Switching -
Data portability upon switching

Table of contents
Questions to start the discussion on topic 4 ........................................................................................................ 2
Framework: switching providers, cloud service and data portability ................................................................. 3
Problems: switching cloud services and data protection ...................................................................................... 3
Problems: switching cloud services and portability .......................................................................................... 4
Possible solutions: data protection ................................................................................................................ 5
Possible solutions: portability .......................................................................................................................... 6
Introduction of contractual terms/provisions ...................................................................................................... 8
APPENDIX 1 EXCERPT FROM THE PLANNED GENERAL DATA PROTECTION REGULATION .................. 10
APPENDIX 2 DATA PORTABILITY POLICY FOR .TEL DOMAINS ................................................................ 12
APPENDIX 3 TEN QUESTIONS REGARDING THE MODEL DATA PORTABILITY POLICY COMMISSIONED
BY THE DATA PORTABILITY PROJECT .................................................................................................. 14
APPENDIX 4 TOP CLOUD COMPUTING SERVICES PROVIDERS .................................................................... 15
APPENDIX 5 Description customer environment and Backup ........................................................................... 21

1 This discussion paper is written by Itte Overing, representative of ICTRecht bv, and Maciej Gawronski, member, for the meeting of the 29th of January 2014 of the Expert Group on cloud computing contracts
Questions to start the discussion on topic 4

Instead of a summary, we thought a list of questions would be the more appropriate way to allow everyone to formulate their own answers. Naturally, we hope you will use our paper as a source of inspiration.

1) Should (certain) questions below (4-8) be answered differently depending on the cloud service model (IaaS, PaaS or SaaS) and/or the cloud deployment model (private, community, public or hybrid cloud) that is used?

2) Should the questions below (4-8) be answered differently, depending on whether the service is free-of-charge or a paid service?

3) Should the questions below (4-8) be answered differently depending on the reason for switching providers?

4) What is required (Data protection)?
   a. What kind of data should be transferred and/or transferable?
   b. What kind of data should consumers be able to inspect?
   c. What data should be deleted after termination and should the cloud provider provide proof of deletion?
   d. Is interoperability required or is the mere supply of data sufficient in this context?
   e. How do we deal with a chain of cloud providers that jointly supply an end product (cloud service)?

5) What are the SEs’ needs? (Outside the scope of data protection)
   a. What data should SEs be able to transfer (does a SE have the right to switch services and to take along its data)?
   b. What data should or should not be deleted after termination? Which (other) post-termination assistance is required?
   c. Is interoperability required or is the mere supply of data (in its original format) sufficient?

6) What are the consumer’s needs? (Outside the scope of data protection)
   a. What data should consumers be able to transfer (does a consumer have the right to switch services and to take along its data)?
   b. What data should or should not be deleted after termination? Which (other) post-termination assistance is required?
   c. Is interoperability required or is the mere supply of data (in its original format) sufficient?

7) Solutions: which contract terms are fair, save and reasonable? By what means should we introduce the fair, save and reasonable contract terms and coerce industry to comply with them? (and do we define the legal solution in accordance with currently available technical solutions or do we define the legal solution independently and expect technical solutions to comply? Wishful thinking?)

8) What are the potential consequences for suppliers?
   a. Competition;
   b. Cost (should suppliers be allowed to charge additional fees for data portability or migration of data)?.
Framework: switching providers, cloud service and data portability

The description of topic 4 begins with, “The option of switching and changing cloud providers appears to be a key right for consumers and small firms. In practice, however, switching providers means that it must be possible to transfer personal and other data to a new provider in a format that is commonly used and without hindrance from the former provider.”

During the first meeting the Experts also emphasised the importance of switching from one provider to another and of data portability. Furthermore, reference was made to the deletion of data, government access to data and retention of metadata – topics that should also be addressed in this context.

Before examining the barriers which consumers and small enterprises encounter when switching providers and the possible solutions, we need to define the terms used for this topic as clearly as possible or at least specify the possible meanings of the terms. Any discussion requires a framework.

**Switching** refers to switching from one cloud service (provider) to another. The reasons for switching services and/or providers may vary. For instance, a customer may switch voluntarily, because (s)he thinks another provider and/or service is better. In some cases, the service in question may be terminated by the provider, for example due to a lack of commercial success, or a change in focus of business activities. Another possibility is that the provider terminates the service for a specific user, due to a violation of the terms of service by that user. In addition, if the cloud service provider goes bankrupt, this may lead to termination of the service.

**Cloud services** come in various shapes and sizes: SaaS, PaaS and IaaS, where the various cloud services can be implemented on an infrastructure which is, to a greater or lesser extent, dedicated or shared (private, community, public or hybrid cloud).² Naturally, the demarcation of these different kinds of cloud services is not absolute, but rather a relative indication.

The **cloud services provider** can play different roles when providing the service: the provider can be the controller and/or the processor for the personal data processed by the cloud services.

At the first meeting it emerged that in addition to data that was entered or generated individually, **data** can also represent metadata. It was emphasised that **portability** not only covers the portability of the data that was entered, but also the structure of the data (metadata).

**Problems: switching cloud services and data protection**

People have a right to privacy. If someone’s personal details are processed, that person has the right to inspect them. Individuals must be able to take note of which of their personal details the provider has processed, on request, by way of a copy. One can also avail oneself of the right of inspection in the case of switching.³

In the context of protecting personal data, this is a good thing. In terms of portability, it is of little benefit. The copy cannot usually be migrated to a new application. In any case, this will also require accompanying metadata.

