CLOUD ACCOUNTABILITY PROJECT

D-4.4 Remediation guidelines and tools

Deliverable Number:	D44.4
Work Package:	WP 44
Version:	Final
Deliverable Lead Organisation:	TiU
Dissemination Level:	PU
Contractual Date of Delivery (release):	31 December2015
Date of Delivery:	22 December2015

Editor
Dimitra Stefanatou (TiU)

Contributors
Ronald Leenes (TiU), Martin Gilje Jaatun (SINTEF), Vasilis Tountopoulos (ATC), Christian Frøystad (SINTEF), Anderson Santana de Oliveira (SAP), Lorenzo Dalla Corte (TiU), Chris Reed (TiU), Eleni Kosta (TiU), Dimitra Stefanatou (TiU), Rehab Alnemr (HP), Brian Dziminski (QMUL), Kees Stuurman (TiU), Colette Cuijpers (TiU), Maurice Schellekens (TiU), Adele Calamo Specchia (TiU), Niamh Christina Gleeson (QMUL), Alexandr Garaga (SAP), Bryce Newell (TiU)

Reviewer(s)
Alain Pannetrat (CSA), Siani Pearson (HP)

SEVENTH FRAMEWORK PROGRAMME

Executive Summary

This deliverable contains guidance for remediation in the event of data protection violations occurring in the cloud computing setting. To this end, the document presents two technical tools, the Incident Management Tool (IMT) and the Remediation and Redress Tool (RRT). These tools respond to the needs of different actors, namely, to the needs of cloud providers and cloud subjects[1].

As far as the broader issue of digital security is concerned, there is wide agreement that it is vital to help mitigate potential losses (e.g. economic consequences, lawsuits) arising from incidents, making cloud-specific incident handling and effective mechanisms for providing redress critical components of any plan to adequately address these problems. The cloud computing environment is, especially, prone to incidents—which, for the sake of the present analysis, are defined as follows: "any event, deliberate or not, that infringes the contracts, policies or regulations applicable to the cloud service in place. "Certain types of incidents are cloud specific, while others are common in all information technology (IT) settings. However, current approaches to incident handling are not tailored to the particularities of the cloud, and individuals affected by data protection violations across EU Member States hesitate to seek remediation.

Both incident management and remediation are hard to define in a uniform way across disciplines. From a technical point of view, what might be considered an "*incident*" under a certain taxonomy might not be covered at all by law; similarly, a corrective technical action might very well remedy a technical failure, while the outcome of a request for a legal remedy is not only uncertain but, also, often inadequate to ensure full restoration. For instance, financial compensation following a personal data breach is a form of legal remedy, but financial damages cannot entirely repair non-monetary harms.

IMT is targeted at organisations and teams that handle computer security incidents involving personal data, which in practice amounts to any organisation providing or consuming internet services. The target audiences for IMT, therefore, are professional incident handlers and privacy officers. IMT produces a simplified incident format and a simplified incident exchange protocol—making the solution usable for small companies as well as large ones. The tool provides support across cloud service provisioning chains, while maintaining traceability of incidents as they make their way through the chain. Integrating the tool within the A4Cloud toolset allows the incident handler to send notifications to the affected end users.

RRT aims to assist cloud data subjects to respond to (perceived) incidents related to the handling of their personal data in the cloud, as well as alleviating the difficulties that individual cloud subjects have in accessing judicial or administrative remedies. If an incident occurs (as identified by IMT), RRT is triggered and proceeds to identify what type of incident has occurred and what possible actions can be taken. It then guides the user through a set of possible corrective actions, both technical (e.g. change of password) and legal (e.g. submission of a complaint to the competent supervisory authority). In view of the latter option, the tool produces "accounts" of the incident including a simple chronicle of the event (e.g. what happened, when it happened, etc.) and a report with technical evidence (e.g. logs); the latter can potentially support individual cloud subjects to sustain their claims in court.

These tools to be discussed in detail in this document fit the set of A4Cloud tools assisting in reporting, controlling the data operations or providing information/advice as it is the case for other project tools such as the Accountable Privacy Policy Language (A-PPL), the Audit Agent System (AAS) or the Transparency Log. In particular, the IMT -primarily- supports reporting, RRT supports providing information/advice, while they both strengthen the exercise of control on processing operations. Moreover, IMT and RRT form clear examples of how automated processes and human decision making may intertwine in the same case: the notification of incidents by IMT to RRT is automated, while the final decision on whether -and when- a specific incident should be notified to end user or competent authorities may be up to a Privacy Officer or a head of an IT department to decide.

[1] A detailed description of all cloud roles identified by the project can be found in Dziminski et al., "D:C-2.1*:* Report detailing conceptual framework", page 3, available at: http://www.a4cloud.eu/sites/default/files/D32.1%20Conceptual%20Framework.pdf

Table of Contents

Executive Summary 2

1 Introduction 5

1.1 Setting the scene 5

1.2 Remedies in general 6

1.3 Accountability in relation to incident handling and remedies 7

1.4 Aims of the Deliverable 8

1.5 Outline of the Deliverable 8

2 Incidents in a cloud ecosystem 9

2.1 Introduction 9

2.2 Incident detection and management 9

2.3 The impact of cloud incidents 11

3 Remedies for data protection violations in the cloud 13

3.1 Setting the scene of relevant terms in common law and civil law countries 13

3.2 Regulatory framework for redress and remediation 15

3.3 Cloud providers, regulators and the A4Cloud toolset 19

3.4 Data subject redress and remediation under the regulatory framework 20

3.5 Data subject redress and remediation via contractual liability 22

3.6 Data subject redress under extra-contractual liability 24

3.7 Proving a data subject's claims 25

4 Use case scenarios 27

4.1 Virtual Machine (VM) Migration 27

4.2 Data retention violation 30

4.3 Lost laptop 31

4.4 Misconfiguration 32

4.5 Data access attempt for illegitimate purposes 33

4.6 Right to know vs. Need to know 33

4.7 Unavailability 34

5 Incident Management Tool (IMT) 35

5.1 Introduction 35

5.2 General Concept 35

5.3 User Interface 36

5.4 Incident Format 38

5.5 Incident Exchange API 41

6 The Remediation and Redress Tool (RRT) 43

6.1 Overview 43

6.2 RRT functional specifications 43

6.3 The high level architecture of RRT 44

6.4 Current implementation aspects 45

7 IMT and RRT as accountability tools 51

7.1 IMT and RRT as accountability tools in the cloud environment and other future Internet services 51

8 Conclusions 55

9 References 57

10 Appendices 59

Appendix 1 59

11 Index of Figures 70

12 Index of Tables 70

1 Introduction

This section gives a general overview of incident management and remedies for data protection violations relevant, also, for the cloud computing context. To this end, it first points out the increasing importance of digital security and the need to strengthen users' sense of control over processing operations. Second, it provides a high level discussion about remedies, highlighting certain differences across legal systems. Third, it reflects briefly on the relation between incident handling and accountability. Finally, the Section below explains the aims of this Deliverable and sets the outline for the discussion to follow.

1.1 Setting the scene

On the 7th of December 2015, Member States of the European Union (EU) agreed on the first cybersecurity law to provide for multiple industry sectors[2,3]. The agreement reached reflects the attention digital security has been gaining over the years due to the growing number of incidents leading to severe consequences for the public and private sector as well as for individuals. These consequences can create a technical, economic, legal and societal impact as, for example, reputation damage, loss of trust, lawsuits and the denial of service[4]. The occurrence of incidents, therefore, affects several parties; a breach of personal data, for instance, affects the individuals to whom personal data relate, as well as the reputation of the company that was targeted, and even the confidence in cloud services of society at large may be affected. The impact of such incidents, obviously, increases significantly in environments like cloud computing that allow for massive processing of information and where several actors are involved, on the other hand the concentration of data at a limited number of organizations allows them to put spend more resources on security.

The involvement of multiple actors processing information through the cloud further increases dependencies both in business to business and in business to consumers relationships, compared to outsourcing in general. These dependencies are reflected in the set of the cloud accountability roles identified by the project to describe effectively the complexity of the cloud and how different stakeholders relate to it[5]. In particular, the project has identified seven cloud accountability roles, amongst which figure the:

1) "Cloud Subject: An entity whose data is processed by a cloud provider, either directly or indirectly. When necessary we may further distinguish:
   a) Individual Cloud Subject, when the entity refers to a person
   b) Organisation Cloud Subject, when the entity refers to an organisation
2) Cloud Customer: An entity that (1) maintains a business relationship with, and (2) uses services from a Cloud provider. When necessary we may further distinguish:
   a) Individual Cloud Customer, when the entity refers to a person
   b) Organisation Cloud Customer, when the entity refers to an organisation
3) Cloud provider: An entity responsible for making a [cloud] service available to Cloud Customers."

A cloud subject may, thus, rely when making use of a service upon an organisational cloud customer, who could then rely on a cloud provider and thereby, potentially, on a set of other actors as, for instance, on cloud carriers and cloud brokers. This increased level of dependencies decreases, therefore, the sense of control, primarily, of cloud customers and cloud subjects over processing.

Moreover, cloud subjects do not have often the actual resources, primarily, the necessary knowledge, that would allow them to better understand the complexities of the cloud setting and, potentially, take action. Small and Medium Enterprises (SMEs), for instance, mostly do not have an IT department or a Privacy Officer that could guide them properly on the occurrence of an incident. From this point of view, security issues and incidents in general, bring about the power asymmetries innate to the cloud offered

[2]European Commission - Press release: Commission welcomes agreement to make EU online environment more secure, available at: http://europa.eu/rapid/press-release_IP-15-6270_en.htm

[3] European Commission, "Proposal for a Directive of The European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union", COM (2013) 48 final, 2013/0027 (COD), Brussels, 7.2.2013.

