy' and 'information privacy', relates to controlling whether or how personal data can be gathered, stored, processed or selectively disclosed.

What is privacy?



[7]

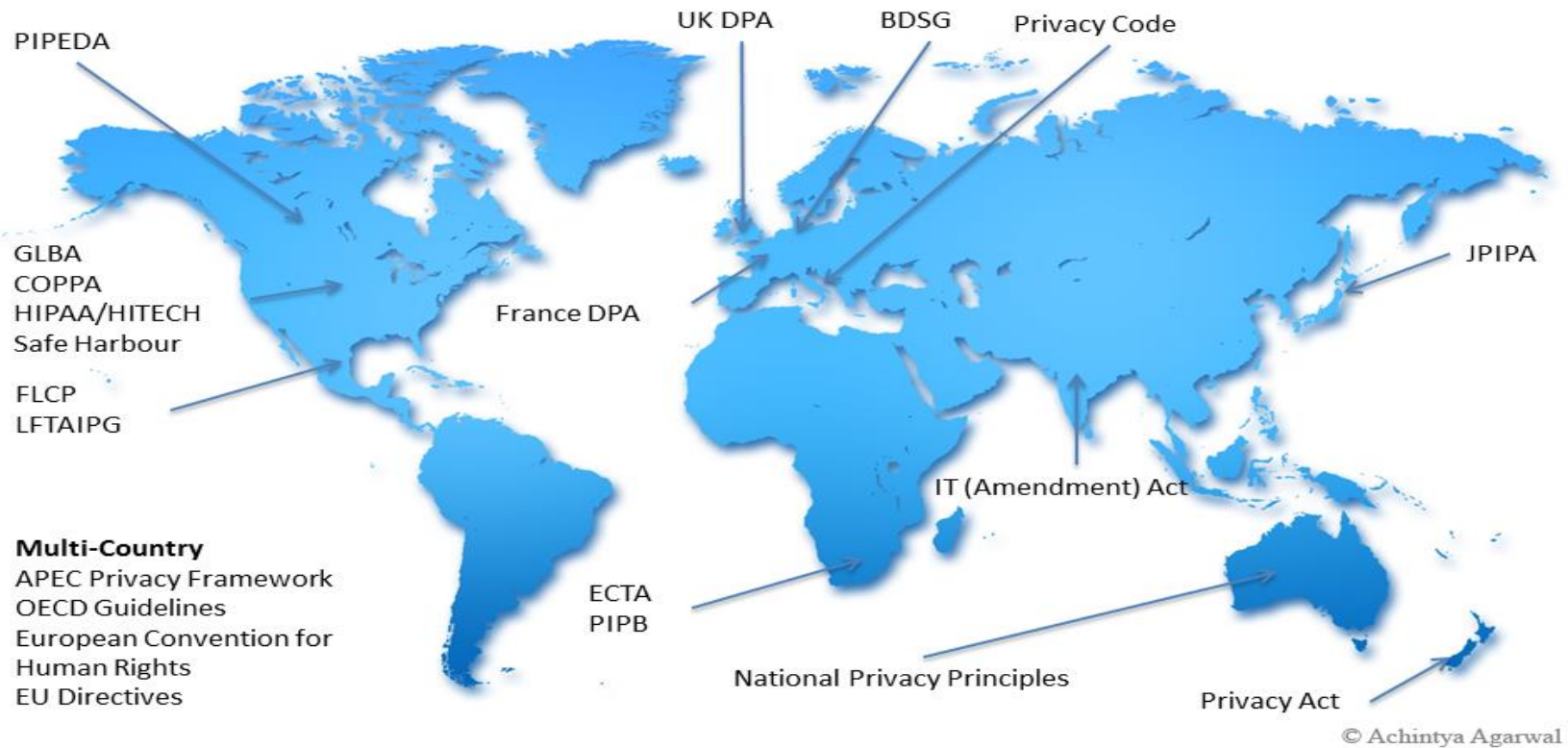
[8]



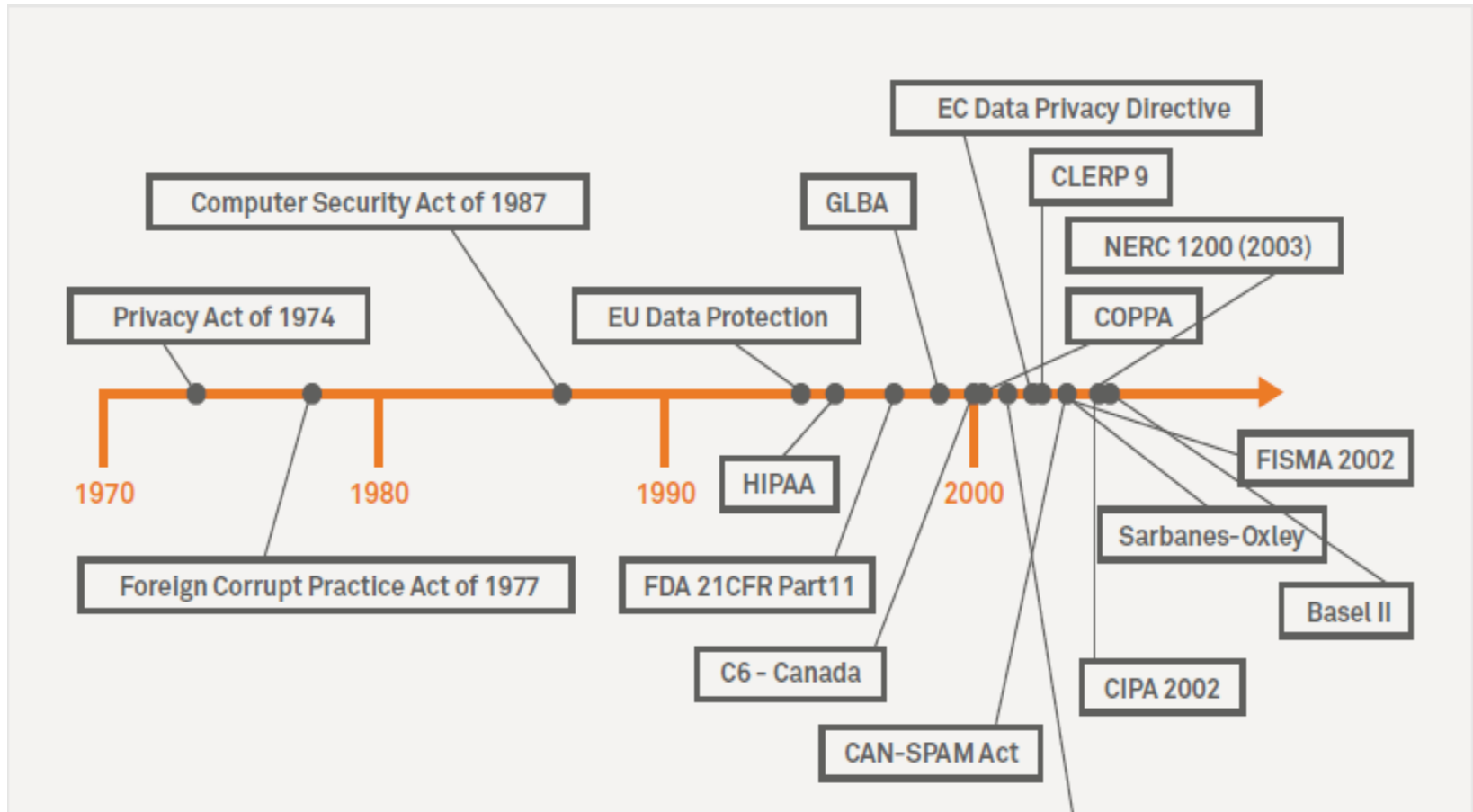
[6]

Privacy is a legal right ...

Global Laws on Privacy & Data Security



Privacy is a legal right ...



By January 2015 the total number of countries with data privacy laws has increased by over 10% to 109. [10]

The privacy policy principles

Common privacy policy principles on privacy laws around the world

Australian Law Professor Graham Greenleaf finds ten elements common to all four international privacy instruments (the OECD Guidelines, Council of Europe Convention, EU Data Protection Directive, and the APEC Privacy Framework):

1. Collection - limited, lawful and by fair means; with consent or knowledge
2. Data quality – relevant, accurate, up-to-date
3. Purpose specification at time of collection
4. Notice of purpose and rights at time of collection
5. Uses limited (including disclosures) to purposes specified or compatible
6. Security through reasonable safeguards
7. Openness to personal data practices
8. Access – individual right of access
9. Correction – individual right of correction
10. Accountable – data controllers accountable for implementation

Comparison of Global Data Privacy regulations

	APEC	OECD	DSCI Privacy Framework	EU DPD (95/46/EC)	EU e-Privacy Directive 2002/58/EC	EU e-Privacy Amendment 2009/136/EC	UK DPA	Germany BDSG	France Data Processing Act	Canada PIPEDA	India ITAA 2008 Rules	Australia Privacy Act (NPP)	Japan PIPA	US GLBA	US HIPAA	US HITECH Act Rule	US Health Breach Notification	US Safe Harbour
Accountability	✓	✓	✓	✓			✓	✓	✓	✓	✓				✓			✓
Notice	✓	✓	✓	✓			✓	✓	✓	✓	✓	✓	✓	✓				✓
Choice & Consent	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓				✓
Collection Limitation	✓	✓	✓	✓			✓	✓	✓	✓	✓	✓	✓					
Use Limitation	✓	✓	✓	✓			✓	✓	✓	✓	✓	✓	✓	✓				✓
Retention Limitation				✓			✓	✓	✓	✓		✓						
Disclosure	✓		✓				✓	✓	✓	✓	✓	✓	✓	✓				✓
Access & Correction	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓		✓				✓
Security	✓	✓	✓	✓			✓	✓	✓	✓	✓	✓	✓	✓				✓
Data Quality	✓	✓	✓	✓			✓	✓	✓	✓	✓	✓						✓
Enforcement	✓			✓			✓	✓	✓	✓		✓		✓				✓
Openness	✓	✓	✓	✓			✓	✓	✓	✓	✓	✓						
Anonymity											✓							
Transborder Data Flow	✓	✓		✓			✓	✓		✓	✓							✓
Sensitivity				✓	✓		✓	✓		✓	✓							✓
Breach Notification						✓		✓						✓	✓	✓		
Identifier Limitation											✓							
Source Identification							✓											

© Achintya Agarwal

What is personal data?

According to the Data Protection Law information can be personal data if any of the following conditions is true-

- If the information (in conjunction with other information) can identify a living individual.
- The information relates to an identifiable living individual.
- The information is obviously about a particular individual; e.g. medical record, criminal record.
- The information is linked to an individual.
- The information informs or influences actions or decisions affecting an identifiable individual.
- The information has biographical significance in relation to the individual.
- The information focuses on the individual as its central theme.
- The information has impact (or potential to impact) on an individual.

Privacy VS Security



[12]

Privacy VS Security

Privacy Criterion Information Security	Reporting of processing	Transparent processing	“As required” processing	Lawful basis of data processing	Data quality conservation	Rights of the parties involved	Data traffic with countries outside EU	Processing personal data by processor	Protection against loss and unlawful processing
Confidentiality			X				X	X	X
Availability									X
Integrity					X	X		X	X

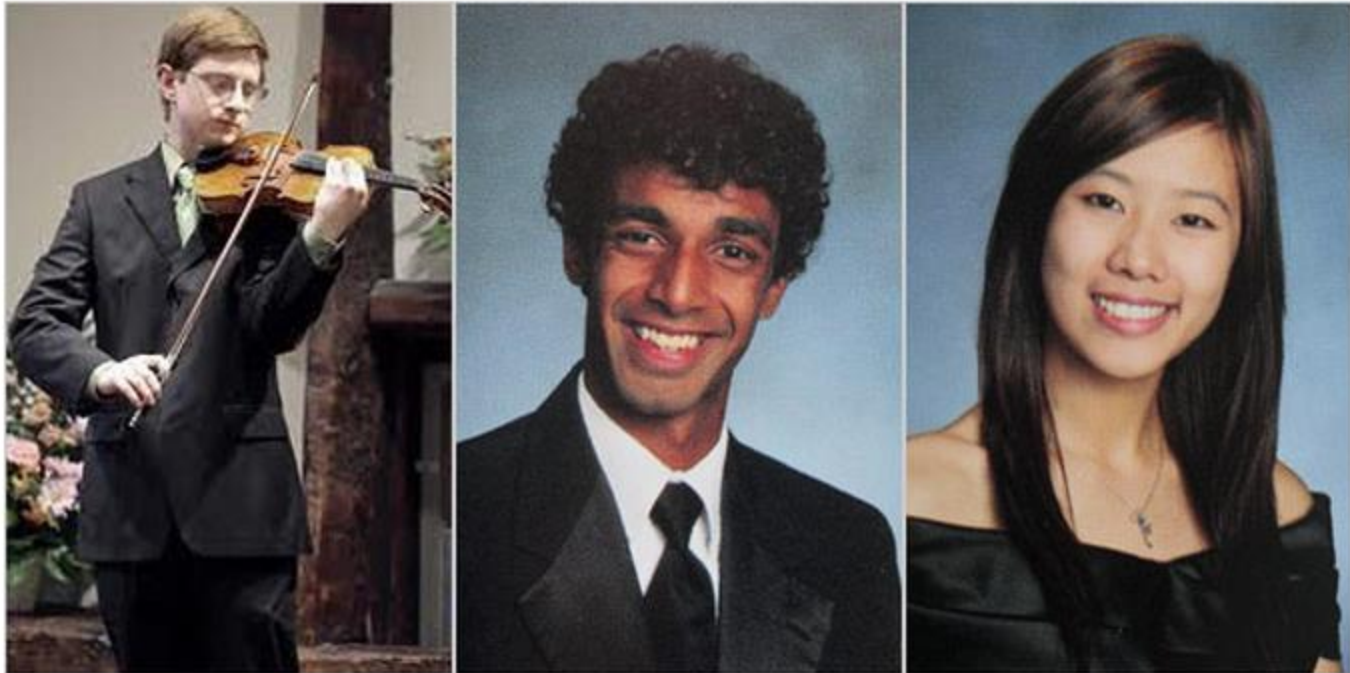
Time for brushing up your
awareness on privacy

Privacy breach payoff



N.Y. / REGION | Private Moment Made Public, Then a Fatal Jump

By LISA W. FODERARO SEPT. 29, 2010



Tyler Clementi, left, is thought to have committed suicide, days after he was secretly filmed and broadcast on the Internet. Mr. Clementi's roommate, Dharun Ravi, center, and another classmate, Molly Wei, have been charged in the case. Center and right, The Star-Ledger

[14]

Privacy breach payoff

There can be a number of negative consequences that can be occurred due to the lack of or poor privacy protection. For example –

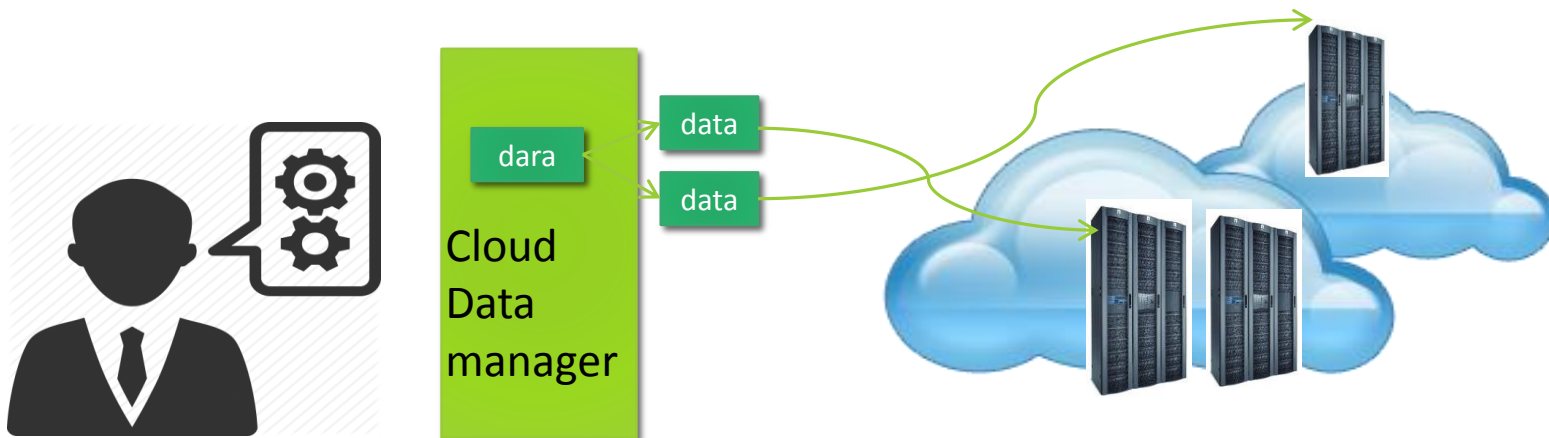
- Harm to the person whose data are used or disclosed inappropriately.
- Become Victim of identity theft
- Damage to an organisation's reputation.
- Financial loss.
- Loss of business due to negative publicity.
- Violation of privacy laws with the possibility of paying huge penalties.
- Destruction of confidence and trust in the industry.