Other data protection dilemmas listed in the case of switching providers include the **deletion** of data and the **retention** of data by the service provider. Individuals have the right to have data deleted pursuant to the data protection regulations. Even if the data subject does not explicitly demand this, the provider must delete the data after a certain amount of time has passed, namely when the processing is no longer necessary for the purpose specified. Both the personal data which the individual entered or left behind and the profiles created on the basis of this data must be deleted. In practice, this deletion frequently does not take place. Sometimes the identifying information is disconnected from other information.

³ 95/46/EC Article 12
From a data protection point of view, law enforcers’ access to data stored by the cloud provider is an important issue. Yet, according to us, this topic falls outside of the scope of the issue of switching cloud services.\(^4\)

The issues surrounding the inspection, deletion or retention of data may escalate if switching providers is not voluntary. Imagine the provider goes bankrupt. In that case, there is no chance of a request for inspection or deletion being carried out. If the wider (unknown) chain of providers continues to exist, there will be no end to it.

From a technical point of view, the inspection request or the deletion obligation may also cause some difficulty. The formats used and various technical procedures, such as making multiple back-ups, can make it difficult to delete personal data. Even if it is technically possible, the suppliers may not always want to cooperate, for example because the consumer paid for the service using his or her personal data and the provider requires the data to get paid.

It may also be unclear which suppliers (processors) all form part of the chain when providing a cloud service. It may be unclear where the data is located and which processor or controller is in possession of the data, even to the controller.

### Problems: switching cloud services and portability

Besides the data protection issues, the consumer’s interests and, probably more so, those of SEs, when switching cloud services lie in the ability to transfer data when switching cloud services. In addition to personal data, other content such as accounting and accumulated expertise is equally important to SE. In some cases SE has a statutory obligation to store data, e.g. financial data, for a minimum period of time. Occasionally, it must also be able to guarantee the authenticity of data. Therefore, data portability from the former to the new provider is an important issue in take-it-or-leave-it public cloud computing contracts.

From a technical point of view, there are certain obstacles to data portability. Switching from one provider to another or transferring data is technically a difficult issue and not all service providers have the infrastructure required. Portability tends to depend on the features of the operating system.

In practice, however, switching providers means that it must be possible to move personal and other data to a new provider in a format that is commonly used and without hindrance from the former provider. Portability not only covers the portability of the data but also the structure of the data. Some experts underlined that the format in which the data should be transferred is a key issue.

As Eric Henault said:

“The first problem is data retrieval. If you’re with one supplier and you want to contract with another supplier you want to get your data back in a useable format. To put it bluntly, if I get all of my data back in a PDF file, I’m not interested.”\(^5\)

All vendors’ cloud environments support one or more operating systems and databases. Each cloud contains hypervisors (virtual machine monitor (VMM)), processes, security, a storage model, a networking model, a cloud API, licensing models and more. Rarely, if ever, do two providers implement their clouds in exactly the same way, with all the same hardware and infrastructure. The main reasons for the lack of data portability between clouds are the following:

(a) The different potential technical angles of approaching the concept of cloud computing;

(b) The variety of cloud services and hardware on the market;

---

\(^4\) It is our point of view this issue is to be discussed within the context of Topic 11

The requirements of cloud computing providers (utilisation of strong market position or technological advantage).  

In addition to technical obstacles, there may also be other barriers such as obtaining access to data. A large chain of providers that ultimately jointly provides a single SaaS service can make it difficult to collect and then transfer data. Take, for example, a Content Management System for which the functionalities and databases of various providers are linked up.

Users may also switch because they are forced to – for example, because their provider went bankrupt. In that case the user must depend on the party which is required to manage the inventory and divide the proceeds. Then this ‘curator’ may soon land a small enterprise with a considerable bill for providing its data.

Developing the requisite software and building the necessary infrastructure may also entail considerable costs for the provider (and therefore also for the user?). Of course, if providers had designed their services differently from the outset – without any lock-in – then they would not have incurred any costs or at least no high costs. However, this ‘would have, could have, should have’ train of thought does not bring us any closer to covering the costs.

The contractual terms used by cloud providers may also cause some problems. Not all providers guarantee portability. Under some contracts, providers delete data immediately when the contract is terminated, while under others it is preserved for a certain time period and portability is assured. Under other contracts the data is in fact kept for a certain amount of time, without guaranteeing its preservation.

Possible solutions: data protection

At the European level, work is currently being carried out on the “General Data Protection Regulation”. The draft published at the start of 2013 included the right of portability for personal data and other information supplied by the user. However, this was eliminated from, or at least considerably limited in, the most recent unofficial draft from October 2013. The initial text, 

“Where the data subject has provided the personal data and the processing is based on consent or on a contract, the data subject shall have the right to transmit those personal data and any other information provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn.”

was replaced with the following (draft) text:

“Where technically feasible and available, the data shall be transferred directly from controller to controller at the request of the data subject.”

In this respect, “data” only seems to refer to personal data and no longer to other information provided by the user. The most recent version also includes the format in which the data must be provided if the service provider (‘controller’) does not migrate to the new system:

“The data subject shall have the right to obtain from the controller a copy of the provided personal data in an electronic and interoperable format which is commonly used and allows for further use by the data subject without hindrance from the controller from whom the personal data are withdrawn.”

---

7 The administrator of the inventory or ‘curator’ is appointed by the court that issues the bankruptcy ruling, at least under Dutch law
8 See APPENDIX 1
9 Article 18 General Data Protection Regulation (draft of 25/1/2012)
10 Article 15 General Data Protection Regulation (consolidated draft of 22/10/2013), and also recitals 51a, 130 and 131
Although this is much better than a hardcopy version in your letterbox, this new draft of the European legislation may still lead to issues such as the requirement to copy complete patient files – preferably without any errors – because the format is incorrect or because other information necessary for portability, such as metadata, is missing.