[4]OECD (2015), Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/9789264245471-en

[5] n 1.

services and explain the reluctance and difficulties of the affected parties to take action and seek remedies for the damage suffered.

1.2 Remedies in general

Remediation in essence is based upon a prior failure of compliance with obligations, which result mostly from law[6] and which may dictate actions or omissions. Given, therefore, that laws and contracts provide for obligations they provide as well for the right to remedies. In this context, the remedies appear to be the legal consequences, in case certain obligations are not met. It should be noted that laws essentially address remedies rather broadly, while contractual agreements that are tailored to the needs of the parties usually include specific indemnifying clauses[7].

As far as the scope of the A4Cloud is concerned, these obligations, primarily, relate to data protection[8].With respect to this specific domain, the Data Protection Directive (1995/46/EC) frames broadly the issue of remedies for the EU context, which are further detailed national laws. The upcoming General Data Protection Regulation (GDPR)[9] is expected to increase the level of harmonisation across Member States, strengthening the powers of Data Protection Authorities and empowering them to impose high administrative fines.

The allocation of liabilities is a key issue linking to remedies both in respect to personal data protection and business sensitive information, given that remedial actions are always sought by the entities held liable (meaning, legally responsible). In practice, this means that the entities having suffered the damages may turn against those held liable. Cloud computing agreements include, though, clauses limiting the liabilities of cloud providers, in order to exempt them from the obligation of, most probably costly, remedial actions (e.g. indemnification). Nevertheless, the Cloud Security Alliance highly recommends that cloud contracts indicate exactly

> "what remedies are available to the cloud customer in the event the CSP [Cloud Service Provider]—and/or the CSP's subcontractors—breaches its contractual obligations (...)such as whether contractual remedies are available for failure to meet data security, monitoring, data breach notification, data portability and/or data retention obligations. Remedies could include compensation for certain types of damages, service credits, and/or contractual penalties (financial or otherwise, including the ability to sue the cloud service provider."[10]

The issue of remedies is an area where civil law and common law tradition take different approaches. In particular, it is considered that

> "civil law focuses on rights and obligation, while common law is oriented towards the jurisdiction of particular courts to grant the sought-after remedy ('remedies precede rights'). It follows that the civil law does not have a clearly defined system of remedies, but relies rather on the courts to choose or even create the appropriate remedy. Conversely, the common law does not have a unitary system of rights and obligations. Courts having a jurisdiction to hear a matter falling within a cause of action set the rights and obligations *au fur et a measure* that they are called to rule on

[6]A4Cloud adopts a rather broad approach on the notion of obligations. Obligations may stem from regulations contracts and social and ethical sources. The notion of obligations is discussed extensively under the project deliverables "D:C-2.1: Report detailing conceptual framework" and "D:C-4.1: Policy Representation Framework", available at: http://www.a4cloud.eu/deliverables

[7] This is not the case for standard cloud contracts that include liability disclaimers in favour of cloud providers. For more on cloud contracts, see, also, the A4Cloud deliverables "D: D-4.2 Report of survey of cloud contract terms" to be published on www.a4cloud.eu. and "D: D-4.3 Guidelines and tools for cloud contracts", currently under review.

[8]Note that the confidentiality obligations for business sensitive information, also, fall under the project's scope. Given that they were not considered relevant for the deployment of technical tools discussed, they are not addressed under the present analysis.

[9] Commission, "Proposal for a 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)"COM 2012 (011) final

[10] Cloud Security Alliance, Privacy Level Agreement Working Group, "Privacy Level Agreement Outline for the Sale of Cloud Services in the European Union, February 2013, available at: https://downloads.cloudsecurityalliance.org/initiatives/pla/Privacy_Level_Agreement_Outline.pdf

them; it is only through precedents that specific rights (always in relation to cause of action) can be found."[11]

Of course, this difference does not apply in absolute terms, given that courts in civil law jurisdictions might, also, decide on the appropriateness of the remedy to be enforced.

Finally, it is worth noting that remedies are considered to contribute to legal certainty, also, within the specific setting of cloud computing. In particular, the Article 29 Working Party states in this respect that in order for a contractual agreement to ensure legal certainty, the contract should set forth, among other things, the

> "Details on the (extent and modalities of the) client's instructions to be issued to the provider, with particular regard to the applicable SLAs (which should be objective and measurable) and the relevant penalties (financial or otherwise including the ability to sue the provider in case of non-compliance)."[12]

The reference to penalties as a means for legal certainty includes both concrete remedial actions of a financial nature, as well as the "ability" to make use of redress/recourse mechanisms by filing a lawsuit. Although the Article 29 Working Party here focuses on the protection of personal data in the cloud, it is being argued that this specific recommendation could easily apply irrespective of the material scope, and therefore, extend to other legal domains as, for instance, consumer law protection.

1.3 Accountability in relation to incident handling and remedies

In the broader IT literature relevant for accountability[13], there are three dimensions assigned to accountability, the preventive, the detective and the corrective. These stages can also be found in incident management. ISO:27035 on incident management distinguishes "prepare", "identify", "assess", "respond" and "learn". Detection in this model is decomposed into identify and assess and the ISO model incorporates a feedback cycle. Accountability maps onto incident management in the sense that an accountable organization can and will provide information (transparency) about incident management in general and the specific phases more concretely. It will also be accountable for the actions taken in each of the stages.

Incident management is aimed at preventing incidents and resolving consequences should an incident occur. Prevention is insufficient in itself

> "There is no such thing as an absolute guarantee that preventive measures will be sufficient to prevent an attack. When complemented with measures aimed at the detection of attempts to intrude a secured infrastructure however, it is possible to minimise the chances of a successful intrusion.''[14]

Accountability aims at taking this process seriously by provides transparency about the incident handling process and taking responsibility for it. Accountability therefore has to "wrap around" the incident management process in its different dimensions: conceptual, technical and organisational. It affects how organisations are structured at a higher level and how responsibilities are distributed within an organisation and service provision chain. The report compiled following an attack with a great impact[15] states in this respect:

> "It is also important to enforce a strict separation in the tasks with competing aims that employees perform, insofar as these tasks may affect the security of the organisation or its infrastructure."

Furthermore, the accountability based approach adopted by the A4Cloud project assigns a key role to the notion of the "account'', which provides the documentation of the process and remedies. The account must give answers to a set of questions i.e who, what, where, when, why and how, while often including

[11] Tetley, William. "Mixed Jurisdictions: Common Law v. Civil Law (Codified and Uncodified)." *La. L. Rev.* 60 (1999): 677, available at: http://digitalcommons.law.lsu.edu/cgi/viewcontent.cgi?article=5822&context=lalrev

[12] Article 29 Working Party, Opinion 05/2012 on Cloud Computing WP 196, adopted on the 1st of July 2012, section 3.4.2.

[13] S. Pearson, "Accountability in Cloud Service Provision Ecosystems'', Secure IT Systems, 19th Nordic Conference, NordSec 2014, Tromsø, Norway, October 15-17, 2014, Proceedings, ed. Springer

[14] " Black Tulip", Report of the investigation into the DigiNotar Certificate Authority breach, August 2012, available at: https://www.rijksoverheid.nl/documenten/rapporten/2012/08/13/black-tulip-update

[15] Ibid

measures taken “to remedy a breach or failure and to prevent such breaches or failures in the future.”[16]The account may take various forms depending on the context (e.g. provisioning of evidence, notification for a data breach).

1.4 Aims of the Deliverable

This deliverable serves multiple goals linking, primarily, to the specific traits of the cloud environment and the difficulties in obtaining redress for data protection violations in general.

Despite the existing research addressing the issue of incident handling, research tailored to the specifics of the cloud setting is more limited. In other words, although there are guidelines available in the market addressing incident handling, this is not the case to the same extent for cloud, where a series of actors is involved in the supply chain. Furthermore, according to the findings of research conducted by the EU Agency for Fundamental Rights[17], individuals are reluctant to take action following an infringement of their right to data protection and hence the existing mechanisms may be inadequate in achieving fair remediation in cases of harms. The reasons underlying this reluctance mainly relate to high procedural and representation costs, a general lack of expertise, the average proceeding’s (excessive) length and the burden of proof.

In this context, this deliverable aims at providing guidance about how enhanced redress can be provided in the cloud setting. To this end, the deliverable describes prototype tools that aim to address these issues and, hence, provide a more satisfactory solution for cloud subjects whose data are processed in the cloud. Furthermore, the research captured in the present document addressed the needs of both cloud providers and cloud subjects affected by data protection violations. It has, therefore, produced an Incident Management Tool (IMT) appropriate for the cloud context and a Redress and Remediation Tool (RRT) addressed cloud subjects. These tools provide important functionality in terms of reporting and/or providing information and advice.

1.5 Outline of the Deliverable

The deliverable is composed of eight sections, including conclusions. A discussion on the proposed Network and Information Security (NIS) Directive[18], agreed at the moment of writing this deliverable, and on the remedies for business sensitive information across different jurisdictions (e.g. UK and United States) produced earlier under internal project reports is incorporated under the appendices; a list of tables and figures are, also incorporated, in the appendices.