Cloud introduces new privacy challenges?



- Data are shared among multiple providers. Multiple providers can have different terms of service, policies and location.
- Lack of organizational control over employee- more possibility of insider threats.
- Service provider typically do not have control over the physical location of the data.
- Possibility of leaving multiple copies of the same data- leading to more data management problems and possibilities of disclosure.
- Identity management for a number of providers.
- Conflicting laws from different jurisdictions.

Consumer VS Provider perspective



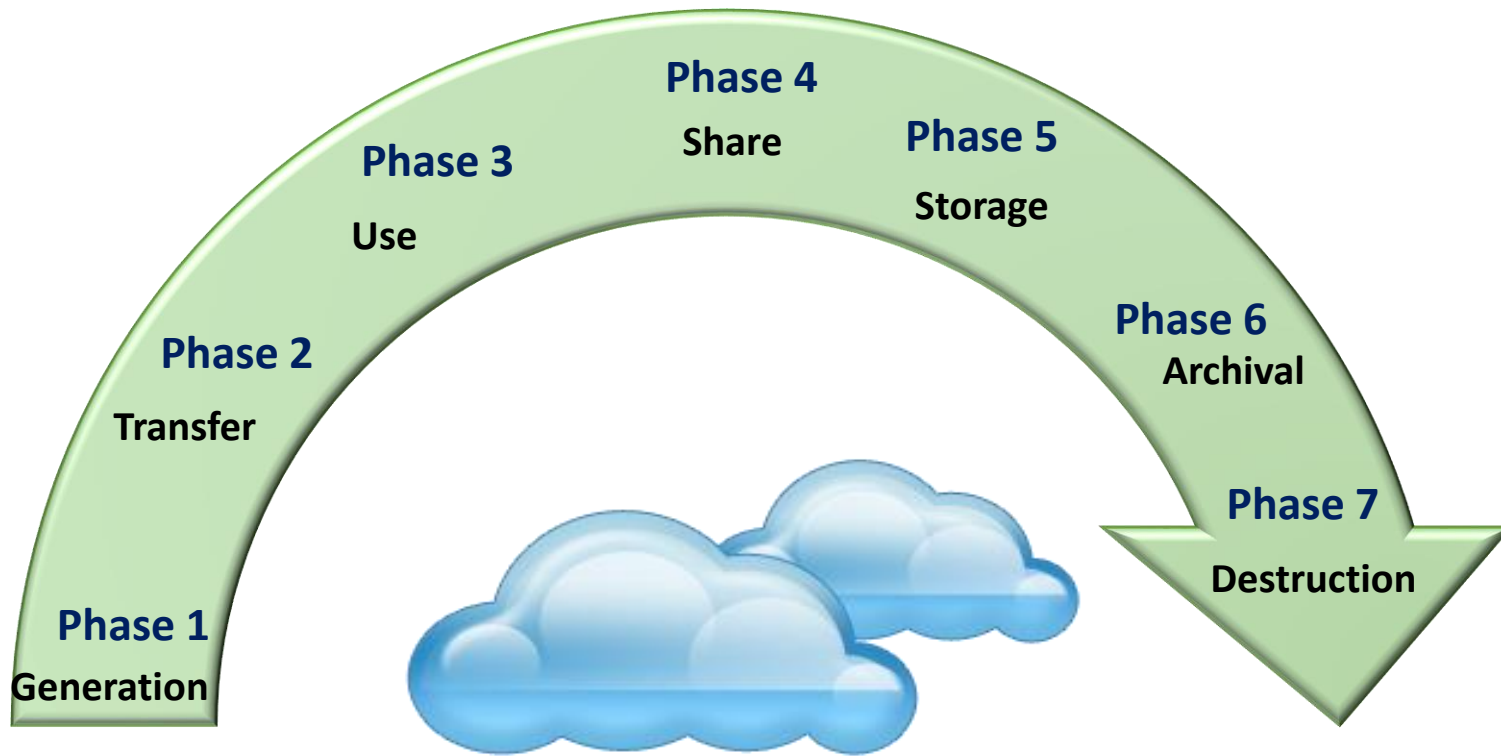
Minimizing risk by cloud consumers

1. Be aware of what you are sharing.
Use service that require less information.
2. Use encryption.
3. Be wise about Wi-fi.
4. Avoid over-sharing personal information in social network.
5. While choosing a cloud service check their privacy policy.
6. Be aware of where is your data going and how it is going to be processed and shared.



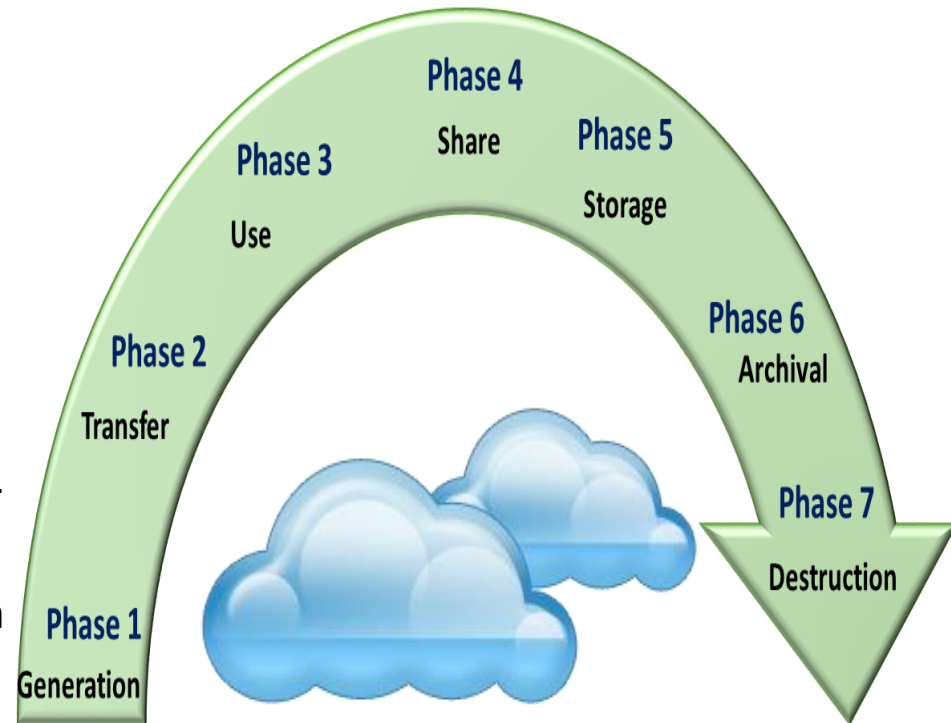
[15]

Data life cycle in the Cloud



Phase 1: Data generation

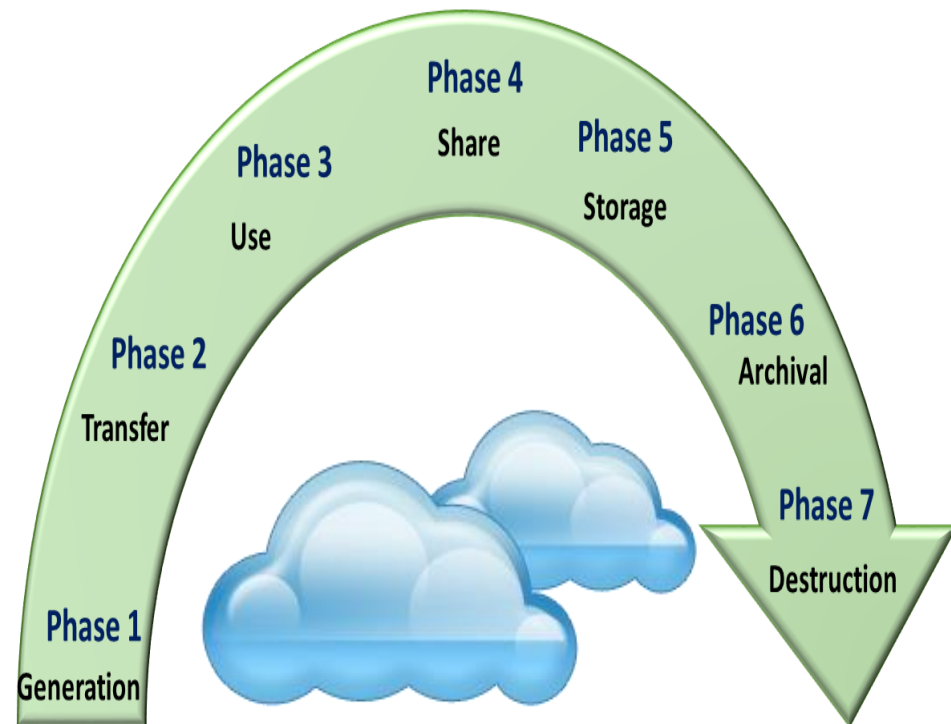
1. Data collected about individuals, e.g., during registration process for a service.
2. Data can be created by themselves, e.g., file or picture uploaded by individuals.
3. Data can be gathered from the context, e.g., time of using a cloud service, location and device used for the service.
4. Inferred data deduced from the own data and monitoring data, for example, a person's credit score from his transaction records.



Phase 1: Data generation

Things to consider at this stage

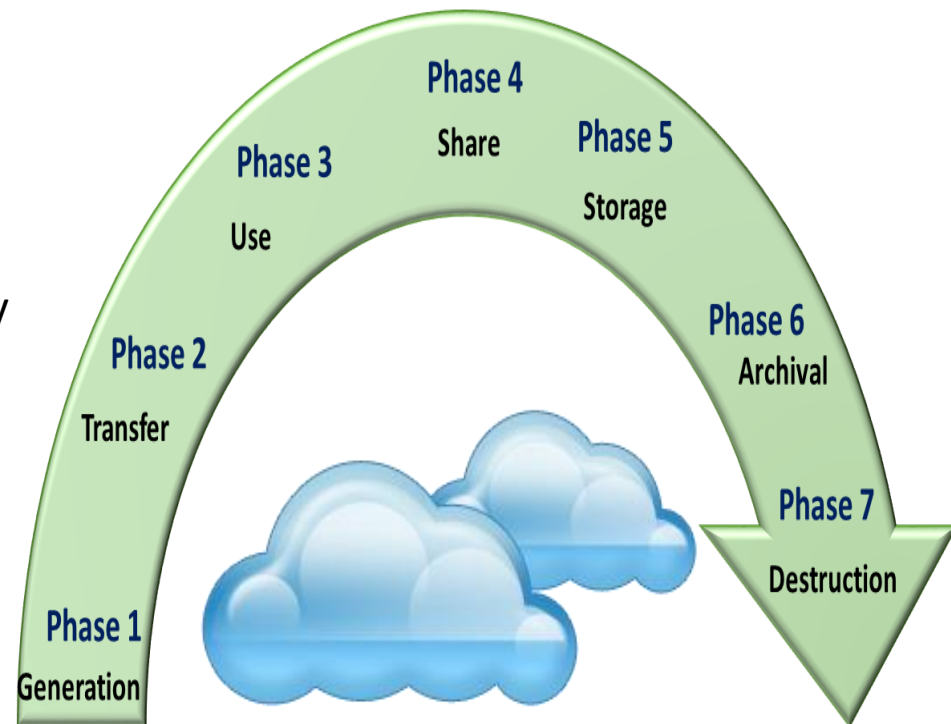
1. Data ownership
2. Data classification
3. Collection Limitation
4. Purpose specification
5. Consent



Phase 2: Data transfer

Things to consider at this stage

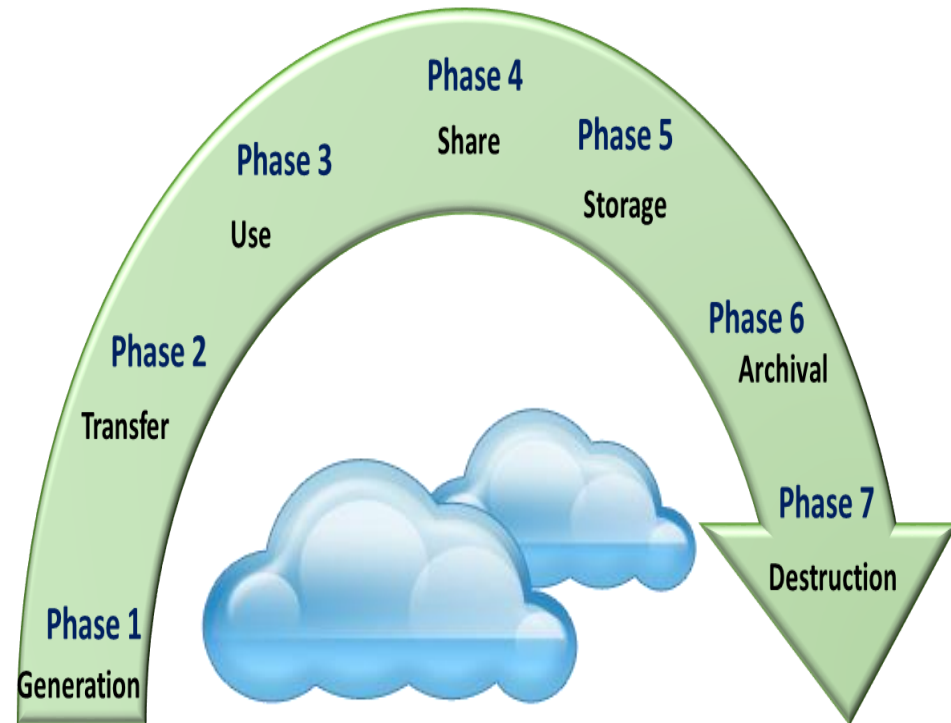
Encryption: While transferring via public network encryption is necessary to protect confidentiality and integrity of data.