The most recent draft version of the Regulation deletion is regulated in Article17. This may present a solution insofar as the cloud provider comes under the scope of and complies with European law. However, this will mean that many cloud providers must technically modify their services. This does not take into account the technological differences between cloud services either, although this is probably required for a thorough solution.

According to the Dutch enforcement agency, CBP, ‘unlinking’ data is sufficient in certain cases. Of course, it must be impossible to re-link it. This is often not the case.\[^11\]

**Possible solutions: portability**

The current draft of the General Data Protection Regulation does not offer any solution to data portability and its technical aspects, access to data – in the case of a chain of providers or a bankrupt provider – and the apportionment of costs. However, inspiration for solutions may be found by way of (existing):

1. (technical and organisational) (industry) standards;
2. codes of conduct;
3. (standard) contractual terms/provisions in terms and conditions;
4. data portability policies.

When drafting the appropriate contract clauses, we think that it is also necessary to take into account the difference between the cloud service models (and deployment models):\[^12\]

**SaaS**: the cloud customer is substituting software with new software. The focus is on preserving or enhancing the functionality provided by the application.

To ensure data portability at least following factors should be considered: Open specifications of APIs (Application Program Interface), integration technologies, application server/operating system and data formats.

For a smooth switch the content, data and metadata (application configurations) should be portable to a new environment.

**PaaS**: the focus is on minimising the amount of application rewriting while preserving or enhancing controls, and successful data migration. In this model some degree of application modification will be necessary.

To ensure data portability at least following factors should be considered: documented programming languages for application development, open data formats, tight integration or loose coupled services, abstraction layers for queuing and messaging services.

For a smooth switch the code base, application frameworks, data and metadata needs to be transferred.

**IaaS**: the application and data migrate and run at a new cloud provider.

To ensure data portability at least following factors should be considered: Ability to port VMs (Virtual Machines) and the underlying configurations across infrastructure providers.

(technical and organisational) (industry) standards - Current (international) initiatives are by TOSCA\[^13\] and ETSI\[^14\] and the Data Portability Project\[^15\].

---

\[^11\] Facebook documentary: Terms and conditions may apply http://www.youtube.com/watch?v=wbj8s-qwC6E

\[^12\] Towards a Service-Based Internet, W. Abramowicz, ServiceWave Poznan 2011 (pages 66-67)

The goal of the Topology and Orchestration Specification for Cloud Applications (TOSCA) Technical Committee is to substantially enhance the portability of cloud applications and the IT services that comprise them running on complex software and hardware infrastructure.

TOSCA will facilitate this goal by enabling the interoperable description of application and infrastructure cloud services, the relationships between parts of the service, and the operational behaviour of these services (e.g., deploy, patch, shutdown) independent of the supplier creating the service, and any particular cloud provider or hosting technology. TOSCA will also enable the association of that higher-level operational behaviour with cloud infrastructure management.

On 11 December 2013 ETSI published the Cloud Standards Coordination Final Report. The overall objective of the Cloud Standards Coordination initiative led by ETSI was to identify a detailed map of the standards required to support a series of policy objectives defined by the European Commission. It also addresses the following Key action 1 of the European cloud computing strategy (Unleashing the Potential of Cloud Computing in Europe):

"Cutting through the jungle of standards [...] Promote trusted and reliable cloud offerings by tasking ETSI to coordinate with stakeholders in a transparent and open way to identify by 2013 a detailed map of the necessary standards (inter alia for security, interoperability, data portability and reversibility)."

Data Portability is the name of a project which goal is the definition of general practices to implement the Data Portability idea. To achieve this goal, existing open standards and protocols should be used to enable the portability of user data between online tools, social networks and other online services.

The Project commissioned ten questions regarding the model data portability policy with a structured answer (yes/no, multiple choice) and a recommended narrative for the answer (see the part: Possible solutions, data portability policy).

Several major web industry players supported the workgroup (among others): Google, Facebook, LinkedIn, Twitter and Microsoft. While this is good for the effectiveness of the workgroup, it is probably less desirable in the context of data protection.

Successful standardisations are also in progress on a smaller scale: A standard (quality label), Zeker-Online, has been developed in the Netherlands, in which respect the portability of data (in this case financial data) is a requirement for participation. This standard has been developed for the entire chain of providers which jointly provide an online accounting system. To participate, the parties must release the vendor lock-in. The providers promise to ensure that clients will continue to be able to determine the fate of their own data. The providers must offer the financial data stored in a standardised manner by way of an audit file. The benefit for users of the accounting system is the link to the Belastingdienst ('Dutch tax authorities'): the Belastingdienst will be able to inspect the audit file immediately and ease further filing requirements.

Providers have decided to take part because it will give their clients the desired security. This outweighs the loss of the benefit of vendor lock-in.

---

14 The European Telecommunications Standards Institute, : http://www.etsi.org/
15 Several major web industry players supported the workgroup (among others): Google, Facebook, LinkedIn, Twitter and Microsoft, http://en.wikipedia.org/wiki/DataPortability
16 See APPENDIX 3
17 www.zeker-online.nl" www.zeker-online.nl
Codes of conduct – One Dutch example is the DHPA\(^{18}\). Since participants of the DHPA wish to distinguish themselves in the market as professional and top-quality service providers, they have drafted a code of conduct. The following is an excerpt from this code of conduct:

“DHPA participants are generously contributing to the finalisation of customer terminations such as the supply of data or migration to other service providers, provided that the customer in question has complied with its contractual obligations.”