Section 2 discusses incidents within cloud ecosystems. It sets the context for incidents occurring in the cloud (e.g. taxonomies, definitions), gives an overview of incident detection and addresses the impact of incidents for cloud end users. Section 3 provides a more detailed consideration of remedies following data protection violations and explains how individuals can obtain redress within common law (the UK) and civil law jurisdictions (the Netherlands serving as an example). Also, Section 3 discusses how individuals are currently expected to sustain their claims in front of administrative and judicial authorities. Section 4 presents sample use case scenarios for the Incident Management Tool (IMT). Sections 5 and 6 discuss respectively further in detail the Incident Management Tool (IMT) and the Redress and Remediation Tool (RRT) by explaining their functionalities and technical characteristics, including the notification format and the user interface. Following this discussion, Section 7 sets the bigger picture by explaining how IMT and RRT fit into the A4Cloud tool architecture. Finally, the last section of this Deliverable highlights the findings and concerns surfaced in the course of this research that will be further addressed within the ongoing project work regarding the socio-economic impact assessment of accountability mechanisms and the A4Cloud tools.

[16] An extensive discussion on the notion of the account is included Dziminski et al., "D:C-2.1*:* Report detailing conceptual framework”, page 3, available at:
http://www.a4cloud.eu/sites/default/files/D32.1%20Conceptual%20Framework.pdf
[17] European Union Agency for Fundamental Rights, “Access to data protection remedies in EU Member States”, FRA, 2013.
[18] n 3.

2 Incidents in a cloud ecosystem

This section discusses specific incidents occurring in the cloud. Following a brief introduction on incidents in general, the discussion points at existing taxonomies appropriate for the cloud, in order to explain later the choices made for the development of the IMT. Finally, the section stresses the particularities of harm resulting from an incident occurring within the cloud setting.

2.1 Introduction

There is no single way to define incidents. The OECD, for instance, defines incidents in general as:

"Events that can change the expected course of activities and impact objectives …"[19].

Under such an approach, incidents would obtain different forms; they can be physical, digital or even caused by a human intervention. For the current deliverable we only address incidents caused within the digital environment or caused by humans because these are most common and also potentially detectable.

Incidents caused by humans exhibit a huge variety of relevant differences in detectability, effects and remedies. These incidents may be caused intentionally (e.g. cyberattack) or unintentionally (e.g., overwriting a file by mistake). Other distinguishing factors relevant for incidents can be the level of sophistication, the duration or whether an incident can occur only within a specific IT setting.

Furthermore, not all incidents can be detected automatically. For instance, it may not be possible to detect that a systems administrator has made a copy of the data in their system and sold it to an outsider. In case an incident can be detected automatically, its detection and handling can in principle be built into the tools developed within the project. For incidents that cannot be detected automatically additional mechanisms need to be developed. For instance in the case of the rogue administrator, someone would have to trigger the event in order for the tool then to take appropriate follow up actions, such as reporting to affected individuals or the appropriate authorities. Of the incidents that can be reported, some, but not all, may need to be reported to entities outside the cloud supply chain (Cloud Customer, Cloud Subject, Cloud Supervisory Authority)[20].

2.2 Incident detection and management

There is a wide variety of incidents affecting cloud ecosystems related to personal and business data. In spite of this, there are few relevant academic works analysing and categorizing cloud incidents. Some studies surveyed potential cloud security issues, for instance[21,22,23]. Further works revealed new security vulnerabilities particular to cloud environments, such as[24,25,26]. The Cloud Security Alliance attempted some years ago to create a taxonomy based on incidents reported in the press[27]. The classification, however, is superficial and confuses actual incidents with vulnerabilities, as shown in Table 1*:* CSA incident categories and A4Cloud categories, examples taken from [D7]

[19] n 2.
[20] n 1.
[21] Meiko Jensen, Jörg Schwenk, Nils Gruschka, Luigi Lo Iacono: On Technical Security Issues in Cloud Computing. IEEE CLOUD 2009: 109-116
[22] Hassan Takabi, James B. D. Joshi, Gail-Joon Ahn: Security and Privacy Challenges in Cloud Computing Environments. IEEE Security & Privacy 8(6): 24-31 (2010)
[23] Siani Pearson, Azzedine Benameur: Privacy, Security and Trust Issues Arising from Cloud Computing. CloudCom 2010: 693-702
[24] Thomas Ristenpart, Eran Tromer, Hovav Shacham, Stefan Savage: Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. ACM Conference on Computer and Communications Security 2009: 199-212
[25] Christopher Dabrowski, Kevin L. Mills: VM Leakage and Orphan Control in Open-Source Clouds. IEEE CloudCom 2011: 554-559
[26] Yinqian Zhang, Ari Juels, Michael K. Reiter, Thomas Ristenpart: Cross-VM side channels and their use to extract private keys. ACM Conference on Computer and Communications Security 2012: 305-316
[27] https://cloudsecurityalliance.org/download/cloud-computing-vulnerability-incidents-a-statistical-overview/

. We suggest a much simpler and clearer classification composed of Service, Security or Privacy incidents. This categorisation is used in the Joint Risk and Trust Model of the work package C-6[28].

Table 1: CSA incident categories and A4Cloud categories, examples taken from [D7]

CSA Classification	Definition	Example	Incident type
Hardware Failure	Hardware, from switches to servers in data centers, may fail making cloud data inaccessible.	Swissdisk, a US cloud storage supplier, suffered a catastrophic hardware failure denying users access their data (http://www.theregister.co.uk/2009/10/19/swiss disk_failure/).	Service incident
Natural Disasters	Based on the geographical location and the climate, data centers may be exposed to natural disasters such as lightning, storms, and earthquakes, which can affect the cloud services.	One of Amazon's data centers was hit by lighting, taking out its cloud servers http://www.theregister.co.uk/2009/06/12/lightni ng_strikes_amazon_cloud/	Service incident
Closure of Cloud Service	Disputes with the cloud provider or non-profitability of the cloud service may result in the termination of the cloud service, leading to data loss unless end-users are legally protected.	Iron Mountain gave up its public cloud storage and closed down for good[http://www.theregister.co.uk/2011/04/11/i ron_mountain_exits_public_storage_cloud/]	Service incident
Cloud-related Malware	Attackers can use cloud-specific malware, such as bugs and Trojans, to either infiltrate or corrupt the network.	Hackers introduced a Trojan specially designed to disable cloud-based anti-virus security defenses [http://www.theregister.co.uk/2011/01/20/chine se_cloud_busting_trojan/]	Security Incident
Inadequate Infrastructure Design and Planning	Providers cannot cater to sudden spikes in demand, perhaps due to insufficient provisioning of computing resources and/or poor network design.	Nokia's Ovi store experienced extraordinarily high spikes of traffic resulting in some performance issues [http://www.theregister.co.uk/2009/05/27/ovi_d own/]	Service incident

[28]De Oliveira A.S et all, ''D:C-6.1: Risk and trust models for accountability in the cloud'', available at: http://www.a4cloud.eu/sites/default/files/D36.1%20Risk%20and%20trust%20models%20for%20accountability%20in%20the%20cloud.pdf

Governmental Agency access	Governmental Agency Mass Surveillance Program scrutinises personal data	See the NSA scandal http://www.theguardian.com/world/2013/nov/26/nsa-surveillance-europe-threatens-freeze-us-data-sharing	Privacy Incident
CSP fails to comply with data protection regulation	Privacy policies, practices, etc. are not up to the requirements of specific country's law about data protection	Google To Be Punished In France For Failing To Pare Back Its Overreaching Privacy Policy [http://techcrunch.com/2013/09/30/cnil-slaps-google/]Dutch privacy watchdog says Google in breach of data law [http://www.reuters.com/article/2013/11/28/dutch-google-privacy-idUSL5N0JD3K620131128]	Privacy Incident
Nefarious use of cloud computing	Attackers use cloud resources to perpetrate attacks	A hacker used Amazon's Elastic Computer Cloud, or EC2, service to attack Sony's online entertainment systems[http://www.bloomberg.com/news/2011-05-15/sony-attack-shows-amazon-s-cloud-service-lures-hackers-at-pennies-an-hour.html]	Security Incident
Cloud service vulnerability	A flaw or weakness in a service's design, implementation, or operation and management that could be exploited to violate its security policy.	Identity-theft vulnerability fixed in Microsoft Office 365, says security firm [http://news.idg.no/cw/art.cfm?id=B86C4FDD-B9F4-5751-101B1C570CA6ECAD]	Not an incident, unless the vulnerability was actually exploited

Using this categorisation, a service outage originated by a Distributed Denial of Service (DDOS) attack is a security incident, revealing a vulnerability in the cloud service. However, a service outage due to resource exhaustion because of weak capacity planning is a service incident. Note that frequently a security incident leads to a violation of the data protection rules, but not vice versa. For instance, a CSP may collect personal data without the consent of the data subject. This scenario forms an "*incident*" from the data protection point of view, but not necessarily from a security point of view. We have used the taxonomy presented here as a starting point for developing IMT and A-PPL. The taxonomy is, however, not binding. CSPs need not adopt our taxonomy and IMT and A-PPL are flexible in the sense that they can operate on any trigger (and associated response) defined by the entity adopting the tools.[29]

2.3 The impact of cloud incidents

The impact of an incident occurring in the cloud varies depending, among other things, on who has been affected by the incident. For example, if an SME were using cloud services for the processing of personal information, an incident might lead to financial losses by the SME itself, its customers and individuals whose data it processes. Where the fundamental human rights of individuals have been infringed, those individuals might have contractual claims against the SME, though not against the responsible CSP. In addition, human rights are protected by laws which might give individuals direct claims against one or more of those who share responsibility for the incident, for example under EU data protection law if personal data are wrongfully accessed for marketing purposes or where personal data collected within EU are transferred to a country outside the EU that does not afford an "adequate" level of protection.

[29]Introducing new triggers and responses requires the multiple stakeholders to agree on the semantics of the triggers and responses and also carefully communicate this to the end-users.