Phase 3: Data use

Things to consider at this stage

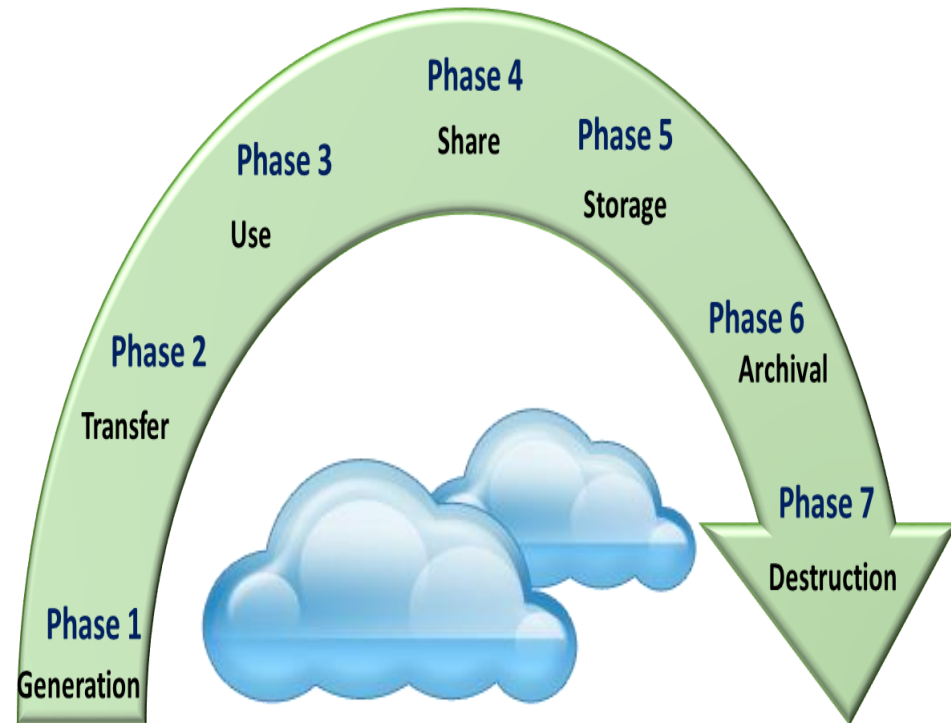
1. **Appropriateness:** The use of information should be consistent with the purposes for which it was collected and the commitments made to the consumer by the provider.
2. **Access control:** Proper access control should be enforced.
3. **Legal compliance:** Information needs to be managed in way that the compliance with the legal requirements can be verified.



Phase 4: Data share

Things to consider at this stage

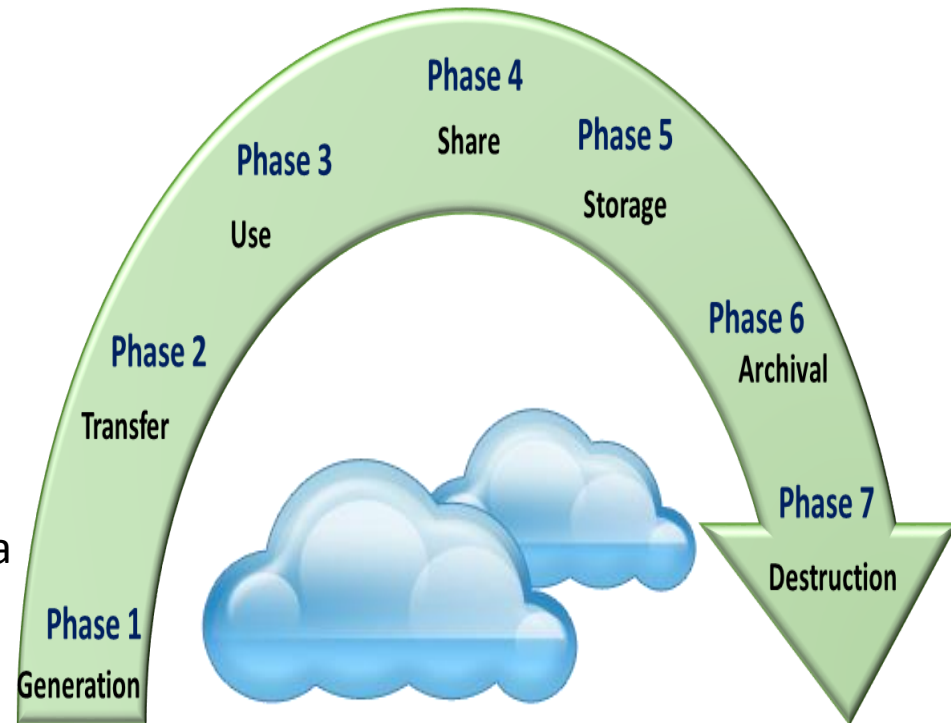
1. **Consent:** While sharing data with a third party consent of the data subject needs to be considered.
2. **Access control:** Access control mechanism should allow only the authorised party to access the data .
3. **Location control:** While sharing data the location of data where it is going would be an important factor to consider due to compliance requirement.
4. **Sharing granularity:** Sharing granularity depends on the sharing policy and the granularity of content.



Phase 4: Data share

Things to consider at this stage

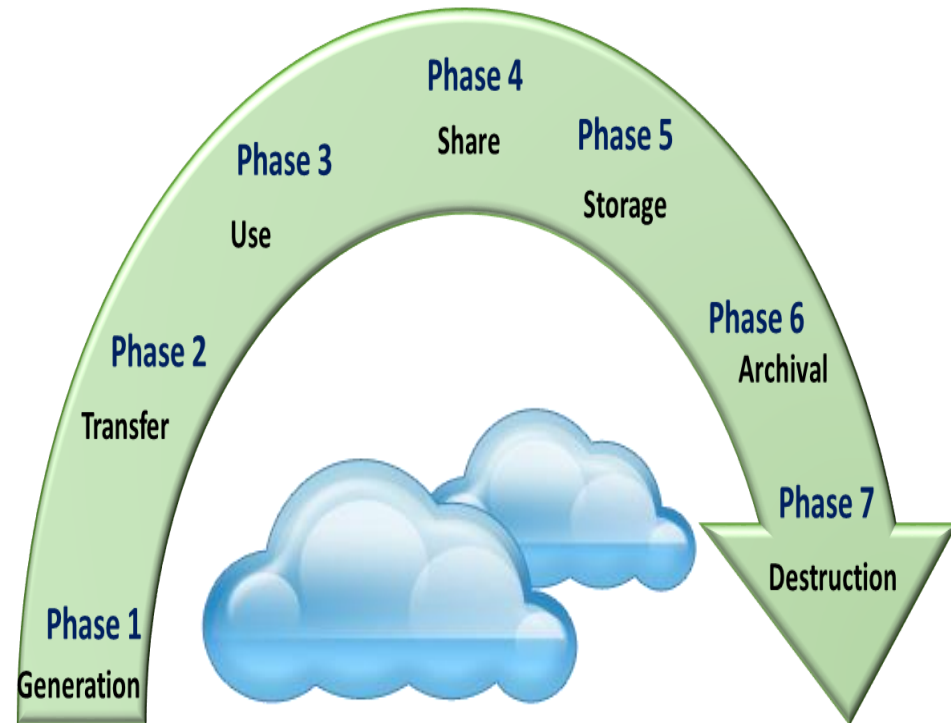
- 5. Data transformation:** Before sharing personal data some transformation might be necessary ,e.g., isolation of sensitive information, ensure anonymity and unlinkability.
- 6. Notification:** Some regulations require the data subject to be notified when data is shared. Therefore, notification mechanism needs to be considered.



Phase 5: Data storage

Things to consider at this stage

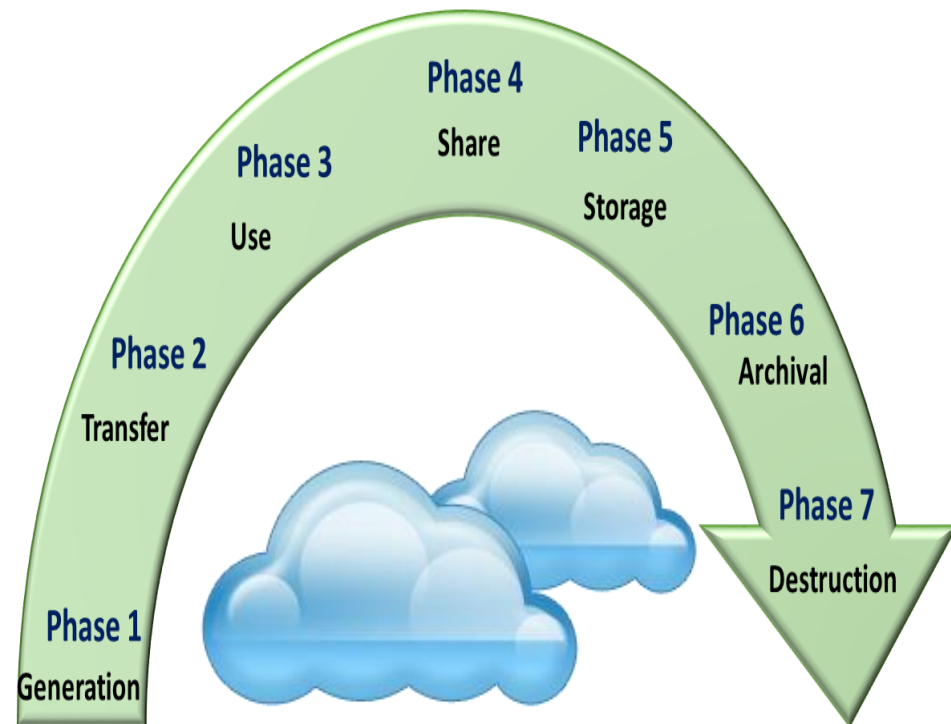
1. **Encryption or transformation:** Data stored in the cloud can be encrypted. It might be difficult to process or doing search in the encrypted data. Other forms of transformation might be used, e.g., isolation of sensitive information, ensure anonymity and unlinkability.
2. **Access control:** Proper access control should be enforced also should consider insider attack.
3. **Location control:** While storing data the location of data where it is being stored would be an important factor to consider due to compliance requirement.



Phase 6: Data archival

Things to consider at this stage

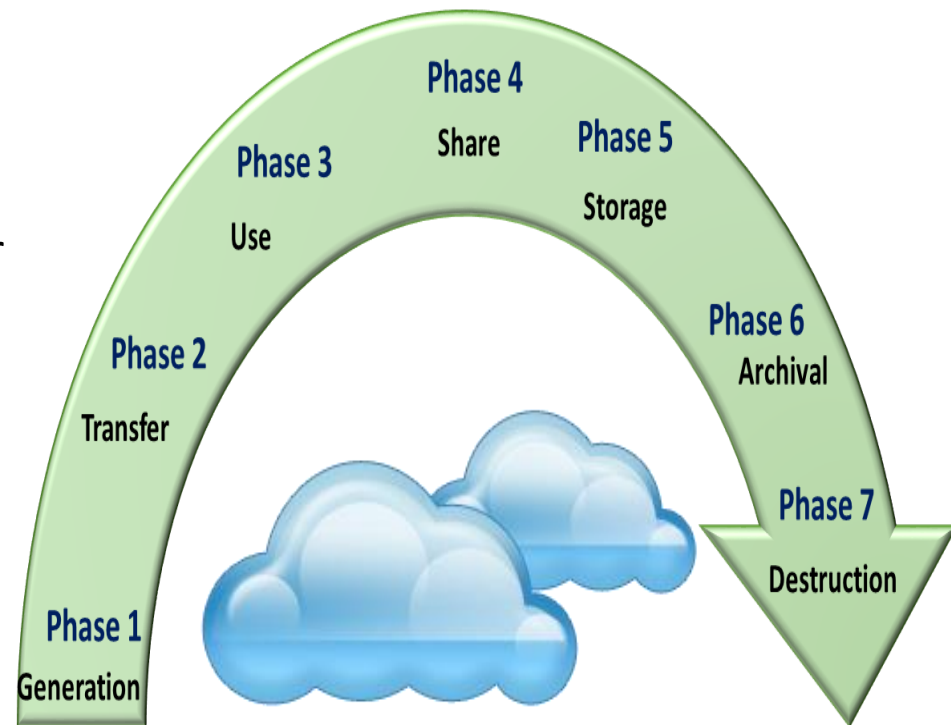
1. **Storage media:** Portability of storage media might increase the possibility of losing data.
2. **Duration of storage:** Data can be stored only for the time necessary for which it was collected. .

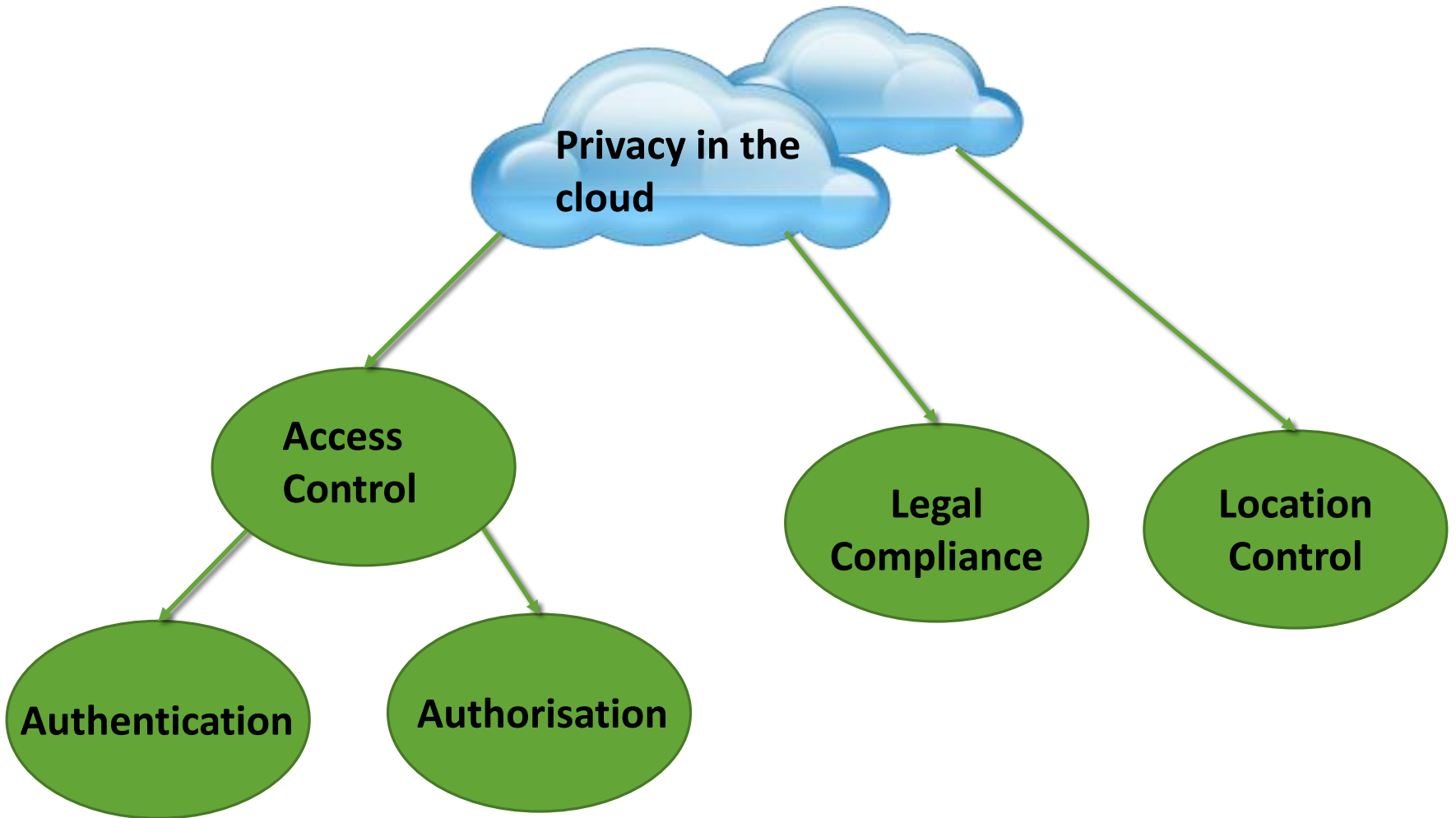


Phase 7: Data destruction

Things to consider at this stage

Complete erasure of all copies: Proper care should be taken to ensure all the copies of the unwanted data are deleted.