The benefit of a code of conduct (as well as a standard) that comes from the industry is that the industry will endorse it and comply with it. Nevertheless take into account any such code is drafted by the industry and therefore, it does not need to guarantee all of the client’s interests.

(standard) contractual terms/provisions in terms and conditions – a small-scale comparative study will demonstrate that the 15 biggest cloud providers handle the client’s data as follows in the event of the termination of the contract:\(^{19}\)

- 6 cloud providers offer their users the right to get back their data;
- 1 cloud provider may give users the option to have their data returned to them;
- 4 cloud providers may delete user data;
- 2 cloud providers automatically delete user data;
- 2 cloud providers have no provisions for users’ right to have their data returned.

As regards the period for retaining data and making the data available to users:

- 2 cloud providers keep data for 30 days;
- 1 cloud provider keeps data for 60 days;
- 1 cloud provider keeps data for 90 days;
- 1 cloud provider keeps data for "a commercially reasonable period of time";
- 1 cloud provider does not specify the period.

Data portability policies – examples included as APPENDIX 2.

Introduction of contractual terms/provisions

We consider contractual clear and understandable terms, preferably implemented by the industry, in combination with sufficient transparency, an effective solution. While users must be given a choice, they do not have to receive everything 'free of charge' (apart from rights such as the recorded data protection regulation).

We think the contract terms (or data portability policy) should at least include:

1) a definition of data;
2) whether data is portable;
3) in which format (maybe with the use of a technical standard?\(^{20}\)) the data is delivered;
4) the (reasonable) cost, if there are any;
5) for which period of time after the termination of the contract the provider preserves the data;
6) data cannot be deleted by the provider during an ongoing dispute, unless the removal is done at the customer’s request.

\(^{18}\) Dutch Hosting Provider Association, dhpa.nl
\(^{19}\) Overview of the terms and conditions of the biggest cloud providers from the Talkin’ Cloud 100 list (source: http://talkincloud.com/tc100), also see APPENDIX 4
\(^{20}\) Find an example of IaaS portability in appendix 5
Introduction of transparency about portability through the use of icons – this was briefly discussed at the first meeting. You can already see standard provisions which can be displayed in a brief summary. Take, for example, the summary displayed when installing android applications. This transparency may increase even further with an icon that can be used to indicate whether a user may transfer its metadata, whether this can be migrated to another cloud service and whether you need to pay for this. Of course, this should go hand in hand with a technological standard. Otherwise, you cannot determine whether or not data can be migrated.

Standardising the contract terms will clarify what the cloud service provider does and does not offer. This, combined with simple symbols (icons) or a traffic light system, should give users a choice.
APPENDIX 1   EXCERPT FROM THE PLANNED GENERAL DATA PROTECTION REGULATION

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the protection of individuals with regard to the processing of personal data and
on the free movement of such data (General Data Protection Regulation)

ARTICLE 15
RIGHT TO ACCESS AND TO OBTAIN DATA FOR THE DATA SUBJECT

2. The data subject shall have the right to obtain from the controller communication of the personal data undergoing processing. Where the data subject makes the request in electronic form, the information shall be provided in an electronic and structured format, unless otherwise requested by the data subject. Without prejudice to Article 10, the controller shall take all reasonable steps to verify that the person requesting access to the data is the data subject.

2a. Where the data subject has provided the personal data where the personal data are processed by electronic means, the data subject shall have the right to obtain from the controller a copy of the provided personal data in an electronic and interoperable format which is commonly used and allows for further use by the data subject without hindrance from the controller from whom the personal data are withdrawn. Where technically feasible and available, the data shall be transferred directly from controller to controller at the request of the data subject.

Recitals:

(51a) To further strengthen the control over their own data and their right of access, data subjects should have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain a copy of the data concerning them also in commonly used electronic format. The data subject should also be allowed to transmit those data, which they have provided, from one automated application, such as a social network, into another one. Data controllers should be encouraged to develop interoperable formats that enable data portability. This should apply where the data subject provided the data to the automated processing system, based on their consent or in the performance of a contract. Providers of information society services should not make the transfer of those data mandatory for the provision of their services.

(130) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission for: specifying standard forms in relation to the processing of personal data of a child; standard procedures and forms for exercising the rights of data subjects; standard forms for the information to the data subject; standard forms and procedures in relation to the right of access; the right to data portability; standard forms in relation to the responsibility of the controller to data protection by design and by default and to the documentation; specific requirements for the security of processing; the standard format and the procedures for the notification of a personal data breach to the supervisory authority and the communication of a personal data breach to the data subject; standards and procedures for a data protection impact assessment; forms and procedures for prior authorisation and prior consultation; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country or a territory or a processing sector within that third country or an international organisation; disclosures not authorized by Union law; mutual assistance; joint operations; decisions under the consistency mechanism. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the
Commission's exercise of implementing powers. In this context, the Commission should consider specific measures for micro, small and medium-sized enterprises.

(131) The examination procedure should be used for the adoption of specifying standard forms in relation to the consent of a child; standard procedures and forms for exercising the rights of data subjects; standard forms for the information to the data subject; standard forms and procedures in relation to the right of access; the right to data portability; standard forms in relation to the responsibility of the controller to data protection by design and by default and to the documentation; specific requirements for the security of processing; the standard format and the procedures for the notification of a personal data breach to the supervisory authority and the communication of a personal data breach to the data subject; standards and procedures for a data protection impact assessment; forms and procedures for prior authorisation and prior consultation; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country or a territory or a processing sector within that third country or an international organisation; disclosures not authorized by Union law; mutual assistance; joint operations; decisions under the consistency mechanism, given that those acts are of general scope.
APPENDIX 2   DATA PORTABILITY POLICY FOR .TEL DOMAINS

Telnic.org is the hub of the .tel community and the registry for .tel domains. This page is a work-in-progress centralizing information about portability of information stored in .tel domains.