According to the findings of a study conducted by the European Parliament[30], EU citizens benefit from substantial legal protection against what the study describes as "cloud harm", more specifically privacy infringements and the imposition of unfair terms in cloud contracts. But, as the study notes, consumers may not easily be able to benefit from these legal protections because many mass cloud providers are located outside the EU, with the result that 'in practice European consumers are highly unlikely to be able to seek or obtain redress'. This parallels the findings of the earlier mentioned report produced by FRA regarding data protection violations in general.[31]

The study for the European Parliament suggests that this problem of consumer access to effective redress needs to be dealt with:

> "Providing adequate means for complaints and redress is necessary for the future in the consumer services area; both alternative means – such as online disputes procedures – and collective means of redress, since there is a strong imbalance of powers between consumers and providers of cloud services.''

This suggestion clearly envisages that redress will be by means of legal claims, which in practice would mainly be claims for financial compensation. Such an approach is unlikely to be effective for two reasons: first, it cannot reduce the cost of cross-border litigation, which is the major barrier to consumer claims under existing laws; and secondly it fails to recognise the adverse effects which imposing liability would have upon the development of cloud computing services for consumers. This second issue arises because a single failure within a CSP's systems has the potential to result in loss to a very large number of consumers. Furthermore, the nature of cloud computing implies that a cloud provider has no practical way of knowing what kinds of data its customers are processing, and thus of predicting the likely scale of losses which it might have to compensate. Finally, one of the main advantages of cloud computing is its low cost compared with other forms of data processing, and that low cost means that the margin from which compensation claims can be paid is also very small. This is the reason why CSPs consistently disclaim liabilities for damages. If there were a more effective way of making CSPs liable to consumers, either the price of cloud services would rise substantially or CSPs would find it uneconomic to provide those services to European consumers[32]. This is not to argue that a more effective imposition of liability would be wrong in principle, but rather to point out that it is not costless in terms of benefits to consumers, so that any decision on this point needs to take those costs into account. It is perhaps worth noting that a similar cost-benefit analysis led to the introduction of the intermediary immunities in articles 12-15 of the E-Commerce Directive.[33]

[30] European Parliament, Cloud computing Study, section 5.2.3, available at http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO_ET(2012)475104_EN.pdf

[31] n.17.

[32] Note that the term ''consumer'' refers to individuals.

[33] Directive 2000/31/EC on electronic commerce OJ L 178/1, 17 July 2000. This issue is discussed at further length in D-4.5, Legal and Regulatory update – embedding accountability in the international legal framework (in preparation).

3 Remedies for data protection violations in the cloud

This section captures the legal research conducted for the development of IMT and RRT. The discussion below is especially relevant for RRT, given that it explains what an individual can actually do to obtain redress for a data protection violation on the basis of data protection rules and contract law. Legal systems differ in the options they provide for redress. A major distinction is between common law versus civil law traditions. The analysis below focuses on a common law country (UK), while references to civil law countries (Netherlands, Italy) will be made where necessary or appropriate. Finally, the section explains the role of proof for individuals in supporting claims for remedies in front of administrative authorities and courts, which provides the foundation for the "account" that RRT should provide to the end user (see section six). Note that for clarity purposes, the section below maintains the terms and roles prescribed in relevant laws and regulation.

3.1 Setting the scene of relevant terms in common law and civil law countries

It is useful here to include a brief explanation of some of the terminology, which the cloud computing industry has adopted from law but uses with different meanings. We have tried to avoid using these terms in the discussion below, and this explanation of their potential for confusion should explain why.

First, "direct and indirect losses". The industry regularly uses these terms in discussion with lawyers as if they had a fixed legal meaning. In fact, the law makes little use of them. As will be seen below, the UK Data Protection Act makes a distinction between compensation for damage and for distress, while UK negligence law treats material losses differently from purely financial losses, and may not offer any compensation at all for distress, which falls short of psychological injury. In UK contract law, direct damage means all losses, which ought to have been foreseen as likely consequences of a particular breach, assessed at the time the contract was made.[34]

On the contrary, in Dutch civil law, the term "direct loss" is also not commonly used and has no specific meaning. When talking about causality, the relation between the act causing the loss and the actual damage may be said to be more direct or more distant. However, also this is not common parlance. The criterion used in Dutch civil law for causality is that the loss can be attributed to the actor in view of the nature of the liability and of the damage (art. 6:98 Dutch Civil Code). Under this umbrella criterion, other more specific criteria may be used to assess causality. As subrules, the following can be mentioned:[35]

1. If the consequence is more probable according to rules of experience, attribution is easier justified,
2. If the result is less far removed from the act, attribution is easier justified,
3. Traffic or safety standards that have been set in order to prevent accidents justify a broader attribution of losses though injury or death,
4. If the negligence underlying the causatory act is larger, a broader attribution is justified,
5. Loss through death or injury is more easily attributed than damage to an object, damage to an object easier than damage consisting of extra costs or expenditures, and the latter damage is easier attributed than loss through foregone profits.
6. Damage caused by a company is more easily attributed than damage caused by a private person or a person in a professional capacity (such as a GP, architect, lawyer etc.). Although this is not common parlance, one might say that "direct loss" is a proxy for 'more easily attributable" or – in terms of the subrules - for "easier foreseeable"
    a. "a shorter causal chain"
    b. "a clear violation of safety norms"
    c. "based on more apparent negligence"
    d. "a loss consisting of death, injury or damage to an object"
    e. or "loss caused in the course of the exercise of a business"

[34] British Sugar Plc v NEI Power Projects Ltd (1998) 87 BLR 42. In GB Gas Holdings Limited v Accenture (UK) Limited and others [2010] EWCA (Civ) 912 the court held that direct loss included compensation payments made by the claimant to its customers, among other purely financial losses.

[35] Hartkamp, A.S. (1988). Mr. C. Asser's Handleiding tot de Beoefening van het Nederlands Burgerlijk Recht, Verbintenissenrecht, Deel 1, De Verbintenis in het Algemeen, Tjeenk Willink, Zwolle, p. 373-374. See also C.J.H. Brunner, Causaliteit en toerekening van schade (I), VR 1981, p. 210-217.

f. If "direct loss" is to be used in any of these meanings, this should be explicitly defined so.

Although the term direct and indirect losses does not appear under the Dutch Civil Code, these terms do appear often in Dutch ICT-contracts.[36] It seems to be assumed that the meaning of these concepts is clear. However, Dutch scholars disagree in this respect. On the one hand direct damage is explained as damage to the property as such, while indirect damages refers to monetary damage. On the other hand, direct damage is considered to be close to the product or service delivered, while indirect damage is more detached damage, like lost profit. Another frequently used term is "gevolg schade" (consequential damage), mainly used as the opposite of direct damage – and thus more like a synonym for indirect damage – but some exoneration clauses explicitly refer to both indirect damages and consequential damages, assuming a difference between the two.

Readers from industry should therefore not think that their own understanding of these concepts necessarily has any meaning in law, or that their contracts, which place different limitations on liability for indirect losses, have any meaning at all, let alone the meaning they are intended to have. It is commonplace in legal practice for a lawyer to investigate the words used by the parties in negotiating drafts, and to discover that each party has a clear idea what they mean by the words but that the two intended meanings are completely different. The ultimate decision-maker on what the words mean is a court, based on previous judicial interpretations of those words and the court's view about what an objective third party (the "officious bystander" in English contract terminology) would think they meant. The UK British Sugar case[37] is a notorious example, where the judges gave a meaning to the words "direct loss" that was almost certainly different to what either contracting party intended based on earlier judicial decisions. Additionally, as explained below, exclusion and limitation clauses are likely to be completely ineffective against contracting parties who are consumers.

Second, there seems to be an understanding in the cloud industry that exercising "*due diligence*"[38] is sufficient to avoid liability. This is untrue. The industry sees due diligence as taking reasonable care, and/or following good practice, in the design and implementation of a computer system. The closest legal equivalent is the legal concept of negligence, expressed by the common law in terms of reasonable care and skill and by civil law in terms of the expected care or diligence of a person. The legal concept goes beyond merely the design and implementation of a system, and includes its operation and how system failures are dealt with. Whether "due diligence" is sufficient to discharge a legal duty of care will depend on how far adherence to that concept leads to the cloud actor behaving in the way required by the law. In most cases the law's obligations of this kind are expressed in terms of reasonableness, such as "reasonable care and skill"[39], or some equivalent language such as "appropriate technical and organizational measures".[40] In Dutch law, these obligations are called 'zorgplichten'. As the English translation (duties of diligence and care) indicates, this is not just a duty to omit behavior that is damaging, but also the positive duty to shield others from harm where the primary cause lies elsewhere. The extent of the duty is not (necessarily) fixed in a formal legal instrument, but is based on a moral, socially recognised duty to care for others. Pre-existing knowledge and experience in social practices is a pre-requisite to legal enforceability.[41]

[36] T.F.E. Tjong Tjin Tai, Directe schade in het contractenrecht, *MvV* 2007/11, p. 226-231.
[37] n 34
[38] The most common meaning of "due diligence" in legal language is as a description for the process of investigating the financial and other characteristics of another contracting party, and of the subject matter of the contract, before entering into that contract. Thus in an outsourcing, for example the due diligence process would require (amongst many other matters) the customer to check the financial status of the outsourcing provider, whilst the provider would want to review all the customer's software licenses.
[39] The duty of care and skill implied into contracts by UK Supply of Goods and Services Act 1982, s 13 – see section **Error! Reference source not found.** for further discussion.
[40] Art 17 of the Data Protection Directive (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, available at http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf) in relation to data security.
[41] Tjong Tjin Tai, T.F.E., Op Heij, D.J.B., e Silva, K.K., Skorvanek, I. and Koops, B.J. (2015). Duties of care and diligence against cybercrime, Tilburg University, p. 17-18. Available at: https://www.gccs2015.com/sites/default/files/documents/Bijlage%202%20-%20Duties%20of%20care%20and%20diligence%20against%20cybercrime%20(1).pdf

Acting less carefully than other industry members do is almost certain to be negligent or inadequate. But it is also important to note that copying others may not be sufficient. It is quite possible for a court to find that an entire industry sector falls short, because the test is not how others *do* behave but how a reasonable person *ought* to behave. This is what happened in the US case of the *TJ Hooper*[42], where the plaintiff's barges were lost in a storm at sea whilst being towed by the defendant's tugs. If the tugs had been fitted with radios, they could have received warning of the storm and taken shelter, thus avoiding the loss of the barges. In spite of the fact that it was not common industry practice to fit radios to tugs, the court held that the defendant ship owner was negligent – the technology was easily available, comparatively cheap, and its utility to prevent the loss was clear. The defendant might have been exercising "due diligence" by industry standards, but those standards were not good enough to satisfy the law's demands.