Access Control Models

- **Identity based access control**
- **Role Based Access Control (RBAC) model**
- **Attribute Based Access Control (ABAC) model**

Identity based access control

Access Control Matrix

Subject	File 1	File 2	File 3	File 4
Larry	Read	Read, write	Read	Read, write
Curly	Full control	No access	Full control	Read
Mo	Read, write	No access	Read	Full control
Bob	Full control	Full control	No access	No access

Capability = row in matrix
ACL = column in matrix

ACL

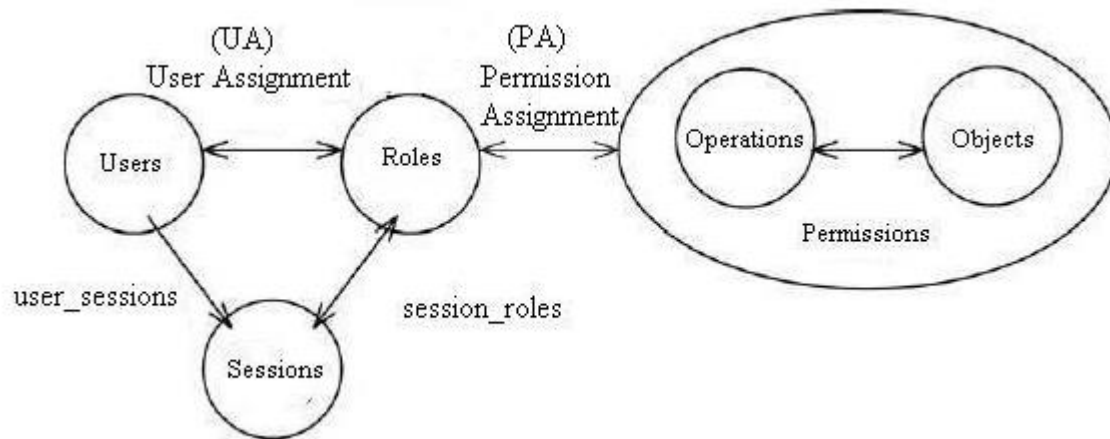
In an identity based system the access rights are based on the **identity of the subject**

It can be implemented using an **access control matrix**,
access control lists or capabilities (Sandhu and Samarati 1994).

Role Based Access Control (RBAC) model

The main concept of RBAC is that permissions are associated with roles and users get permissions based on the roles assigned to them.

Unlike identity based systems adding or removing users is much easier in this model.



Attribute Based Access Control (ABAC) model

The Attribute Based Access Control Model is an extension of the RBAC Model where permissions are given based on the attributes possessed by the user.

Attributes are not limited to organisational roles, they can be anything such as degree, qualification, name, age and of course roles.

Attributes (usually assigned by Attribute Authorities (AAs)), are assigned to users and permissions are assigned to attributes and thus users get permissions based on the attributes they possess.

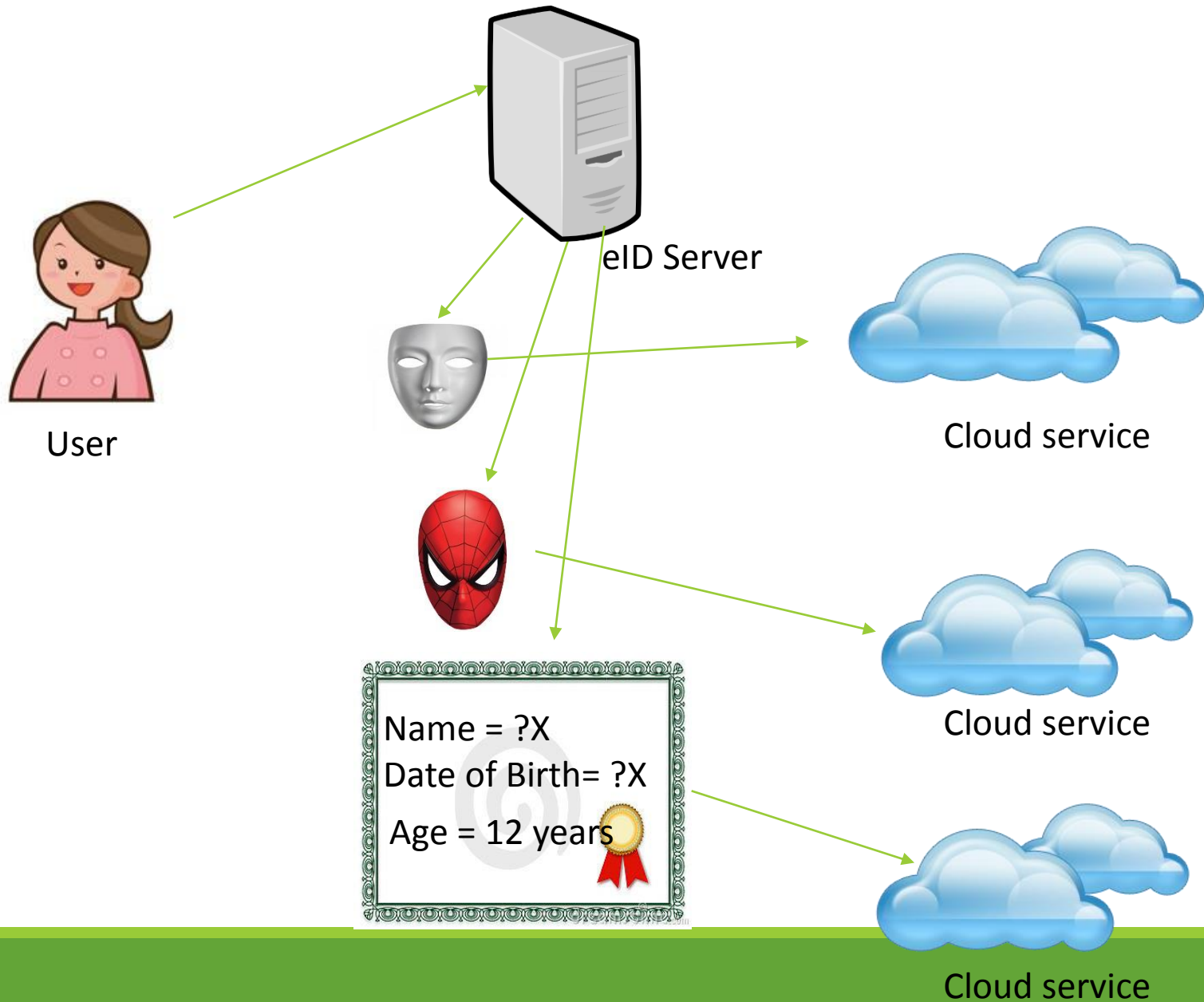
Authentication

Authentication is a way of identifying an entity and is a process by which it is possible to determine whether someone/something is genuine.

Privacy preserving authentication technique should allow

- Anonymity
- Unlinkability
- Minimum disclosure

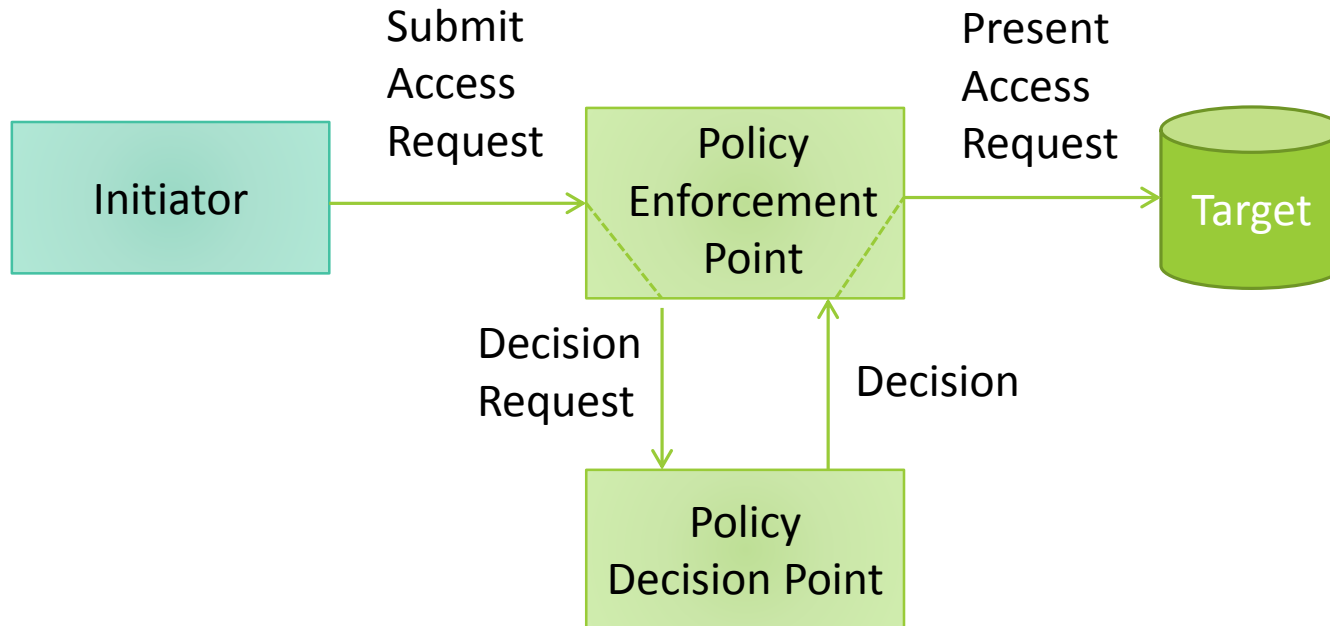
Privacy Preserving Authentication



Authorisation

An authorisation system determines who is authorised to do what i.e. it assigns privileges to users and provides a decision on whether someone is allowed to perform a requested action on a resource.

Policy based authorisation system



Example Policy

```
<Policy PolicyId="PolicyNo1forMedicalData"
  RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-
algorithm:deny-overrides">
  <Target/>
  <Rule RuleId="MedicalDataAccessByMedicalProfessional"
Effect="Permit">
  <Description>Medical Professional of this organisation can read the
medical data </Description>
  <Target>
    <Subjects> <Subject>
      <SubjectMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <AttributeValue
DataType= "http://www.w3.org/2001/XMLSchema#string">Medical
Professional</AttributeValue>
          <SubjectAttributeDesignator AttributeId=Role
DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </SubjectMatch>
      </Subject> </Subjects>
```

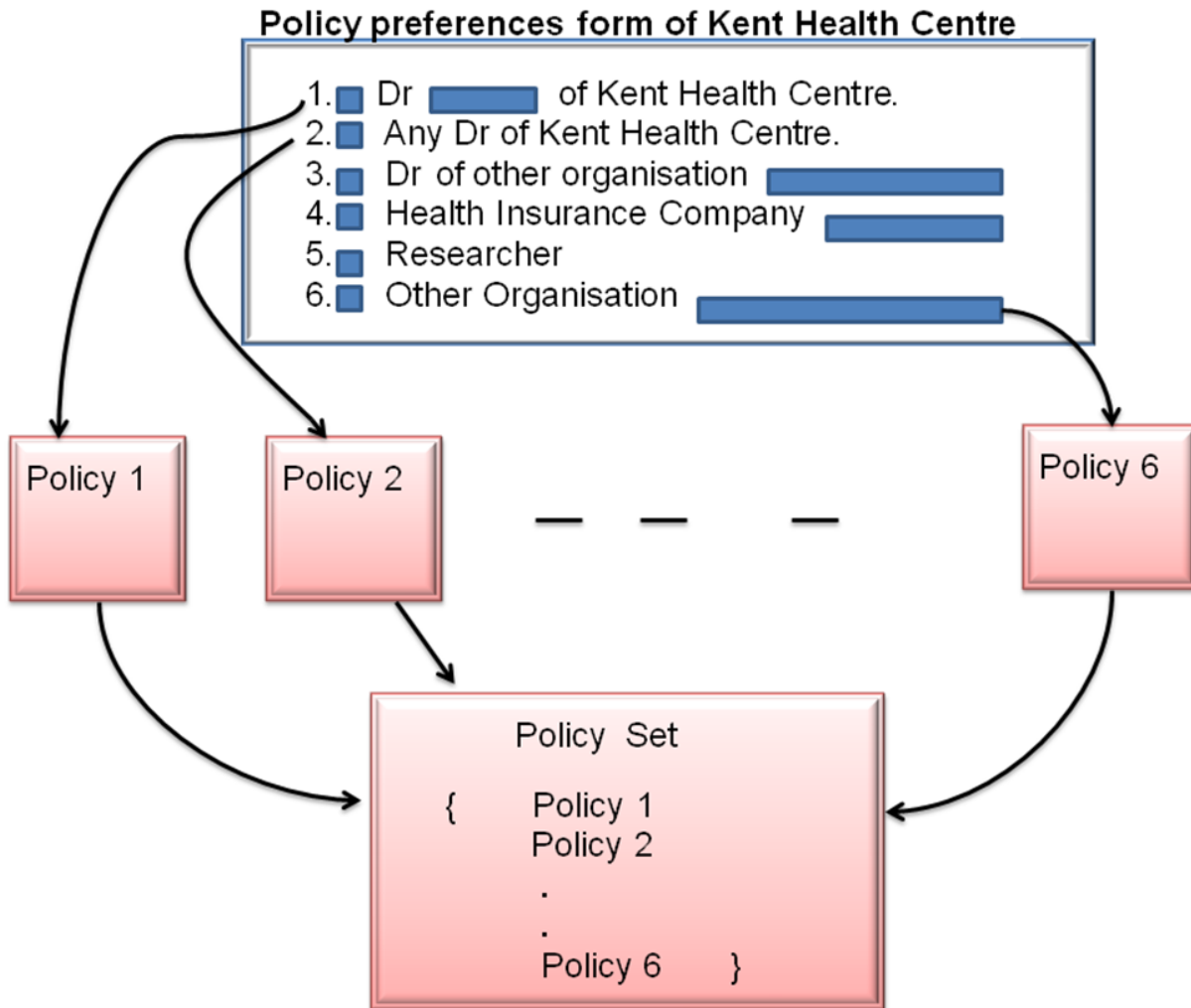
Example Policy

```
<Resources> <Resource>
  <ResourceMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
  <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Medical
Data</AttributeValue>
  <ResourceAttributeDesignator
DataType="http://www.w3.org/2001/XMLSchema#string"
AttributeId="ResourceType"/>
  </ResourceMatch>
</Resource>
</Resources>
<Actions> <Action> <ActionMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
  <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">READ</Attr
ibuteValue>
  <ActionAttributeDesignator
DataType="http://www.w3.org/2001/XMLSchema#string"
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"/>
  </ActionMatch>
</Action> </Target> </Rule> </Policy>
```

Adding privacy protection to policy based authorisation system

- **Needs to add policies from Data Subject to honour his/her wishes.**
- **Needs to enforce obligations to notify the data subject.**
- **Needs to add policies from the data protection legislations.**
- **Needs to integrate the policies of all the authorities who have any control over the data such as the controller, issuer.**
- **Needs to resolve conflicts among multiple independent policies of all the stakeholders.**
- **Needs to have facility to enforce policies in a distributed environment.**
- **Needs to have the facility to include and execute policies from multiple languages.**