A .tel domain is primarily a data Visitor in the sense that its main purpose is to be the central hub for all your communication channels, pointing at all the resources that you use to communicate, be they phone numbers, email addresses or blogs.

A .tel domain does not broadcast updates: its data is served by DNS servers which behave as on-demand "pull" repositories.

Whatever registrars .tel domains are purchased from, they can be accessed via common read and write APIs. These APIs provide Delegated Access, Personal Backup and Public Data.

.tel domain zone files are normally deleted along with their associated data when the ownership lapses and/or changes hands.

**APIs and Data Formats**

.tel domains can be managed by a set of published APIs on the Telnic Developer Portal. The format of the complete import/export data structures is located within the WSDL file of the SOAP API specification. TelHosting Provider’s systems must allow Domain Name holders to import and export domain contents and metadata, including any protected contacts, readers and groups, and profile provisioning data in an XML format.

Reading .tel information is achieved through DNS queries for NAPTR, TXT, NINFO, LOC and other record types on the relevant .tel domain. The anatomy of a .tel domain is described in the Developers Manual for .tel Client Applications.

**Identity and Authentication**

Create a new Identity - .tel domains are globally unique, their purpose is to be a single point of contact for the owner. A Domain Name holder can have a portfolio of multiple domains, all managed by one or multiple accounts at one or multiple registrars or TelHosting providers. Authentication to manage .tel domains can be done via a standard username/password web interface or via OAuth WRAP. .tel domains are also OpenID providers, in the sense that you can connect to OpenID-enabled sites with your .tel domain.

**Working with Things Stored Somewhere Else**

Home and Visitor - Your .tel domain is a central switchboard for all your communication channels, and its main purpose is to publish all the means by which you can be communicated with. It is not a content platform, but it stores and publishes links to your content.

**Watching For Updates**

No Imports - .tel domains don’t automatically watch for updates to your communication channels or personally identifiable data. However, third-party software products exist that utilize the TelHosting APIs to provide 2-way linkages with other services such as Twitter.

**Broadcasting Changes Made Here**

Silent - When you modify data in your .tel domain, the zone file for your domain is updated but the changes are not broadcast.

**Delegated Access**

Other Products Can Read and Write - Any device has read access to your published public data in your .tel domain through DNS queries. Published private data is encrypted using PKI and hidden in
individual subdomains to be accessed only by the targeted entities. Products can be given different levels of write access via OAuth WRAP protocol.

**Personal Backup**

Every accredited TelHosting Provider must support exporting and importing all of a user's data via the SOAP API's ExportData() method. This is to ensure that .tel owners are independent and can switch TelHosting providers and registrars as needed.

**Public Data**

Full access - A person can make use of any publicly published data on any .tel domain.

**Account Mortality**

Accounts Deleted upon Expiration - When a .tel domain ownership expires or is transferred, the data is normally automatically unpublished and the orphan TelHosting account subsequently deleted.

**Termination**

.tel domains are allocated for fixed periods of time with current holder having a priority right for renewal. At the conclusion of the registration period failure to renew the domain within the time determined by the registrar shall normally result in cancellation of registration. The previous holder can still redeem the domain within 30 days after such cancellation has been done, subject to its payment of the redemption fee. Cancelled (deleted) domains, upon expiration of all applicable post-expiration periods (normally 35 days) become available for re-registration.

**Appeal**

The .tel domain names are subject to the Uniform Domain Name Dispute Resolution Policy (UDRP), which establishes a procedure for resolving certain trademark disputes relating to domain names. You can also seek redress in court. Please get a qualified legal advice to determine the appropriate venue for resolution of your dispute

**Where Things are Stored**

Data is stored at the registrar or TelHosting provider's data centers. Furthermore, cached copies of your data can reside on relaying DNS servers at any point in time, due to the nature of the distributed DNS infrastructure.

Source: [http://www.telnic.org/portabilitypolicy.html](http://www.telnic.org/portabilitypolicy.html)
APPENDIX 3  
TEN QUESTIONS REGARDING THE MODEL DATA PORTABILITY POLICY COMMISSIONED BY THE DATA PORTABILITY PROJECT

1. Are your APIs and Data Formats Documented? (Yes/No/Doesn't Apply)

2. Do people need to create a new identity for this product, or can they use an existing one? (Fresh Start, Existing Identity, Doesn't Apply)

3. Must people import things into this product, or can the product refer to things stored someplace else? Can this product work with objects and information whose "authoritative home" is another product, or can this product only work with things that it hosts directly? (Home, Visitor, Doesn't Apply)

4. Can this site watch for updates that people make on other sites? In cases where the product tracks or manages things that the person has stored on some third party product, can this product automatically keep itself up to date? (No Imports, One Time Import, Watch For Updates, Doesn't Apply)

5. If person updates something here, is that change stored only here or can it notify another product? Does this product provide a way for others to ask for updates? (Silent, Chatty, Doesn't Apply)

6. Can the person allow other sites to use the things they've created or updated here? Does this product provide a way for third parties to authenticate a person and read or write? (No Access, Other Products Can Read, Other Products Can Write, Doesn't Apply)

7. Can the person download or remotely access a copy of everything they've provided to this service? As part of their standard use of most products, people import or create things. Does this product provide an open, DRM-free way for people to retrieve or access via third party all of the things they've created or provided? (No Download, Some Download, Full Download, Doesn't Apply)