In addition, many legal and regulatory obligations are absolute, rather than dependent on negligence. Thus lack of negligence is no defence to most breaches of data protection law, nor to breach of a contractual obligation, which is not expressed in terms of care and skill.

Finally, we should mention that foreseeability is an important concept throughout this legal discussion. It is part of the test for whether a defendant has been negligent, because it is not possible to guard against unforeseeable losses, and the standard expected must bear some relevance to the likelihood even of foreseeable losses. As an example, many cloud providers have data centres in Ireland. Earthquakes big enough to destroy those facilities are foreseeable, but so unlikely that it would be out of proportion to the risk to invest in the kind of earthquake protection that would be common in, say, parts of California. Foreseeability is also relevant when courts are awarding compensation. Foreseeability is an aspect of risk assessment, a concept with which the industry is familiar. But for legal purposes it requires consideration of ways in which a system or its operation might fail, and more importantly the potential consequences of that failure for outsiders affected by the system. The industry is used to considering the consequences for the system itself, but less focused on outsiders (for example, the industry would consider the consequences for its customers, but might overlook those data subjects whose personal information is processed by those customers). Attention needs to be focused both on the risk of a failure occurring *and* the potential consequences for those affected if it does occur, and the courts undertake a risk balancing exercise in that light. For example, in the UK case of *Paris v Stepney Borough Council*[43]the House of Lords held that the council were not negligent in failing to provide eye protection for a particular group of employees generally, because the risk of eye injury was very low. However, the plaintiff employee had only one eye, and so the court held that a reasonable employer *would* have provided eye protection to him because of the particularly serious consequences if the unlikely risk of injury happened. This case highlights the relevance of special knowledge on the part of cloud providers, which therefore needs to be taken into account in risk assessments in individual cases.

3.2 Regulatory framework for redress and remediation

The current regulatory framework is set out in the Data Protection Directive (DPD)[44], which establishes the basic principles for redress and remediation but leaves their implementation to the Member States. As a consequence the precise remedies available for breaches differ between Member States, as do the enforcement policies of national supervisory authorities.

The DPD's redress and remediation principles are set out in Arts 22-24. They require Member States to provide a judicial remedy for the breach of any rights granted to a person under the national law implementation, including a right to compensation from the controller for damage suffered as a consequence of such a breach[45], and to lay out a sanctions regime for breach of the regulation.

To illustrate the differing approaches of Member States we briefly explain the UK and Dutch national law implementations here.

[42](1932) 60 F 2d 737.
[43][1951] AC 367.
[44]European Commission (EC) (1995) 'Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data', available at: http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf
[45] Subject to the defence that the controller was not responsible for the event giving rise to the damage – Art 23(2).

In discussing the UK implementation, effected via the Data Protection Act 1998, it is worth beginning by noting that the ICO cannot order compensation to be paid to those who suffer loss because of a regulatory breach – this requires a court claim as further explained below. A data subject is, however, entitled to make a complaint to the ICO, which may then lead to administrative action as explained below.

Under the UK Act the primary remediation mechanism is an enforcement notice issued to a data controller by the UK Information Commissioner's Office (the ICO). That notice is issued under section 40 of the Act; it specifies the regulatory contravention and requires the controller to do (or stop doing) specified matters in order to remedy the contravention. The ICO has wide discretion as to what it can require the controller to do, including ceasing or modifying its processing, notifying affected persons, and so on.

In investigating contraventions, usually as result of a complaint from the data subject although the ICO has power to investigate on its own initiative, the ICO can issue an information notice under sections 43 and 44, which requires a controller to provide specified information relating to compliance.

In addition, section 55 of the Act creates a criminal offence of knowingly or recklessly obtaining data from a controller without the controller's consent, or disclosing or procuring the disclosure of such data. This offence is prosecuted by the ICO.

Failure to comply with either of the enforcement or information notices is itself a criminal offence under section 47, and the ICO can initiate a prosecution of the data controller before the courts.

In the initial implementation of the DPD via the Act the ICO was given no powers to impose monetary penalties directly, but these powers were introduced by the Criminal Justice and Immigration Act 2008 as new sections 55A to 55E. These sections give the ICO power to impose directly a monetary penalty for any "serious" contravention by a controller of the data protection principles which is "of a kind likely to cause substantial damage or substantial distress", provided that the controller knew or ought to have known of the risk of contravention and its likely consequences.[46]

However, the guidance issued by the ICO makes it clear that:

> "A monetary penalty notice will only be appropriate in the most serious situations. Therefore in such cases the monetary penalty must be sufficiently meaningful to act both as a sanction and also as a deterrent to prevent non-compliance of similar seriousness in the future by the contravening person and by others."[47]

Enforcement notices therefore remain the primary means of achieving remediation in the UK. This is confirmed by analyzing the enforcement actions published by the ICO from January to August 2015[48]. Only three monetary penalties were issued under section 55A and five prosecutions completed[49]. By contrast, seven enforcement notices were issued, and no less than 19 undertakings given by controllers to make their processing compliant. In addition there were 15 follow-up actions to check compliance with an undertaking or enforcement notice. It is clear that in the UK the ICO's focus is primarily on forcing controllers to comply with their data protection obligations, and that imposing monetary penalties or prosecuting breaches is seen very much as a last resort.

In discussing briefly the Dutch implementation, Chapter 10 of the Dutch Data Protection Act (DDPA) [50]is entirely devoted to sanctions including administrative penalties (Art.65 - 66) and criminal sanctions (Art. 75). Article 65 states that the Dutch Data Protection Authority is competent to impose incremental

[46] Section 55A (1)-(3).

[47]Information Commissioner's guidance about the issue of monetary penalties prepared and issued under section 55C (1) of the Data Protection Act 1998 (ICO 2015) p 6, https://ico.org.uk/media/for-organisations/documents/1043720/ico-guidance-on-monetary-penalties.pdf.

[48]https://ico.org.uk/action-weve-taken/enforcement/. The analysis excludes prosecutions for nuisance marketing calls, which are made under the Privacy and Electronic Communications (EC Directive) Regulations 2003 rather than the Data Protection Act.

[49] Two under section 47 for failure to comply with a notice, two under section 55 for unlawful disclosure, and one for failure to register as a controller.

[50] In Dutch Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens, Wbp). All Dutch legislation can be retrieved from www.wetten.nl

penalties for infringements of the DDPA and, according to Art. 66, has the authority to impose punitive fines of up to 4500 euro. As off the first of January 2016, a bill becomes effective that heightens this amount of damages to 810.00 euro.[51]Article 75 concerns criminal fines that can be imposed only when certain provisions of the DDPA are violated, among which the obligation that controllers must appoint a point of contact in the Netherlands when the controller has no Dutch establishment (art. 4 DDPA), and the obligation to notify certain data processing activities to the Dutch Data Protection Authority (articles 27 and 28 of the DDPA).

The General Data Protection Regulation (GDPR) will, once it is adopted and implemented, produce a far more uniform scheme of redress and remediation across the EU. The GDPR was proposed by the Commission in 2012[52]. Since then, LIBE Committee of the European Parliament has produced a competing version and so has the Council.[53]In a number of trialogues between the three entities in the European legislative process a draft compromise has been produced that has been adopted by the LIBE Committee on 17 December 2015.[54] The EU Parliament will vote on the compromise in January 2016. The analysis in section is based on the three versions (Commission, EP, Council) that were available in Autumn 2015 and that could only provide an overview of the likely final shape of the regulatory scheme (and therefore glossing over the differences of detail in most cases).

There are three main elements to the GDPR's redress and remediation scheme: the powers of supervisory authorities to investigate and issue orders; the granting of remedies and issuance of sanctions for breaches; and a wide range of new obligations to notify breaches of the regulation.

Article 53 of the GDPR gives supervisory authorities the powers to (a) order data controllers or data processors to remedy breaches of the regulation, and (b) to undertake investigations into how processing is undertaken. These powers are specified in far greater detail than under most current national implementing legislation, but the ultimate effect is likely to be broadly similar once the text is finally agreed. The two big changes are:

a. These powers extend to the activities of data processors as well as data controllers; and
b. The obligations imposed on data controllers and processors are more extensive, as partially explained below, so that the range of matters which can be investigated or about which orders can be issued is extended.

The new remedies and sanctions regime will apply to both controllers and processors. Data subjects have the right to complain to the supervisory authority that the processing of their personal data is not in accordance with the regulation (art 73) and the right to a judicial remedy against a controller or processor if the subject's rights under the regulation have been infringed (art 75). The data subject may choose to take either or both of these routes to redress. Under Article 77, compensation can be claimed by a data subject for damage suffered as a result of processing which is unlawful under the regulation, subject to the same defence as under the DPD that the defendant is not responsible for the act, which gave rise to the damage. It is not clear from the text whether compensation claims can be decided by the supervisory authority or must be taken to court, though the Council text limits them to decision by the courts.