Obtaining policies from users

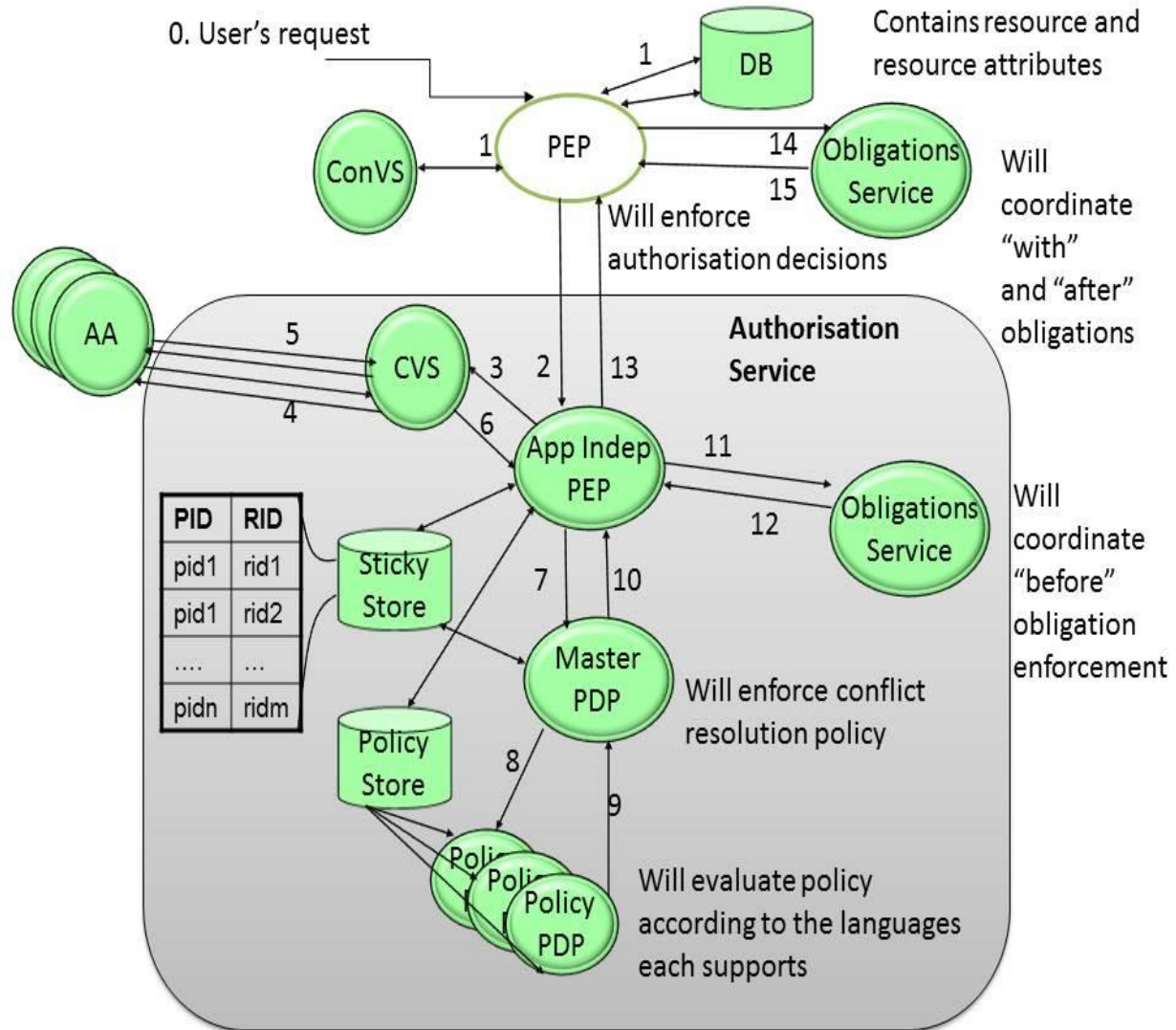


Obtaining policies from users

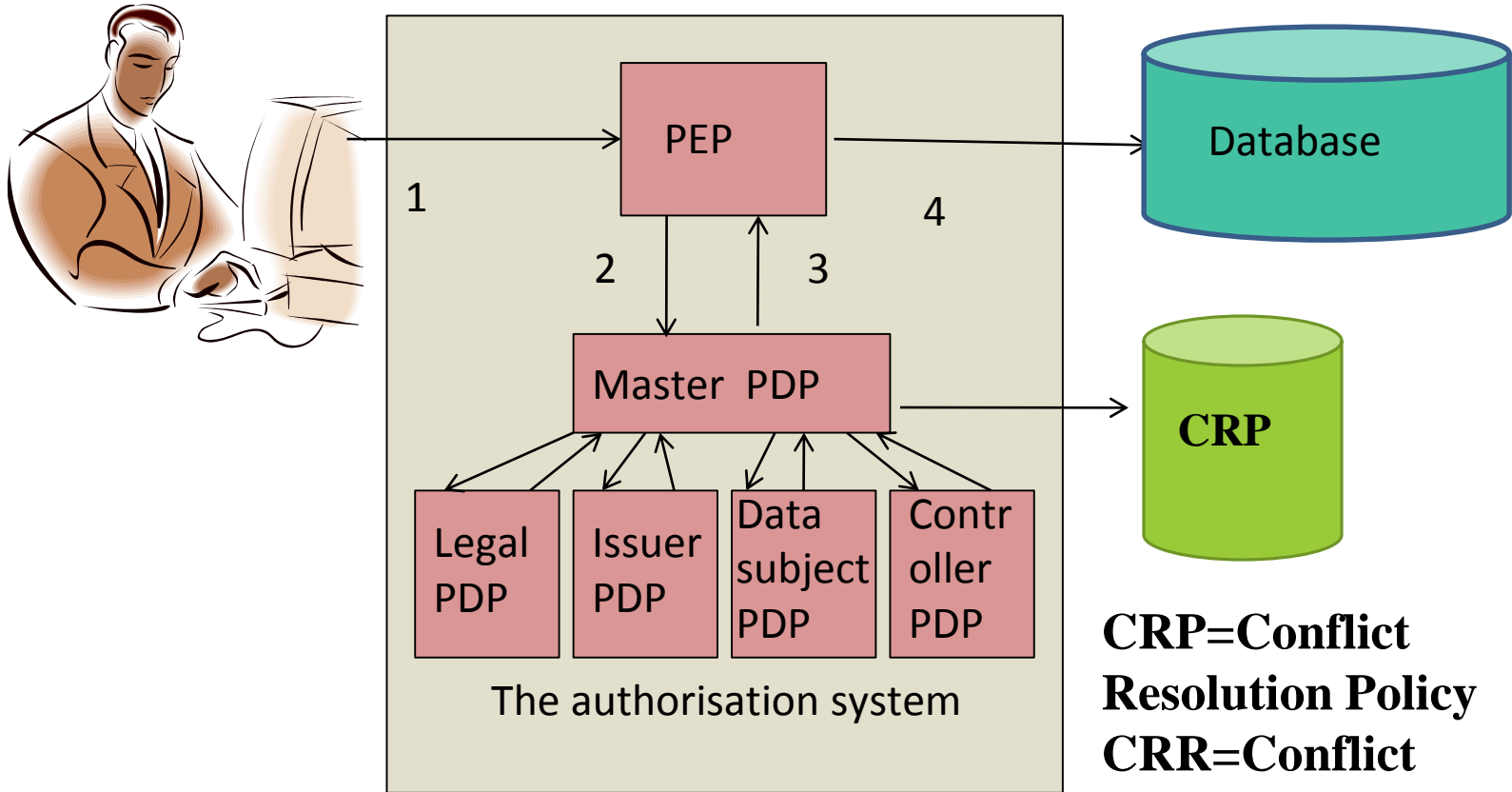
Option 1

```
<Subject>
  <SubjectMatch
    MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
      <AttributeValue
        DataType="http://www.w3.org/2001/XMLSchema#string">Dr.
        D</AttributeValue>
      <SubjectAttributeDesignator AttributeId="Name"
        DataType="http://www.w3.org/2001/XMLSchema#string"/>
    </SubjectMatch>
  </Subject>
```

Privacy-Preserving Advanced Authorisation System (P-PAAS) infrastructure

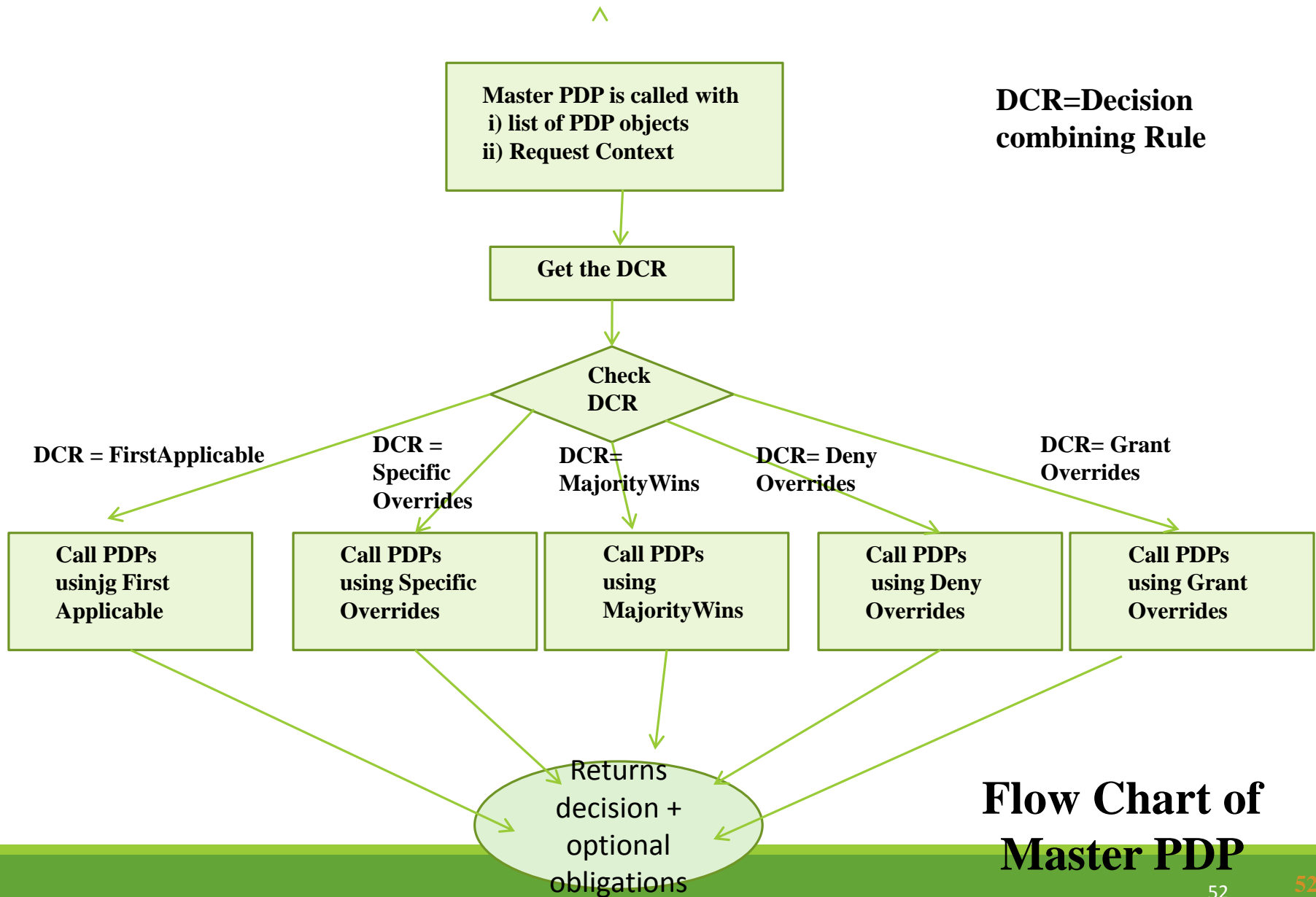


P-PAAS infrastructure in a simplified form

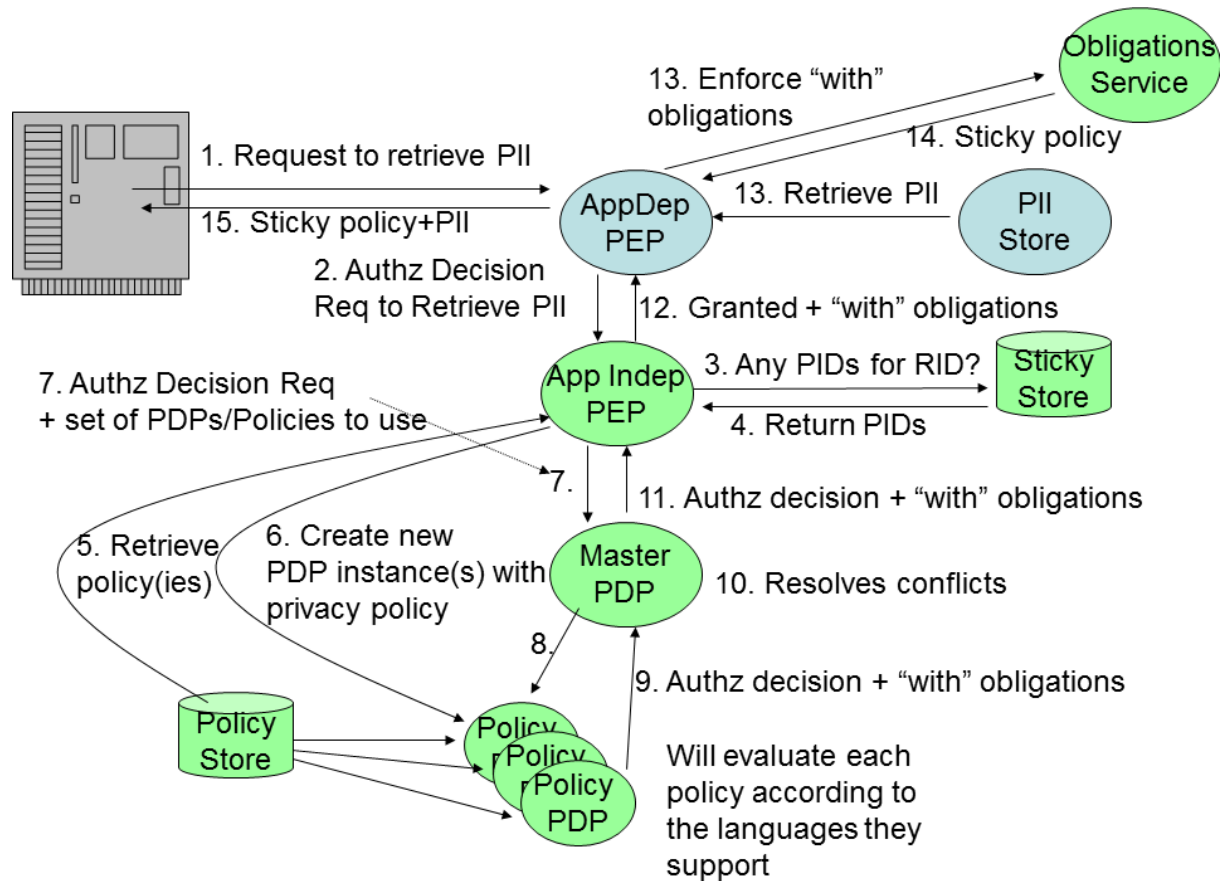


CRP=Conflict Resolution Policy
CRR=Conflict Resolution Rule
{condition, DCR}
DCR=Decision Combining Rule

Dynamic Conflict Resolution



Distributed enforcement of policies



Checking with the requirements of EU data protection directive ...

1. Purpose specification
2. Consent specification
3. Limited collection
4. Limited use and limited disclosure
5. Limited retention
6. Accuracy.
7. Safety
8. Openness
9. Compliance
10. User's control
11. Enforcing privacy obligation
12. Privileged access
13. Transferring data
14. Contract based access to personal data

Do you think this model is fit for cloud environment?

Where to improve then?