8. Can the person download or remotely access information that others have provided to the product? In cases where the product allows download or remote access, can the person export or access all of the data to which they have access, or only data which they have directly created? (Provider Only, Full Access, Doesn't Apply)

9. Will this site delete an account and all associated data upon a user's request? If the user creates a password or account for use with this product, does the product provide a way to cancel the account and erase all data associated with it? (Immortal Accounts, Data Expires, Accounts Deleted Upon Request, Doesn't Apply)

10. Do you disclose where my data is being kept in the real world? If Yes, where can I learn where my data is kept? Can I request to have my data stored in one jurisdiction or another? (Yes, No, Doesn't Apply)

APPENDIX 4  TOP CLOUD COMPUTING SERVICES PROVIDERS

1. Salesforce:
4.4 Master Subscription Agreement
12. TERM AND TERMINATION
12.5. Your Data Portability and Deletion. Upon request by You made within 30 days after the effective date of termination or expiration of this Agreement, We will make the Your Data available to You for export or download as provided in the Documentation. After that 30-day period, We will have no obligation to maintain or provide Your Data, and will thereafter delete or destroy all copies of Your Data in Our systems or otherwise in Our possession or control as provided in the Documentation, unless legally prohibited.
Source:  http://www.salesforce.com/company/legal/agreements.jsp

2. Amazon Web Services:
7.3. Effect of Termination.
(b) Post-Termination Assistance. Unless we terminate your use of the Service Offerings pursuant to Section 7.2(b) [Termination for Cause], during the 30 days following termination:
(i) we will not erase any of Your Content as a result of the termination;
(ii) you may retrieve Your Content from the Services only if you have paid any charges for any post-termination use of the Service Offerings and all other amounts due; and
(iii) we will provide you with the same post-termination data retrieval assistance that we generally make available to all customers.
Any additional post-termination assistance from us is subject to mutual agreement by you and us.
Source:  http://aws.amazon.com/agreement/

3. Microsoft Office 365
Online Services Use Rights: January 2014 r.
Online Service Expiration or Termination
Upon expiration or termination of your online service subscription, you may contact Microsoft and tell us whether to:
disable your account and then delete the Customer Data; or
retain your Customer Data stored in the online service in a limited function account for at least 90 days after expiration or termination of your subscription (the “retention period”) so that you may extract the data.
If you indicate (1), you will not be able to extract the Customer Data from your account. If you do not indicate (1) or (2), we will retain the Customer Data in accordance with (2).
Following the expiration of the retention period, we will disable your account and delete your Customer Data. Cached or back-up copies will be purged within 30 days of the end of the retention period.
The online service may not support retention or extraction of software provided by you to run in the online service.
NO LIABILITY FOR DELETION OF CUSTOMER DATA
You agree that, other than as described in these terms, we have no obligation to continue to hold, export or return the Customer Data. You agree that we have no liability whatsoever for deletion of the Customer Data pursuant to these terms.


4. **Oracle cloud:**

ORACLE CLOUD SERVICES AGREEMENT

3. RIGHTS GRANTED

3.3 To enable Oracle to provide You and Your Users with the Services, You grant Oracle the right to use, process and transmit, in accordance with this Agreement and Your order, Your Content and Your Applications for the duration of the Services Period plus any additional post-termination period during which Oracle provides You with access to retrieve an export file of Your Content and Your Applications. If Your Applications include third party programs, You acknowledge that Oracle may allow providers of those third party programs to access the Services Environment, including Your Content and Your Applications, as required for the interoperability of such third party programs with the Services. Oracle will not be responsible for any use, disclosure, modification or deletion of Your Content or Your Applications resulting from any such access by third party program providers or for the interoperability of such third party programs with the Services.

3.4 Except as otherwise expressly set forth in Your order for certain

9. SERVICES PERIOD; END OF SERVICES

9.2 Upon the end of the Services, You no longer have rights to access or use the Services, including the associated Oracle Programs and Services Environments; however, at Your request, and for a period of up to 60 days after the end of the applicable Services Period, Oracle will make available Your Content and Your Applications then in the Services Environment for the purpose of retrieval by You. At the end of such 60 day period, and except as may be required by law, Oracle will delete or otherwise render inaccessible any of Your Content and Your Applications that remain in the Services Environment.


5. **Google:**

Google Apps for Business (Online) Agreement

11. Termination.

11.2 Effects of Termination.

If this Agreement terminates, then: (i) the rights granted by one party to the other will cease immediately (except as set forth in this Section); (ii) Google will provide Customer access to, and the ability to export, the Customer Data for a commercially reasonable period of time at Google’s then-current rates for the applicable Services; (iii) after a commercially reasonable period of time, Google will delete Customer Data by removing pointers to it on Google’s active servers and overwriting it over time; and (iv) upon request each party will promptly use commercially reasonable efforts to return or destroy all other Confidential Information of the other party. If a Customer on an annual plan terminates the Agreement prior to the conclusion of its annual plan, Google will bill Customer, and Customer is responsible for paying Google, for the remaining unpaid amount of Customer’s annual commitment.

6. **Sap:**

Problem z formatem plików
Sap uczestniczy w inicjatywie mającej na celu standaryzację
Source: https://www.oasis-open.org/news/pr/tosca-tc

7. **Softlayer (IBM):**

Master service agreement

16. TERMINATION.

16.4 Access to Customer Content. The deletion of Customer Content is automatic upon termination or expiration of the MSA. Consequently, unless SoftLayer determines otherwise, Customer will not have access to Customer Content, and SoftLayer may immediately erase or delete Customer Content from its computer infrastructure after the effective date of termination or expiration of this MSA.