Sanctions for breach of regulation may be imposed by supervisory authorities under Article 79, though there is substantial disagreement between the Parliament and Council texts on the extent of a supervisory authority's powers. There is agreement that supervisory authorities should have power to impose

[51] The Dutch Data Protection Authority has published guidelines on its website to provide more transparency on how the height of administrative fines will be established: https://www.cbpweb.nl/nl/nieuws/cbp-publiceert-conceptboetebeleidsregels

[52] Proposal for a 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), COM(2012) 11 final, 25 January 2012, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

[53]The organisation European Digital Rights has produced a useful side-by-side comparison of these texts https://edri.org/files/EP_Council_Comparison.pdf.

[54] The informal text the LIBE Committee voted on can be found here: http://www.statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf At the time of finalizing this deliverable the official text was not available yet.

administrative fines; the disagreement is about whether there is discretion to impose no penalty at all, and about what additional sanctions the authorities should be able to impose.

Finally, the GDPR imposes a number of new notification obligations on data controllers and processors.

The new notification obligations fall into two categories. The first is the right of data subjects under Articles 13-19 to receive information about the processing of their personal data, obtain access to it, demand its rectification or erasure in certain circumstances, request that it not be processed for certain purposes, and to gain access to that data in a portable form so that it can be transferred to a different service provider. Article 12 requires data controllers to provide information in response to such requests, and the Parliament text provides that the information should normally be supplied in electronic form.

The second category is notification about personal data breaches, which are defined in Article 4 as:

> the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

Article 31 requires such breaches to be reported by data controllers to the supervisory authority, although there is a difference between Parliament and Council about whether all breaches, or only serious ones, should be reported. The Article sets out the required content of such a report in some detail, including information about how the controller proposes to act in relation to the breach. Data processors are required to report breaches to their controller, who would then of course be subject to the obligation to report to the supervisory authority.

Under Article 32 there is also a requirement to report personal data breaches to the data subject provided they are of sufficient seriousness, though Parliament and Council are in disagreement about how the required level of seriousness should be defined. Again, a minimum level of information to be provided in the report is prescribed.

Outside the EU the regulatory framework for redress and remediation is incoherent and confusing.[55] Some states, such as Canada and Australia have enacted comprehensive data privacy laws while others have only legislated for specific data privacy issues. The US is particularly confusing, with a mixture of Federal laws regulating data privacy for data processing by Federal institutions, State laws, which are often sectoral regulation, and the majority of redress and remediation left to private law tort or contract actions. The one area where some consistency is developing is breach notification, with the majority of large states enacting some kind of breach notification law,[56] though as before the US position is complex and differs from state to state.[57] Even here, the 'trigger conditions' for determining whether a data breach requires to be notified vary widely, as do the persons to whom notification must be made.

In practical terms, only the very largest cloud providers might even consider attempting to identify all the applicable laws and setting up a scheme for redress and remediation which aims to address all the potentially applicable legal and regulatory requirements. Most providers will need to adopt a more pragmatic approach, by discovering the laws and regulations which are most likely to give rise to redress and remediation obligations (typically those of their country of establishment and the countries from which their biggest customers operate) and implementing systems which satisfy those obligations. In doing so, two important issues need to be considered:

- Data breaches might occur at any point in the cloud ecosystem, and remediation may require action on the part of others than the cloud provider to be effective. Thus contracts with sub-providers need to ensure that data breaches, which occur via the sub-provider's systems are reported to the provider. Sub-providers may themselves use sub-sub-providers, so ideally these reporting obligations should extend fully across the cloud chain. The same applies to obligations

[55]For a comprehensive overview see Christopher Kuner, Transborder Data Flows and Data Privacy Law (Oxford: OUP 2013).

[56] A useful comparative table is in Alana Maurushat, Data Breach Notification law across the World from California to Australia (2009, 11 University of New South Wales Faculty of Law Research Series, http://law.bepress.com/cgi/viewcontent.cgi?article=1153&context=unswwps-flrps09).

[57] See Jill Joerling, Data Breach Notification Laws: An Argument for a Comprehensive Federal Law to Protect Consumer Data, 32 Wash. U. J. L. & Pol'y 467 (2010).

to take remedial action, which should also extend fully across the chain. However, achieving such matching contractual obligations is very difficult in practice, because each cloud provider focuses on its own national and regulatory regime and will be reluctant to agree to obligations and liabilities, which go beyond those it is forced to accept at home.

- Technical mechanisms, such as those being developed for the A4Cloud toolset, are likely to be more effective than contracts in offering appropriate redress and remediation. If they can identify and provide evidence about data breaches, and offer effective means for remediation without excessive manual intervention by providers and sub-providers, they are likely to be seen by those organisations as useful additional features for which a commercial argument can be made, rather than as 'legal compliance' matters which are inherently difficult to understand and risky.

3.3 Cloud providers, regulators and the A4Cloud toolset

A main purpose of the A4Cloud toolset, from a legal perspective, is to *assist* cloud providers to comply with data protection regulation. It is worth restating here that compliance is not hard-wired into the tools because the open-textured and contextual nature of law and regulation makes it impossible to do so in a useful way. It is also worth noting that although the research has focused on EU data protection law, the toolset will be equally useful in improving compliance with other applicable laws. It will therefore go some way to improving the current situation where, in a complex case where the relevant cloud ecosystem spans multiple jurisdiction, each entity acts independently by focusing on its national legal and regulatory obligations and thus a failure across the whole ecosystem is inevitable.

The primary connection between the toolset and data protection regulatory obligations is via *policies*. These are machine-readable statements of how data should and must be processed. Some policies, or elements of policies, will be designed to achieve technical ends; some will be designed to achieve regulatory compliance; and some will aim at both. Producing a set of policies, which, if adhered to, will achieve regulatory compliance is primarily a human decision-making function. It requires input from those who understand the nature of the processing, the personal data content and the risks to data subjects if data is processed improperly, and from those who understand the regulatory obligations. The AccLab tool provides assistance in the partial automation of policy generation, and in consistency checking, but the final responsibility for the correctness of the policy set rests on human decision-makers. COAT and DPIAT assist those decision-makers in selecting suitable cloud providers and identifying the risks created by the processing. The APPL-Engine forces policy compliance and identifies policy compliance failures, and the remainder of the A4Cloud toolkit deals with the consequences of policy compliance failures.

Where failure to comply with a policy amounts to a regulatory breach, then (as explained above), cloud providers have obligations under the GDPR[58] to take action to report some breaches, to remedy breaches, and to provide data subjects with information which can assist them in obtaining redress or remediation.

IMT's main functions are:

- To report policy compliance events (incidents) to cloud providers. This makes cloud providers aware of incidents which might amount to regulatory breaches, or which are breaches, and thus enables them to take appropriate action. Monitoring data processing in this way is a fundamental requirement for regulatory compliance. Where supervisory authorities have and exercise enforcement discretion, as in the case of the UK Information Commissioner's Office (ICO), effective monitoring coupled with prompt remediatory action is likely to persuade the authority that enforcement action is not needed, unless the authority considers that the failure leading to the incident should have been anticipated and guarded against.

  This reporting function will also assist cloud providers who are in the process of one-off or continuous audit by their supervisory authority. Research by A4Cloud[59] has identified that supervisory authorities are increasingly demanding reports on incidents, which arise during

[58] The remainder of this section is written as if the GDPR were enacted and in force, because the tools have been designed on that basis in order to future proof them as far as possible.
[59] Asma Vranaki and Chris Reed, D:D-4.1 Rise of compliance audits,, available at: http://www.a4cloud.eu/sites/default/files/D44.1%20Rise%20of%20Compliance%20Audits.pdf

processing activities, often in real time, and IMT/RRT together provide a mechanism which could be used to satisfy some of those demands.

- To enable cloud providers to meet their reporting obligations to data subjects and supervisory authorities under articles 12, 31 and 32. It is important to recognise that not all incidents are regulatory compliance failures. For example, a request by a data subject under Article 12 that data be deleted, but which has not been complied with, should generate an incident that the data *has not* been deleted within the required timeframe. That incident needs to be reported to the data subject, in this case to demonstrate that the regulation has been complied with.

  Decisions about which incidents of personal data breach should be reported require human input for two main reasons. First, under Articles 31 and 32 only serious incidents have to be reported, and the factors, which need to be taken into account (such as the potential consequences to data subjects) can only be assessed by a human. Secondly, the information supplied to the service provider by IMT may contain data about more than one data subject, so merely passing on the raw IMT report might itself constitute a regulatory breach. For this reason a human decision-making "air gap" is built into IMT, allowing the service provider to review the report and decide what action to take. Of course this does introduce a vulnerability because the decision maker may determine to withhold information to data subjects or regulators that they should disclose. This issue is, however, difficult to solve and we have not been able to develop an algorithm that helps decide which information should pass and which should not on the basis of obligations resulting from applicable legal rules and policies relevant for a specific context. However, accountability can help prevent unwarranted blocking. By keeping an audit trail of all incidents detected, as explained later in section six, people can be called to account later on, which may affect their behaviour. Note that ordinary breaches of SLAs could be reported automatically, but these are not privacy-related.