Conversion of law into machine enforceable policies

Mont et al. (M. Mont, S. Pearson, et al. 2010) say that **translation of legislation/regulation to machine readable policies has proven to be very difficult.**

Papanikolaou et al. (Papanikolaou, Pearson and Mont 2011) say that it is unreasonable to expect a computer program to fully understand the legal or other policy text. However, **even with the limited capabilities, the automation of Legal policy enforcement significantly reduces the effort required to ensure compliance.**

The Methodology for obtaining Legal Policies

Step1. Listing the Legal provisions that are directly related to access control.

- For our implementation we considered only the articles directly related to access control. A rule is directly related to authorisation if it pertains directly to the processing, prohibiting, accessing, collecting, blocking or transferring of personal data, i.e. it mentions an action on personal data.

The Methodology for obtaining Legal Policies

Step 2. Analysing the Legal provisions

- The nature of the EU DPD is such that the outcomes of rules are subject to explanations, built on "it all depends" upon context, and human interpretation at the point of application (M. Mont, S. Pearson, et al. 2010). It requires human skills and interpretation to obtain deterministic PDP rules from the EU DPD.

The Methodology for obtaining Legal Policies

Step 2. Analysing the Legal provisions (continued..)

The article 6.1 (a) says “personal data must be processed fairly and lawfully” –this legal rule is too vague to form an automated access control rule.

Later in article 7 the criteria for making data processing legitimate are described, these are converted into access control rules.

Article 6.2 states that “It shall be for the controller to ensure that paragraph 1 is complied with.” This rule places responsibility on the controller to ensure that the EDPD (EU Data Protection Directive) is followed, but it does not form an access control rule itself.

The Methodology for obtaining Legal Policies

Step 2. Analysing the Legal provisions (continued..)

Article 12 (c) requires that third parties to whom data were disclosed be notified of any rectification, erasure or blocking carried out in compliance with article 12 (b). This rule is not feasible to present as an access control rule, but rather requires an update mechanism to satisfy the condition.

The Methodology for obtaining Legal Policies

Step 2. Analysing the Legal provisions (continued..)

Article 12(b) states that “as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive” is not possible to convert into an automated rule as it requires human judgement to ensure that the processing complies with the directive or not.

The Methodology for obtaining Legal Policies

Step3. Refining the Access Control Rules

Refining the Access Control Rules by grouping similar rules together and ordering them in terms of their exceptions which need to be evaluated before the ones without. For example, data subjects are allowed unconditional access to their personal data that are held by a data controller, but not if law enforcement would be jeopardised by this. Consequently the rule which concerns law enforcement must be evaluated before the rule which grants the data subject unconditional access.

The Methodology for obtaining Legal Policies

Step 4. Convert into a Controlled Natural Language (CNL).

- **Subject** (who)/ **Action** (can/cannot perform what) / **Resource** (on which data item)/ **Condition** (under which conditions)/ **Effect** (grant/deny) /**Obligation** (subject to these actions being carried out)

Step 5. Converting CNL to PDP rules.

Step 6. Validation

Policies

- If the requested purpose of processing does not match with any of the original purposes of collection or is not for a historical purpose/statistical purpose / scientific purpose deny the request.
- If the validity time of the data is earlier than the request time i.e. the request is made after the validity time of the data has expired, then deny the request.
- A data subject can submit a policy / update a policy.
- The treating Medical Professional can Read/Write on personal data for the purpose of preventive medicine, medical diagnosis, provision of care or treatment or the management of the health care service.

Policies

- A data subject can Read his/her own personal data.
- A data subject is denied access to his/her personal data if there is a national security issue, legal objection, important economic and financial issue or medical objection.
- Personal data can be transferred to a non EU country or to a country not having an adequate level of protection when there is a contract between the controllers (data sender and receiver controllers) to ensure an adequate safeguard.

Facts and findings

From the 53 rules of the EU DPD that were considered for analysis in step 2 (since they mentioned some actions on personal data) 27 of them could contribute to the construction of enforceable authorisation rules.

However, 14 rules among these 53 are found to be **guidelines or instructions** only and there are no means to have authorisation rules from them.

For example,

- Article 6.1.(a) states that personal data must be processed fairly and lawfully,
- Article 17.1 says that controller must implement appropriate technical and organisational measure to protect personal data against accidental or unlawful destruction or accidental loss,
- while Article 25.2 instructs about what to consider for determining whether a third country has adequate level of protections.

Facts and findings

The remaining 9 rules are found to be **too complex or dependent on human judgement** to be turned into access control rules by themselves.

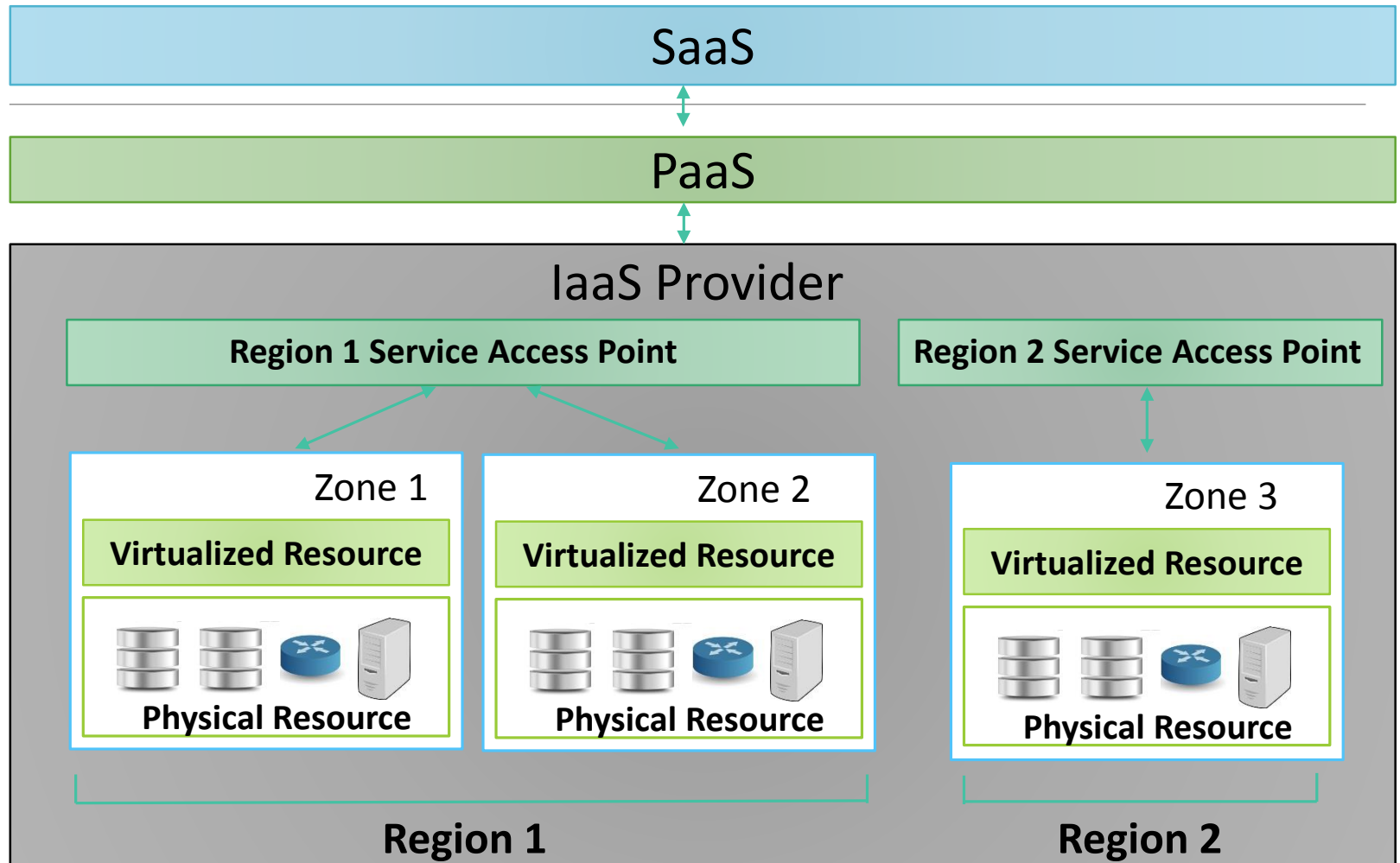
- For example, Article 7(f) “processing of personal data for legitimate interest are allowed except where such interests are overridden by the fundamental rights and freedom of data subject” presents an extremely complex condition where the balance of interests are not feasible to be presented in an access control policy.

Control of data location in cloud

Why Would a Service Provider Copy Data to Multiple Locations?

- Risk mitigation against localised catastrophic events, e.g., equipment failure, fire, etc.
- Minimize operational expenditure
- Storage capacity
- Maintenance
- Localised caching/ content distribution

Location Aware Cloud Model



Example XACML policy element for Location Control

```
<EnvironmentAttributeDesignator AttributeId="Location"  
DataType="http://www.w3.org/2001/XMLSchema#string"/>
```

```
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-bag">
```

```
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
```

Region 1

```
</AttributeValue>
```

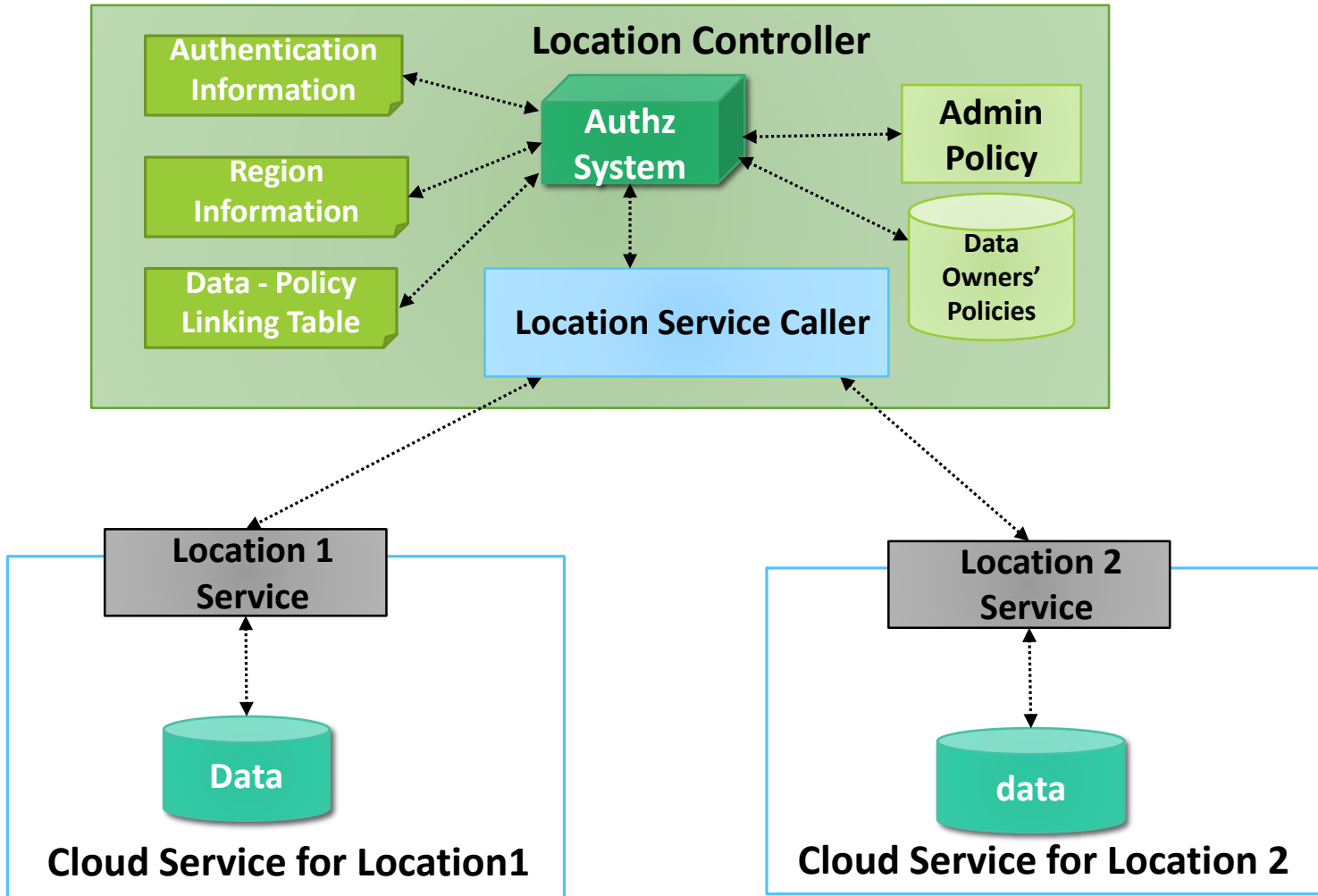
```
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
```

Region 2

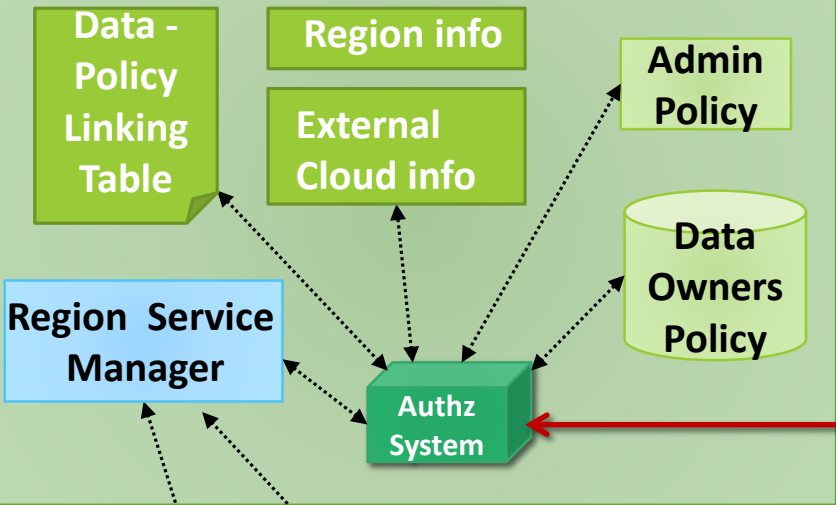
```
</AttributeValue>
```

```
</Apply></Apply>
```

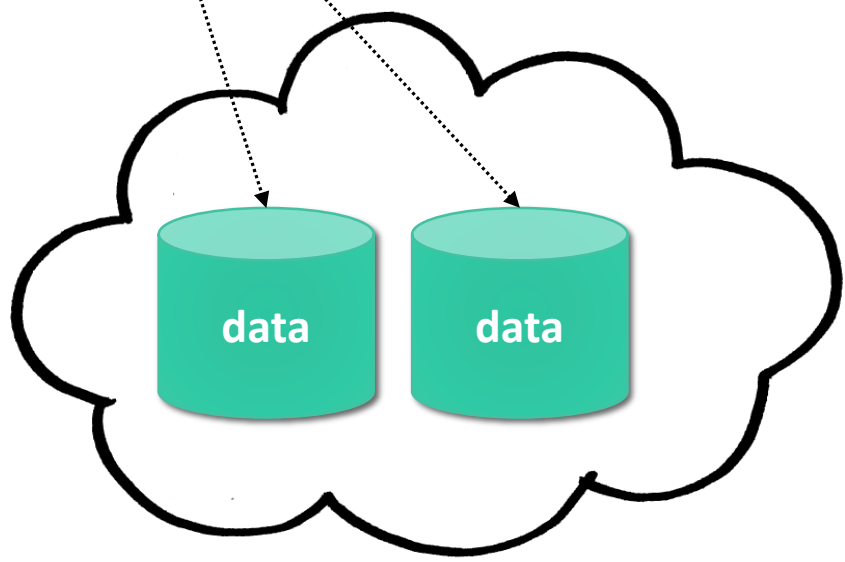
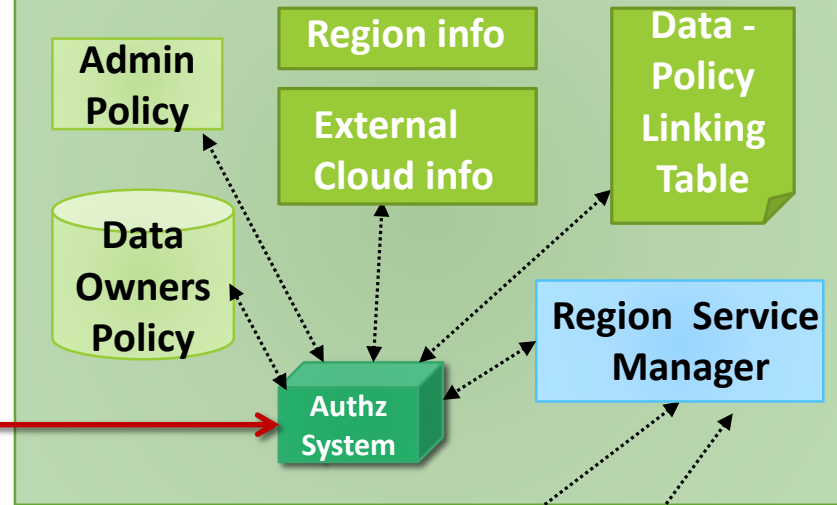
Data Location Control Mode