16.5 Effect of Termination. Upon expiration or termination of the MSA, Customer must discontinue use of the Services and relinquish use of the IP addresses and server names assigned to Customer by SoftLayer and any other materials provided to Customer by SoftLayer in connection with the Services, including pointing the DNS for Customer domain name(s) away from the Services. SoftLayer will have no obligation to provide any transition services or access to data except as expressly stated in Section 16.4 above.


8. **Terremark (Verizon):**

Terremark Cloud Service Agreement

3.7. Data Preservation in the Event of Suspension or Termination.

3.7.1. Suspension Other Than for Cause. In the event of a suspension by Us of Your access to any Services for any reason other than a for cause under Section 3.4., during the period of suspension, (i) We will not take any action to intentionally erase any of Your data stored on the Services; and (ii) applicable Service data storage charges will continue to accrue.

3.7.2. Termination Other Than for Cause. In the event of any termination by Us of any Service or any set of Services, or termination of this Agreement in its entirety, (other than for cause under Section 3.4.), We will take immediate action to erase any of Your data stored on the Services upon the effective date of termination.

3.7.3. Other Suspension or Termination. Except as provided in Sections 3.7.1. above, We shall have no obligation to continue to store Your data during any period of suspension or termination or to permit You to retrieve the same.

9. **Rackspace:**
Cloud Terms of Service

12. **ACCESS TO DATA.**

12.1 You will not have access to your data stored on the Services during a suspension or following termination.

12.2 You have the option to create a snapshot or backup of your Cloud Servers or Databases, respectively, however, it is your responsibility to initiate the snapshot or backup and test your backup to determine the quality and success of your backups. You will be charged for your use of backup services as listed in your Order.

12.3 Although the Rackspace Cloud services may be used as a backup service, you agree that you will maintain at least one additional current copy of your programs and data stored on the Cloud system somewhere other than on the Cloud system. If you utilize Rackspace Cloud backup services, you are responsible for performing and testing restores as well as testing your systems and monitoring the integrity of your data.

Source: http://www.rackspace.com/information/legal/cloud/tos

10. **Netsuite:**
No provisions

11. **Dropbox:**
Dropbox for Business Agreement

**Term & Termination.**

1. **Effects of Termination.** If this Agreement terminates: (i) the rights granted by Dropbox to Customer will cease immediately (except as set forth in this section); (ii) the rights granted by Dropbox to End User will cease immediately; (iii) Dropbox may provide Customer access to its account at then-current rates so that Customer may export its information; and (iv) after a commercially reasonable period of time, Dropbox may delete any data relating to Customer’s account. The following sections will survive expiration or termination of this Agreement: 1(c) (Administrator Control), 2(e) Third Party Requests, 6 (Intellectual Property Rights), 8 (Disclaimers), 9 (Fees & Payment), 10(d) (End User Termination), 10(e) (Effects of Termination), 11 (Indemnification), 12 (Limitation of Liability), and 13 (Miscellaneous).

Source: https://www.dropbox.com/privacy#business_agreement

12. **Savvis:**
Terms and Conditions

7.4. **Effect of Termination.**

Upon any termination of this Agreement: (i) all your rights under this Agreement immediately terminate, (ii) you remain responsible for all fees and charges you have incurred through the date of termination, (iii) you will immediately return or, if instructed by us, destroy all SavvisDIRECT materials in your possession, and (iv) Sections 7, 8, 9, 10, 11, 15, 18 and all other provisions that by their nature are intended to survive expiration or termination of the Agreement will continue to apply in accordance with their terms. If the Agreement or a Service is terminated pursuant to Sections 7.1(iii),
7.2 or 7.3, when such termination is effective, you may have no further access to the Service or your content and your content may be erased by Savvis.

Source: http://www.savvisdirect.com/terms-conditions

13. **Joyent:**

Terms of Service

D. Customer Data Preservation. You are responsible for the preservation of all of your Customer Data. You, and not Joyent, are responsible for backing-up Customer Data and any other content that you use with the Cloud Services. Best practices include routine archiving of Customer Data. Joyent is not obligated to retain any Customer Data after the termination of your access to the Cloud Services for any reason. Joyent may transfer Customer Data within a major geographic region (for example, within the United States or within Europe) for data redundancy or other purposes. Joyent will not transfer Customer Data outside the major geographic region you specify (for example, from the United States to Asia or from Europe to the United States).

Source: http://www.joyent.com/company/policies/terms-of-service

14. **Citrix:**

No provisions


15. **Zoho:**

Terms of Services

Suspension and Termination

We may suspend your user account or temporarily disable access to whole or part of any Service in the event of any suspected illegal activity, extended periods of inactivity or requests by law enforcement or other government agencies. Objections to suspension or disabling of user accounts should be made to legal@zohocorp.com within thirty days of being notified about the suspension. We may terminate a suspended or disabled user account after thirty days. We will also terminate your user account on your request. In addition, we reserve the right to terminate your user account and deny the Services upon reasonable belief that you have violated the Terms and to terminate your access to any Beta Service in case of unexpected technical issues or discontinuation of the Beta Service. Termination of user account will include denial of access to all Services, deletion of information in your user account such as your e-mail address and password and deletion of all data in your user account.

Source: http://www.zoho.com/terms.html

5. **DIMENSION DATA**

Terms of Service - Public CaaS Terms of Service

Effect of Termination

15.4 Upon expiration or termination of this Agreement or any Order:

- (a) Dimension Data will cease providing the applicable Services and Client’s rights and licenses granted under this Agreement with respect to those Services will immediately terminate;
- (b) all outstanding invoices as well as any Early Termination Fees (if applicable) will become immediately due and payable; and
(c) Dimension Data will not be required to maintain or store, and may delete, Client Content hosted or stored in connection with the terminated Services, unless otherwise agreed in the applicable Order.