RRT assists cloud providers to meet their obligations, under Articles 12 and 32, to explain to data subjects the redress and remediation options that are available if the service provider is in breach of the regulation. It does this by converting IMT reports into a more user-friendly form so that the data subject will understand what has happened, and provides assistance to the data subject in choosing amongst the redress and remediation options available. Some options are enforced directly by the A4Cloud toolset. For example, a data subject might decide to change the disclosure permissions for his or her personal data, and this would be translated into a policy change which would then be enforced by the APPL-Engine and reported back indirectly via IMT. Other options might include reporting the incident to the supervisory authority or initiating court action, but the tool needs to make complex compromises here:

- It is important that the tool does not offer legal, or even non-legal advice. Giving legal advice is normally restricted to qualified lawyers, and other kinds of advice can give rise to liability if the advice is not accurate.
- Data subjects will have differing levels of understanding about the technology and the risks created by the incident, and it is not easy (if even possible) for the tool to identify and deal with these differences.
- The functionalities of the RRT will be made available by cloud providers, provided they will show willingness to collaborate, given that it is anticipated that they will naturally be reluctant to assist complainants in bringing actions against them before supervisory authorities and the courts.
- Supervisory authorities might be overwhelmed by multiple complaints arising from a single incident – for example, if a dataset is deleted one day later than specified in the policy and every data subject in that dataset uses RRT to complain.

For these reasons, this element of RRT aims more at educating data subjects about the available options and assisting them to find further information and advice than at making reports to regulators on their behalf.

3.4 Data subject redress and remediation under the regulatory framework

Under the current European data protection framework, it is the national law implementations of the DPD, which determine what a data subject can do to achieve redress or remediation. If the responsible (in a

technical, rather than legal sense) cloud provider refuses to provide redress or remediation voluntarily,[60] the options are to make a complaint to the supervisory authority or to commence an action in court.

Under the UK implementation, the ICO will receive complaints about all aspects of personal data processing and make an assessment about what action it should take. The UK Data Protection Act, section 42, does not mandate the ICO to take any particular action; it has full discretion to decide the most appropriate course of action. Guidance about how the ICO will deal with complaints from data subjects[61] suggests that complaints about incidents more than 3 months old are likely not to be investigated further. That guidance also reiterates that the ICOs main aim is to ensure compliance for the future rather than to sanction breaches.

If the ICO decides to investigate the complaint it can use its power to issue information notices to further that investigation, if the data controller does not voluntarily provide the requested information. If the result of the investigation is that the ICO considers the regulation to have been breached, it has the enforcement powers explained above, although the most likely sanction is an enforcement notice.

A data subject can also bring court proceedings under section 13, which implements Article 23 of the DPD. The claim may be for compensation as a result of "any contravention by a data controller of any of the requirements of this Act". Although this gives a wide scope for compensation claims, section 13 expressly restricts claims for compensation for pure distress – such compensation can only be claimed if other damage can be proved as well. The European Commission has argued that this restriction results in a failure to implement the provisions of Article 23, and in *Google Inc. v Vidal-Hall & Ors*[62]the Court of Appeal agreed, holding that "damage" for the purposes of Article 23 included "moral damage" (which concept includes distress), so that claims for pure distress were not barred by section 13. However, the case is currently under appeal, so the point is not yet settled.

In court proceedings it is for the claimant, i.e. the data subject here, to prove his or her case. The ICO, if it decides to investigate the complaint, may provide a letter to claimant giving the ICO's view about whether a breach of regulation has occurred. This is merely persuasive though – it is for the court to decide this point. The claimant also has to prove the loss suffered. Most of this evidence will be in the hands of the data controller; and although the court has power to order the production of documents and records, making a useful request for an order is legally complex and likely to require professional advice. The information provided to data subjects by IMT and RRT will be admissible as evidence, and thus overcomes this problem at least in part. If the claimant can prove that personal data was processed in contravention of the Act, the burden of proof is on the controller to assert any defence under section 13(3) that the controller took "such care as in all the circumstances was reasonably required" to comply.

In the Netherlands, it is highly unlikely that the national Data Protection Authority will intervene in individual cases. The DPA's policy is to only take action if enough signals are received that certain data processing activities warrant an investigation by the DPA. This leaves data subjects with the possibility to start legal proceedings. In case of infringements by government procedures established in the General Administrative Law Act (GALA)[6364] are to be followed, while in case of infringements by private parties the procedures as laid down in the Dutch Act of Civil Proceedings apply. As a general rule, Dutch civil law establishes that the party that claims damages must prove the damages. In cases of a severe power imbalance, deviation from this general rule is possible. There are no restrictions as to the kind of evidence that is admissible in civil court, and the judge has a passive role: only judging the case on the basis of the claims and evidence that has been submitted to court by the parties.[65] Evidence in Dutch administrative law is characterised by a lot of judicial freedom. The judge can decide how evidence should be delivered

[60] Even if IMT reports that the incident occurred, a provider might (a) dispute that the relevant national law applied or that the court had jurisdiction, (b) dispute that the incident gave rise to liability under that law, or attempt to rely on a contractual exclusion or limitation, or (c) dispute the amount claimed.
[61] https://ico.org.uk/concerns/.
[62][2015] EWCA Civ 311 (27 March 2015).
[63]Algemene wet bestuursrecht in Dutch.
[64] Articles 45 and 46 of the Dutch Data Protection Act specifically state these legal procedures to be available in case of controllers' non-compliance with data subjects' right of access, rectification and erasure.
[65] Rules on evidence in civil proceedings are laid down in Articles 149-207 of the Dutch Code of Civil Proceedings, in Dutch Wetboek van Burgerlijke Rechtsvordering.

and is free in his decision how to value evidence and regarding the division of the burden of proof.[66] The most important difference with civil procedural law concerns the role of the judge. In administrative proceedings the judge is required to actively engage in establishing what actually happened, and thus can go beyond the evidence that has been submitted by the claimant and defendant (art. 8:69 GALA).

Under the GDPR, the same two routes to redress and remediation are available. As explained above, a complaint may be made to a supervisory authority, although it is not yet clear whether the final text will permit the supervisory authority to award compensation, or to the courts. Article 77 explains how compensation claims are to be decided; its wording suggests that it is enough for the complainant to prove that damage was suffered as the result of an unlawful processing operation, and then the only defence available to the controller or processor is to prove that it was not responsible for the event giving rise to the damage. Quite what "not responsible" means is unclear – a court could interpret it as meaning moral responsibility, in the sense that the defendant had taken all reasonable steps to prevent the unlawful operation, or as factual responsibility, i.e. that some other person was responsible. The GDPR will probably leave this question to be decided by the courts.

3.5 Data subject redress and remediation via contractual liability

In addition to a claim for compensation or other redress under the data protection regulatory regime, data subjects might find it possible to make a claim for breach of contract against one of more of those who are responsible for improper processing of personal data. For such a claim to succeed three elements must be present:

- A contract between the claimant data subject and the defendant. The most obvious example, and the one on which this analysis will focus, is the contract between the data subject and his or her cloud service provider. Examples might include Google (for Gmail and Docs), Facebook (social media), Dropbox (file storage and sharing) or Photobucket (image storing and sharing). In all cases, users of those cloud services must sign up to a contract in the form of Terms of Service (or equivalent language).
- The contract must contain a term, which make promises about how the user's personal data will be processed, and that term must have been breached.
- Liability for breach of that term must not be excluded by the contract.

Assuming a contractual relationship exists, the next step is to identify a term, which makes promises about personal data processing. The first place to look is the wording of the terms of service, i.e. an express contract term.

However, it is unlikely that such a term will be found. Previous research for A4Cloud has examined the standard terms of cloud providers, and finds that almost universally they refuse to make any promise about how a user's data will be handled. Indeed, those terms go further by specifically providing that maintaining the confidentiality and integrity of data is solely the responsibility of the user, not the cloud provider.[67] That research suggests that express terms accepting liability for data security and disclosure, which are the most likely basis for claims by a data subject, are unlikely to be found in standard terms in the foreseeable future.

The lack of any express term is not fatal, though. Most national law regimes will imply terms into contracts, and if breached those implied terms will give rise to liability unless that liability has been excluded successfully (see below). The law relating to such liability has been analysed at length in another research deliverable for A4Cloud[68], and what follows is a summary of that analysis.

[66] For very specific cases and circumstances the Dutch Administrative Law Act or other specific legal a
Acts can limit this freedom. It goes beyond the scope of this deliverable to delve into these specific cases.
[67] Niamh Gleeson & Chris Reed, D: D-4.2 Survey of cloud standard contract terms and SLAs in 2015, section 3.6 to be published on www.a4cloud.eu.
[68] Chris Reed, Asma Vranaki, Lorna Cropper, Petra Zabudkova & Lorenzo Dalla Corte, *D-4.12:* A4Cloud Tools, Liability and Compliance Investigations .

Under English law[69] the relevant element of the contract is the data processing service provided to the user. In any contract for the provision of services, section 13 of the Supply of Goods and Services Act 1982 implies into the contract a term that the service provider will take reasonable skill and care in the service provision. The question is therefore whether the service provider failed to take such care.

The test, established over 150 years ago for extra-contractual liability but applied also to contractual duties of care and skill, is as follows:

> 'Negligence is the omission to do something which a reasonable man, guided upon those considerations which ordinarily regulate the conduct of human affairs, would do, or doing something which a prudent and reasonable man would not do.'[70]

This test is clearly context-dependent – for example, what might be adequate care to protect non-sensitive data could be held inadequate in the case of sensitive data. Relevant factors which the court would take into account include the service provider's knowledge of the risks to the data subject if data is insecure or improperly disclosed, any knowledge the provider has about defects in the workings of its systems, and of course whether there are relevant technical standards which the provider has adhered to.