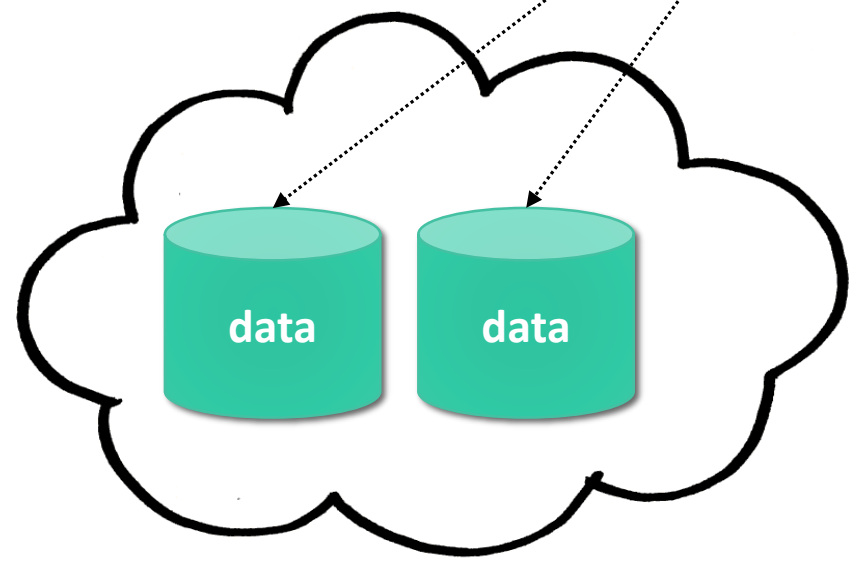
Cloud 1 service Manager



Cloud 2 service Manager



Cloud 1 service



Cloud 2 service

..... Internal communication
— External communication

Location control model interface

User data location control model demonstration

[Admin Login](#)

[User Login](#)

[User Registration](#)

User is given the option to choose location preferences while registering for cloud service

User Registration

Authentication Information

Input a User Name

Input a Password

Input a unique name for your account

Personal Information

Name

Address

Age

Contact number

Location Preference

Our data centres are located in

- US-Northern-Virginia
- US-West-Oregon
- US-West-Northern California
- EU-Ireland
- Asia-Pacific-Singapore
- Asia-Pacific-Sydney
- Asia-Pacific-Tokyo
- South-America-Sao-Paulo

Input an initial location for storage

Input an optional location preference

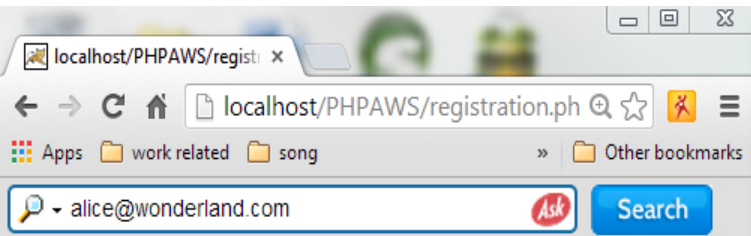
Input an optional location preference

Input an optional location preference

Input your e-mail if you want to be notified for your data movement

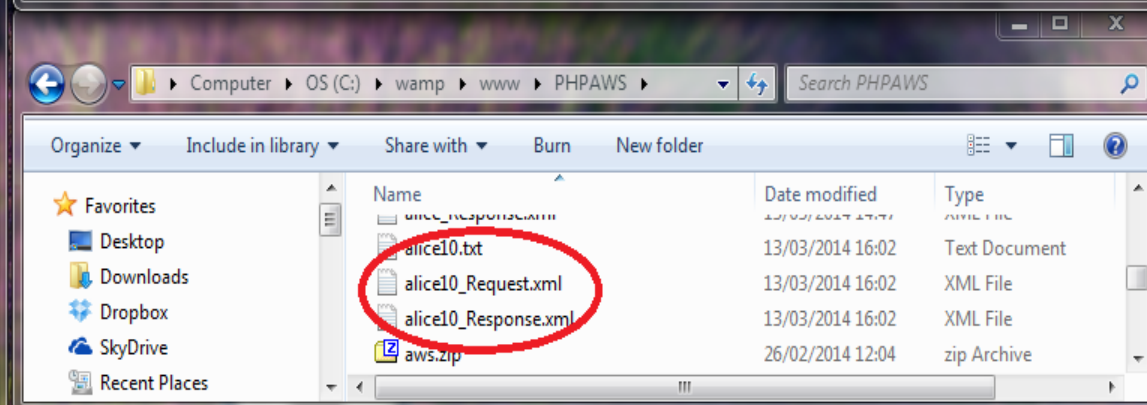
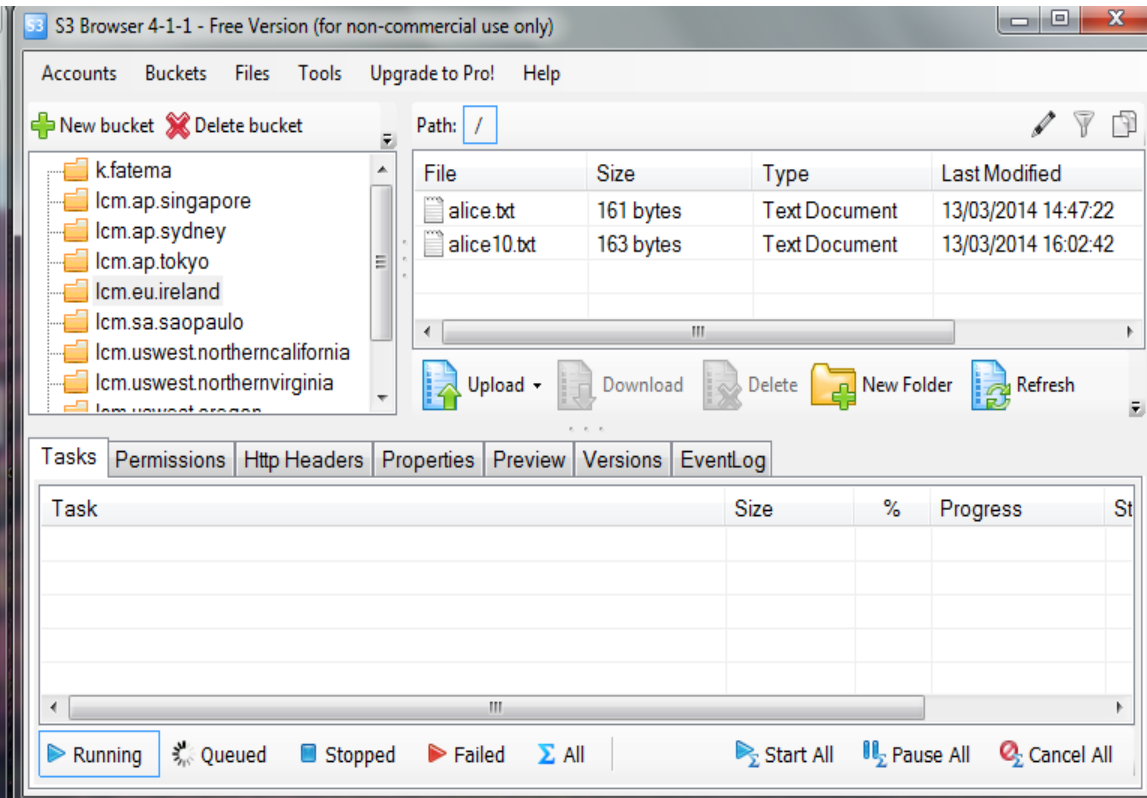
Submit

Automatic Policy creation and data storage



Your policy has been stored successfully.

-----insertion into database successful----- File has been uploaded to the desired primary location



The generated XACML request context from the location preferences

```
C:\wamp\www\PHPAWS\alice10_Request.xml - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
alice_Request.txt user.php registration.php a1_Request.txt admin.php alice10_Request.xml
37 <sp:PolicyContents><PolicySet xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:policy:schema:qs /home/kaniz/Desktop/access_control-xacml-2.0-policy-s
38 <Target xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:qs">
39 <Subjects/><Resources/><Actions/>
40 </Target>
41 <Policy PolicyId="UserLocationPolicy" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides">
42 <Target/>
43 <Rule RuleId="Rule1" Effect="Permit">
44 <Description>My data can be copied/stored/transferred in EUireland, AsiaPacificSingapore, AsiaPacificSydney, </Description>
45 <Target>
46 </Target>
47 <Condition>
48 <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
49 <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-at-least-one-member-of">
50 <ActionAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" DataType="http://www.w3.org/2001/XMLSchema#string">
51 <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-bag">
52 <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">COPY</AttributeValue>
53 <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">STORE</AttributeValue>
54 <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">TRANSFER</AttributeValue>
55 </Apply></Apply>
56 <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-at-least-one-member-of">
57 <EnvironmentAttributeDesignator AttributeId="Location" DataType="http://www.w3.org/2001/XMLSchema#string"/>
58 <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-bag">
59 <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">EUireland</AttributeValue>
60 <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">AsiaPacificSingapore</AttributeValue>
61 <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">AsiaPacificSydney</AttributeValue>
62 </Apply></Apply>
63 </Apply>
64 </Condition>
65 </Rule>
66 <Obligations><Obligation ObligationId="E-mail-To-alice@wonderland.com" FulfillOn="Permit"/></Obligations>
67 </Policy>
68 <Policy PolicyId="UserAccessPolicy" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides">
69 <Target/>
```

eXtensible Markup Language file length: 6813 lines: 97 Ln: 1 Col: 1 Sel: 0 | 0 Dos/Windows ANSI as UTF-8 INS

User is checking the location of his/her data

Check the location of your personal data

Authentication Information

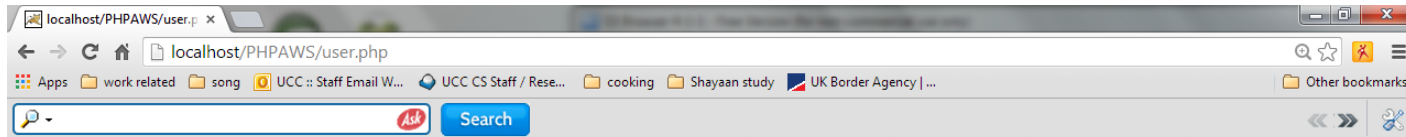
User Name

Password

Name of your account

[Home](#)

User can verify the location of his/her data



Your data are available in ..

- **EUireland**



Scenario #1: Admin tries to copy data to a location approved by the user

Copy operation by Admin

Admin Authentication Information

User Name

Password

Information for copy operation

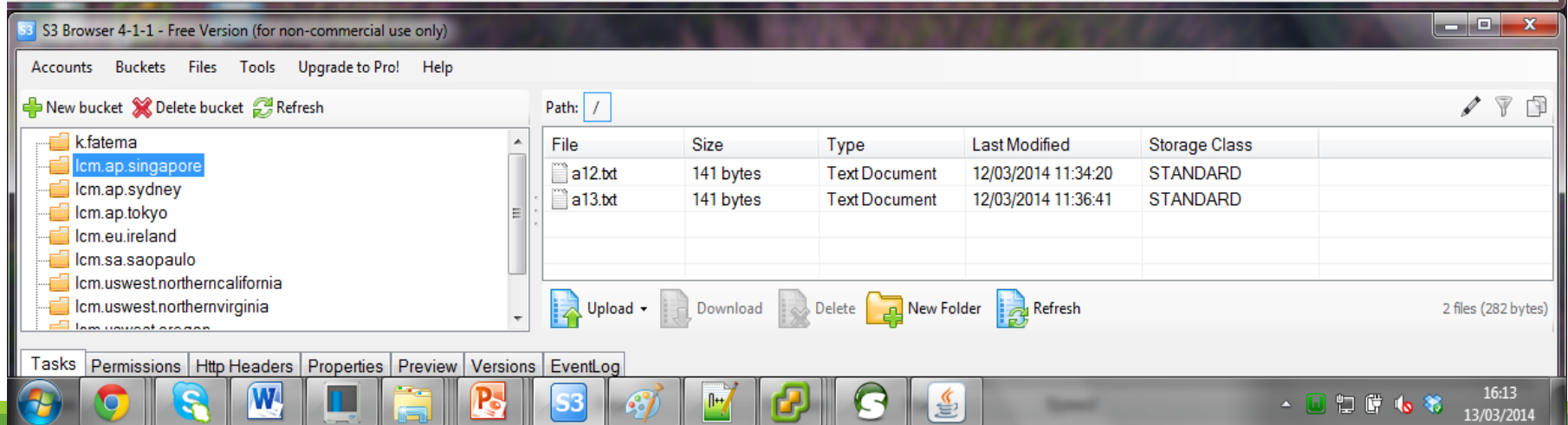
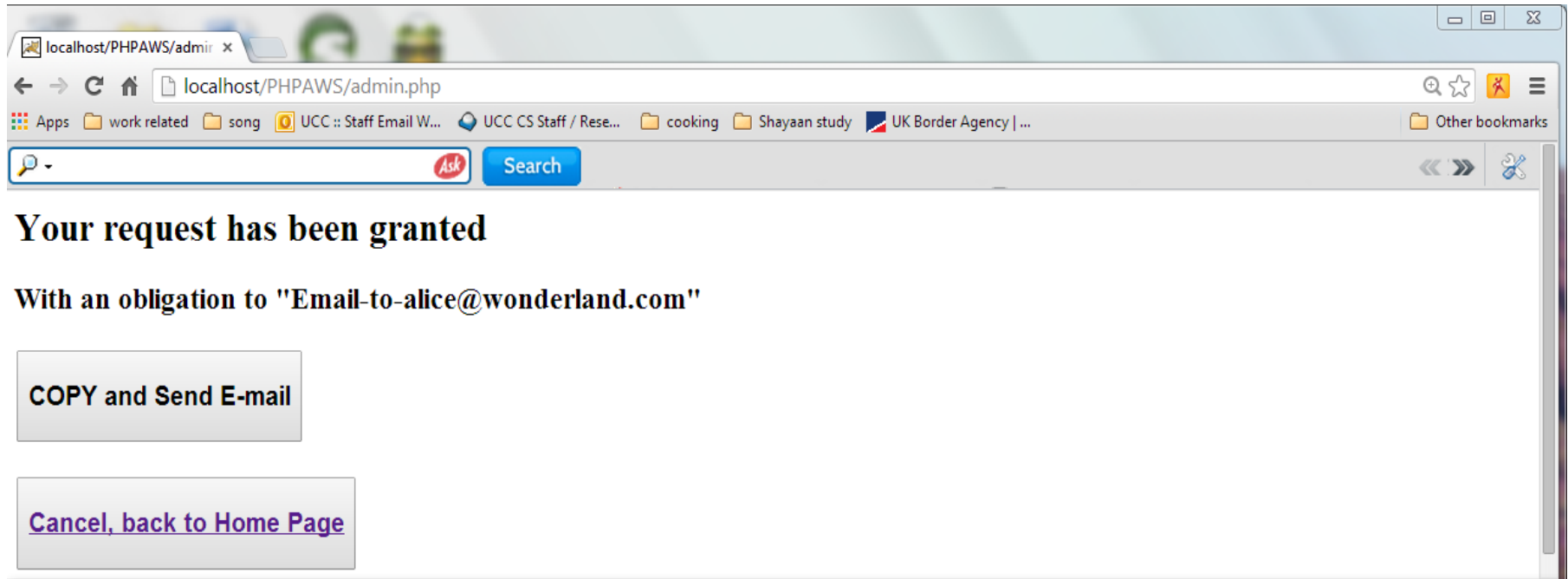
Name of account to copy