Source: http://nacloud.dimensiondata.com/Legal/TOS
APPENDIX 5    Description customer environment and Backup

Backup specifications

Provider A provides Infrastructure as a Service to its customers. Customers build their applications or other customer environments with the use of the IaaS. The back-up includes all the customer data and the data necessary for the Provider B to be able to reactivate the customer’s environment on the IaaS level.

Provider A needs to fill in the table below in consultation with the customer and Provider B. Provider A offers the completed tablet to the trusted third party. The trusted third party decides if and when Provider B has to activate the Backup.

The table includes details related to the Backup and additional information relating to the customer’s environment. With the information Provider B together with the customer are able to activate the Backup if necessary.

Backup requirements

1) The server on which the Backup is placed must be physically located in the European Union;
2) Provider A is responsible for the transmission of the Backup. Provider A transmits the Backup once every day unless other arrangements are made;
Provider B is responsible for receiving and storing the Backup (also once every day unless other arrangements are made)

<table>
<thead>
<tr>
<th>Date:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provider A:</td>
</tr>
<tr>
<td>Provider B:</td>
</tr>
<tr>
<td>Customer environment:</td>
</tr>
<tr>
<td>Service: IaaS</td>
</tr>
<tr>
<td>Onderwerp</td>
</tr>
<tr>
<td>Customer Environment</td>
</tr>
</tbody>
</table>
| Scope | Scope Service provider A and Service provider B | Specify:  
  - Service provider A: IaaS  
  - Service provider B:  
    (IaaS, PaaS or Saas) |
| Tenancy | Fixation of tenancy model Provider A and tenancy model | Specify tenancy type: |

---

21 The table is part of the arrangement developed by the Dutch Hosting Provider Association together with ICTRecht for the continuity of an IaaS service should an IaaS provider go bankrupt
<table>
<thead>
<tr>
<th><strong>Activation and RTO</strong></th>
<th><strong>Provider B.</strong></th>
<th><strong>dedicated environment or instance in an existing environment.</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Within 24 hours after activation notification by TTP</strong>, <strong>recovery within 48 hours after activation</strong></td>
<td>If the set schedule is not feasible or sufficient: specify the alternative scenario &amp; timing</td>
<td></td>
</tr>
</tbody>
</table>

| **RPO** | **Maximum loss of data: one (1) day** | If the set maximum is not feasible or sufficient: specify the maximum loss of data |

## Technical and operational set up

### DNS
- **Domain and zone files can be changed without the involvement of Provider A**
  - Fill in the registrar, method of modifying the zone files; where applicable: access data

### Data
- **List of data sources within the Backup such as Vserver images, databases, filesystems**
  - State purpose, type, brand and version of software

### Replication methods
- **For each data source:**
  - Method of replication
  - Method of encryption
  - Data format
  - Frequency
  - Control
  - Rsync, ftp, etc.
  - Transport and/or files
  - zip, tarballs, files
  - Continuously/timing
  - Controlemechanism(s)

### Passwords
- **Summary of all accounts, user id’s, passwords, including keys for encryption which are of any importance for the hosting service.**
  - Pay special attention to passwords used internally by Provider A (database connections etc.)
  - Method of logging on
  - Method of retention and storage.
  - Describe how Provider B is able to access the information

### Software
- **Summary of used operating systems, platform and software package**
  - Full list of software relevant to the customer environment.
  - The aim is to check whether the Backup is compatible

### Capacity
- **Definition of the required capacity for both replication**
  - Number of Gbytes of storage
  - Number of servers: cpus, storage,

---


<table>
<thead>
<tr>
<th>(Backup) and IaaS-service</th>
<th>RAM; external storage, network, bandwidth.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Certificates</strong></td>
<td>Summary and transferal SSL client- and server certificates.</td>
</tr>
<tr>
<td></td>
<td>Methode of storage.</td>
</tr>
<tr>
<td></td>
<td>In case of private keys - see passwords.</td>
</tr>
<tr>
<td></td>
<td>For the transfer: see Data.</td>
</tr>
<tr>
<td><strong>Location</strong></td>
<td>The co-location of Provider B should not be at the same location as the location used by Provider A for its co-location, but it is, if required by the customer, in the same jurisdiction as that of Provider A</td>
</tr>
<tr>
<td></td>
<td>Specify the location used by Provider B for its co-location and other agreements with the customer about access to its data</td>
</tr>
<tr>
<td><strong>Network</strong></td>
<td>Summary of relevant network information</td>
</tr>
<tr>
<td></td>
<td>• Relevant IPv4 addresses</td>
</tr>
<tr>
<td></td>
<td>• Relevant VPN’s</td>
</tr>
<tr>
<td></td>
<td>• Routering</td>
</tr>
<tr>
<td></td>
<td>• Firewall rules</td>
</tr>
<tr>
<td></td>
<td>• Connectivity to third parties</td>
</tr>
<tr>
<td><strong>Configuration</strong></td>
<td>List of configuration files or configuration options</td>
</tr>
<tr>
<td></td>
<td>Configuration files such as webserver configurations are considered to be data. Other configurations are described and assessed</td>
</tr>
<tr>
<td><strong>Hardware</strong></td>
<td>Describe special hardware such as special servers, 'dongels', network devices, modems etc.</td>
</tr>
<tr>
<td></td>
<td>If possible, describe the solution with regard to this ‘special’ hardware. For instance:</td>
</tr>
<tr>
<td></td>
<td>• By purchasing this hardware; or</td>
</tr>
<tr>
<td></td>
<td>• Work-arounds</td>
</tr>
</tbody>
</table>