Input the location FROM which to copy

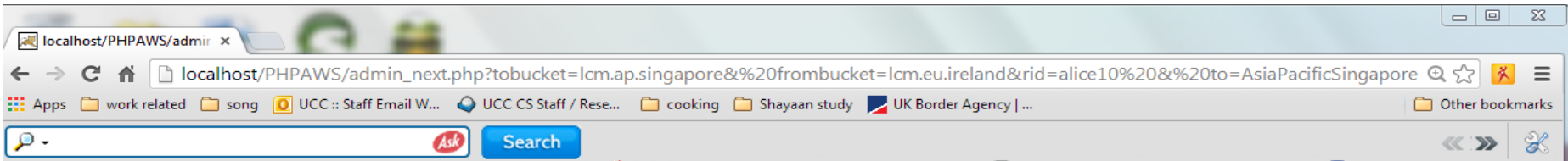
Input the location TO which to copy

[Home](#)

Admin can proceed only by following obligation



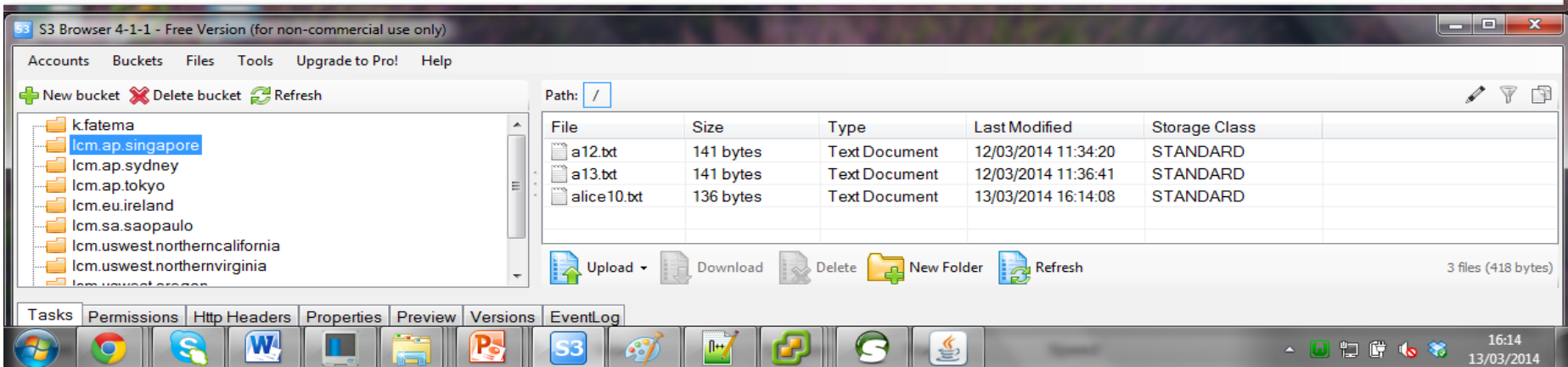
Admin has copied the data after following the obligation



...Database update successful...

The data have been copied successfully to the desired location

[Home](#)



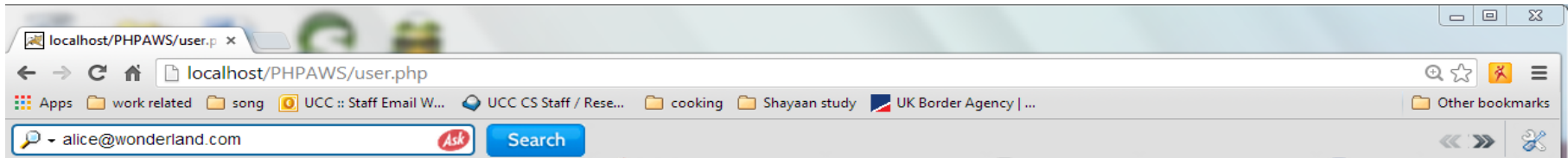
User checks location

The screenshot shows a web browser window with the following details:

- Address bar: localhost/PHPAWS/User_login.html
- Search bar: alice@wonderland.com
- Page Title: Check the location of your personal data
- Form Section: Authentication Information
- Form Fields:
 - User Name: Alice
 - Password: Alice
 - Name of your account: alice10
- Buttons: Submit, Home

The browser's taskbar at the bottom shows various application icons including Windows Explorer, Google Chrome, Skype, Word, and others. The system tray on the right indicates the time is 16:15 on 13/03/2014.

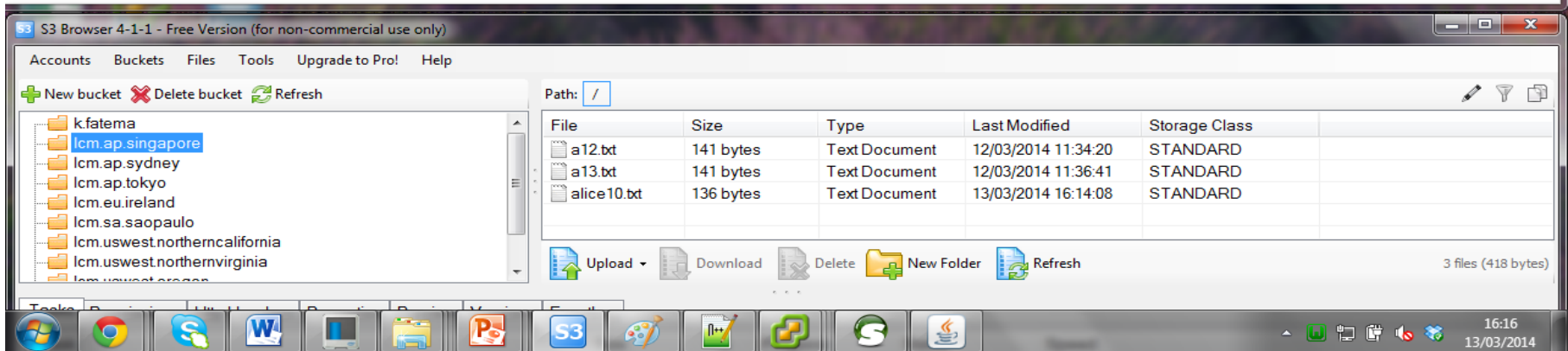
User sees updated location information



Your data are available in ..

- **EU**Ireland
- **AsiaPacific**Singapore

[Home](#)



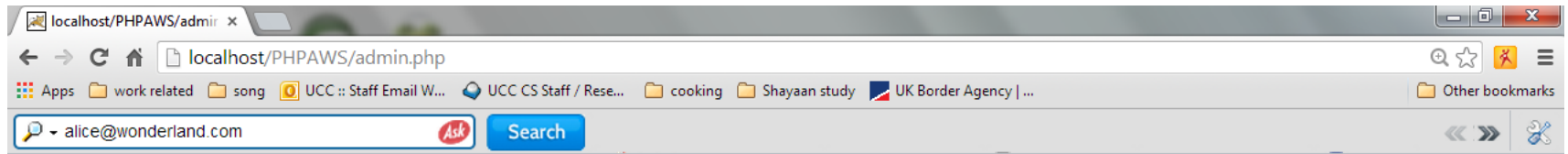
Scenario #2: Admin tries to copy data to a location NOT approved by the user

The screenshot shows a web browser window with the address bar displaying `localhost/PHPAWS/Admin_login.html`. The browser's search bar contains the email `alice@wonderland.com`. The page title is **Copy operation by Admin**. The form is divided into two sections:

- Admin Authentication Information:**
 - User Name:
 - Password:
- Information for copy operation:**
 - Name of account to copy:
 - Input the location FROM which to copy:
 - Input the location TO which to copy:

At the bottom of the form area, there is a **Submit** button and a **Home** link. The Windows taskbar at the bottom shows the time as 16:19 on 13/03/2014.

Request is not granted and copy can't be done



Your request has NOT been granted

[Back to Home Page](#)



Evaluation

Machine setup: Virtual machine running in a vSphere private cloud. The virtual machine was configured with one virtual core Intel Xeon E5620 CPU running at 2.4 GHz with 2 GB of memory.

Test result: 0.04s overhead on processing a transaction which includes 1. time to identify the correct data location 2. time to query authorization system and getting a response from that 3. updating the database.

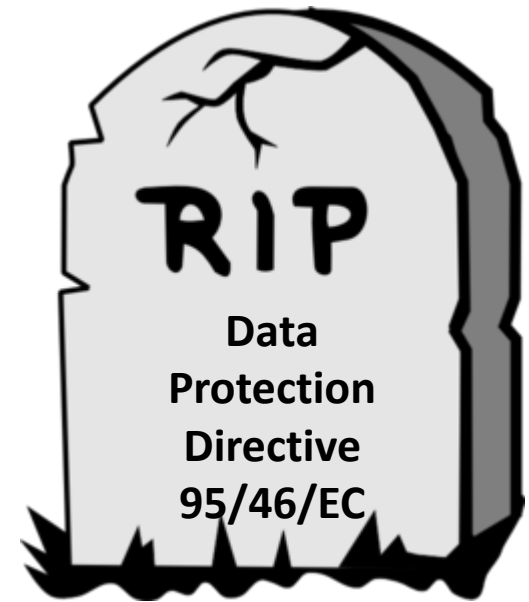
0.2s overhead was observed for connecting to remote storage via SSH and for transferring a file of less than a KB.

Legal compliance

The current rules also need to be modernised - they were introduced when the Internet was still in its infancy. Data Protection Directive 95/46/EC needs reformation to be fit for

- technological developments like social networks and cloud computing
- globalisation.

Therefore a proposal for a regulation was released on 25 January 2012. As of Monday 15 June 2015, the Council of Ministers stated that they will reach agreement by the end of 2015. It will appear as a Regulation and not a Directive, it will have immediate effect on all 28 EU Member States after the two-year transition period.



Re-form of EU Data Protection Law

- A **'right to be forgotten'** will help people better manage data-protection risks online. When they no longer want their data to be processed and there are no legitimate grounds for retaining it, the data will be deleted.
- Whenever **consent** is required for data processing, it will have to be given **explicitly**, rather than be assumed.
- **Easier access** to one's own data and the **right of data portability**, i.e. easier transfer of personal data from one service provider to another.
- Companies and organisations will have to **notify serious data breaches** without undue delay, where feasible within 24 hours.

Re-form of EU Data Protection Law

(cont ..)

- A single set of rules on data protection, **valid across the EU**.
- Companies will only have to deal with **a single national data protection authority** – in the EU country where they have their main establishment.
- More **transparency** about how data is handled, with easy-to-understand information, especially for children.
- Individuals will have the right to refer all cases to their home national data protection authority, even when their personal data is processed outside their home country.

Re-form of EU Data Protection Law

(cont ..)

- EU rules will apply to companies **not established in the EU**, if they offer goods or services in the EU or monitor the online behaviour of citizens.
- Increased responsibility and accountability for those processing personal data - through **data protection risk assessments**, **data protection officers**, and the principles of '**privacy by design**' and '**privacy by default**'.
- Unnecessary administrative burdens such as notification requirements for companies processing personal data will be removed.
- National data protection authorities will be strengthened so they can better enforce the EU rules at home.

Get ready service providers

- Service providers need to have their privacy policies, procedures and documentation up to date: data protection authorities will be able to ask for these at any time.
- Service providers should develop metrics to measure the status of privacy efforts, report regularly and create statements of compliance that will be required as part of your organisation's annual report.
- Service providers should implement a breach notification process and enhance incident management processes - incident detection and response capabilities.



[20]

Get ready service providers

- Service providers should prepare to fulfil the "right to be forgotten", "right to erasure" and the "right to data portability".
- Strategies for data classification, retention, collection, destruction, storage and search will be required.
- Service providers should create and enforce privacy throughout the systems' lifecycles to meet the "privacy by design" requirement.



[20]

Research direction

1. A trustworthy monitoring mechanism for data access and sharing.
2. A verifiable Consent management mechanism – consents have to be adequate and freely given, specific, informed and explicit. Moreover, the consents should be provable.
3. Compliance verification techniques.
4. Identify privacy metrics
5. A trustworthy way of verifying the privacy metrics
6. Technical means to satisfy the right of data portability.

References

- [1] http://askbobrankin.com/privacy_software.html
- [2] <http://www.yugatech.com/curious/the-ultimate-computer-privacy-protection/>
- [3] Lengwiler, M. Privacy, justice and equality: the history of privacy legislation and its significance for civil society. Discussion paper, Berlin: University of Zurich, 2004.
- [4] Allmer, T. "A critical contribution to theoretical foundations of privacy studies." Journal of Information, Communication & Ethics in Society 9, no. 2 (2011): 83-101.
- [5] Clarke, R. "What's privacy." Roger Clarke's web-site. August 2006. <http://www.rogerclarke.com/DV/Privacy.html>
- [6] <http://www.madisonaveinsights.com/2014/06/19/ghostery-assuages-privacy-concerns-through-transparency-and-control/>
- [7] <http://www.123rf.com/stock-photo/cultural.html>
- [8] <http://gogoodscout.com/category/law-and-regulation/>
- [9] <http://blog.achintyaagarwal.com/>
- [10] Graham Greenleaf, "Global data privacy laws 2015: 109 countries, with European laws now a minority", Privacy Laws & Business International Report, February 2015

- [11] Graham Greenleaf, "The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention" International Data Privacy Law, Vol. 2, Issue 2, UNSW Law Research Paper No. 2011-39, Edinburgh School of Law Research Paper No. 2012/12
- [12] http://www.claybennett.com/pages/security_fence.html
- [13] Borking, J. J. "Why adopting Privacy Enhancing Technologies (PETs) takes so much time." In Computers, Privacy and Data Protection: an Element of Choice, 309--341. Springer, 2011.
- [14] http://www.nytimes.com/2010/09/30/nyregion/30suicide.html?_r=0#addendum
- [15] http://www.123rf.com/photo_9811323_freehand-icon-set--weather.html
- [16] Deyan Chen; Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing," Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on , vol.1, no., pp.647,651, 23-25 March 2012.
- [17] Mather, Tim, Subra Kumaraswamy, and Shahed Latif. Cloud security and privacy: an enterprise perspective on risks and compliance. " O'Reilly Media, Inc.", 2009.
- [18] Sandhu, R. S., and P. Samarati. "Access control: principle and practice." Communications Magazine, IEEE, 1994: 40--48.
- [19] http://ec.europa.eu/justice/data-protection/document/index_en.htm
- [20] <http://www.computerweekly.com/opinion/Security-Think-Tank-What-should-UK-business-do-to-prepare-for-new-EU-data-protection-rules-part1>