The existence of data protection regulation will, in our view, be a relevant factor for the court to consider. The regulation, together with guidance material issued by supervisory authorities, sets out a standard which a reasonable service provider should aim to achieve. Nonetheless, we must stress that the contractual obligation is one of care and skill, not an obligation to achieve the regulatory standard, and so breach of the regulatory standards might be evidence that insufficient care and skill was taken but will not be conclusive.

Civil law countries are likely to take a similar approach. For example, although under Italian law there is some uncertainty about how cloud computing contracts should be classified, the most likely approach (supported by DigitPA, the former Italian Agency for the Digital Agenda, in its guidelines on cloud computing and public procurement)[71] is to apply the appalto di servizi regime. Under this regime the primary contractual obligation of the service provider is to perform the contract using appropriate care and skill. The level of care and skill required will be that of the appropriately qualified professional. In the Dutch Civil Code there is an obligation for contractors to carry out their obligations according to a duty of care (Art. 7:401 of the Dutch Civil Code). The scope off the duty of care must be assessed on a case-to-case basis. Guidelines to determine this scope have been developed in case law for specific professional domains such as banks, the notary and real estate brokers. If a contractor has lived up to his duty of care also depends on the expertise of the contractor.

The final obstacle to any claim will be the exclusion of liability clauses that are universally present in cloud computing contracts.[72] However, such clauses are unlikely to be enforceable against data subjects who make their contracts as consumers. This is because the Directive on unfair terms in consumer contracts[73] provides that a term in a B2C contract which is unfair will not be enforceable against the consumer, although the contract will still subsist so far as is possible and its remaining terms will be enforceable.[74] Our previous research concludes that the effect of the Directive is that limitation and exclusion clauses will rarely, if ever, be enforceable against a consumer.[75]

In rare instances, the data subject might enter into the cloud computing contract in a non-consumer capacity (e.g., as the proprietor of a small business) but nonetheless store his or her personal data with the service as well as business data. In these circumstances the unfair terms Directive would not

[69] There are some differences in the UK between the laws of England & Wales, Scotland and Northern Ireland, though the practical effect is very similar so far as the liabilities discussed here are concerned.
[70] *Blyth v Birmingham Waterworks Co* (1856) 11 Ex 781, 784 per Alderson B.
[71] Reccomandazioni e proposte sull'utilizzo del *cloud computing* nella pubblica amministrazione, 28 June 2012, http://www.agid.gov.it/sites/default/files/documenti_indirizzo/raccomandazioni_cloud_e_pa_-_2.0_0.pdf.
[72] Gleeson & Reed, n 67, 3.14-3.16.
[73] Directive 93/13/EEC, OJ L 95 April 21 1993.
[74] Art. 6(1)
[75] Reed, Vranaki, Cropper, Zabudkova & Dalla Corte, n 68, 5.1.4

invalidate the exclusion or limitation of liability, but national law controls on such terms might still produce the same effect.[76]

Thus, our conclusion is that data subjects who enter into cloud contracts as consumers will be able to seek compensation under the contract for wrongful disclosure or breach of security in respect of their personal data. The data subject will need to prove that the cloud service provider failed to take such care as would be expected from a reasonable service provider to prevent the disclosure or security breach, and the court will probably take into account (inter alia) the obligations placed on the service provider by data protection regulation.

3.6 Data subject redress under extra-contractual liability

Extra-contractual liability is extremely complex, and differs markedly between common law and civil law legal systems. In both cases liability is primarily based on negligence, i.e. the failure to take reasonable care to avoid the loss or damage to the claimant. Common law looks for a relationship between claimant and defendant which is sufficiently close to justify imposing a duty of care on the defendant. Civil law imposes an obligation in the relevant civil code on every person to take reasonable care, though in practice the closeness of the relationship may influence the court's decision about how much care should have been taken.

The laws of England and Italy were explained in some depth in previous A4Cloud research[77], and readers are directed there for the detailed analysis and references. Applying that analysis to a data subject's potential claim, we reach the following conclusions.

First, if the claim is in a common law court, the data subject will need to persuade the court that the defendant owes a duty of care. The court considers a range of factors, the most important of which are:

- Whether the defendant ought to have foreseen that its actions or inaction (in our case, in respect of the data it processes) might cause loss or damage to the claimant; and
- Whether the defendant has in some way undertaken responsibility to take care to protect the claimant's interests.

There is a strong reluctance on the part of the common law to impose a duty of care towards the whole world, or even a substantial subset of it. Let us take the example of an SME cloud customer, which collects personal data from data subjects and processes them using a cloud service provider, which makes use of sub-processors. In this example the SME cloud customer will certainly owe the data subject a duty of care in negligence. The cloud service provider might owe such a duty, depending on its knowledge about the personal data which it is processing on the SME's behalf, whilst the sub-processors are very unlikely to owe the data subject a duty of care. Of course, the SME/service provider/sub-provider chain is connected through a series of contracts, so if one is held liable because of the actions of someone further down the chain that liability can be passed on via contract. However, negligence liability is based on the degree of care taken by the defendant – thus if the SME takes reasonable care in choosing a service provider and monitoring its activities, the fact that the service provider was careless will not impose liability on the SME.

By contrast, under civil law all those in the processing chain will owe an obligation of care to the data subject. How far the courts will treat remoteness in the chain as a relevant factor in deciding the level of care to be taken has yet to be decided.

Breach of this obligation of care is assessed by the same standards as for contractual duties of care (see above).

There is one further possible claim under common law, a claim for breach of a statutory duty. The relevant duty here would arise from the obligation imposed by national implementations of the DPD (or directly by the GDPR once enacted and in force) to comply with the data protection principles – in the UK, section

[76] Ibid.
[77] Ibid.

4(4) of the Data Protection Act 1998. This claim was asserted in the *Vidal Hall* litigation referred to above[78], but the full hearing of that claim is delayed pending the appeal on whether damages for distress can be claimed under section 13 of the Act.[79]

For such a claim to succeed, (a) the duty must be intended to protect the individual claimant, which is obviously the case here, and (b) the court must be able to interpret the statutory duty as one for which the legislature envisaged a civil claim, rather than some alternative remedy. This second point is where a claim for breach of statutory duty might fail, as section 13 sets out an express right to claim damages in more limited circumstances than a claim for breach of the section 4(4) duty would permit, and the Act provides an alternative means of enforcing the section 4(4) duty via the ICO.

3.7 Proving a data subject's claims

We have identified three possible routes for a data subject to make a claim if personal data is wrongfully processed (including disclosure or deletion):

- A claim against a data controller for breach of data protection regulation;
- A claim for breach of contract against some person who owes the data subject a duty to process the data in a particular way[80]; or
- A non-contractual claim, most likely for breach of the general law duty not to act negligently.

In each case, the data subject will need to prove that claim to the court or administrative tribunal. This is done by putting forward evidence. Without evidence, the claim will be dismissed.

For all these claims it will be necessary for the data subject to prove the wrongful processing. This is problematic because the evidence about what was done with the personal data will usually be in the possession of the defendant. There are four ways in which the data subject may be able to secure access to that evidence:

- The data subject might have access to information about processing as part of the service it receives from the defendant, e.g. if the claim is against the subject's cloud service provider. Accountability requires a service provider to make information about processing available to customers and data subjects in the ordinary course of events, and that information will be accepted by the courts as evidence of how the data was processed.
- If the supervisory authority has investigated the alleged data breach, some information about the results of that investigation might be made available to the data subject. Whether this happens differs between Member States, and how far the conclusions of the supervisory authority are treated as evidence of a breach will depend on the attitude of the individual court or tribunal.
- The data subject might obtain specific information from the defendant, in advance of making the claim, about the event on which the claim is based. That information might be given voluntarily, e.g. using the IMT tool, or may be provided to fulfil an obligation under the law – examples here include data subject access requests and the new obligation in the GDPR to report data breaches.
- As part of the litigation process, once the claim has been filed the data subject may be entitled to demand or request information. The rules governing this are found in national civil procedure regulations, and so differ from country to country.[81] In very simplistic terms:
    - The principle in the common law countries is that each party to litigation is entitled to disclosure of all information in the other party's current or former[82] possession which is relevant to the litigation. Once these "discovery" lists have been exchanged, each party

[78] Vidal-Hall & Ors v Google Inc [2014] EWHC 13 (QB) (16 January 2014).
[79] If the final decision is that damages for distress can be claimed, our prediction is that the court will make no decision on the claim for breach of statutory duty.
[80] Either to process it as promised in the contract, or more generally to process it using reasonable care and skill.
[81] A helpful explanation of the fundamentally different starting points and their consequences can be found in Geoffrey C. Hazard Jr, "Discovery and the Role of the Judge in Civil Law Jurisdictions" (1997-8) 73 Notre Dame LR 1017.
[82] In our context, this means that each party must disclose the former existence of potentially relevant information which has been deleted, e.g. emails, logs, internal reports, etc.

can request some or all of that information from the other. If they cannot agree whether particular information should be disclosed, the court or tribunal will decide the issue. At first sight this approach seems very favourable to claimants, but in practice the complex rules which control pre-trial disclosure can be used to make the claimant's task more difficult and expensive (e.g. by disclosing a mass of material which requires sophisticated tools to search and analyse), and the rules require litigation expertise to use them effectively.

- In civil law countries there is no principle of compulsory disclosure that potentially relevant information exists. It is for the court or tribunal to decide what, if any, information should be disclosed, and at what point in the proceedings. Civil law courts are not limited to considering the evidence put forward by the parties, but can demand whatever evidence they consider is needed to decide the case.

Even if the data subject has produced evidence of wrongful processing, that may not be enough to establish the claim. For claims based on breach of data processing regulation it will be sufficient, as it is then for the defendant to prove that it was not responsible for the breach.[83] However, if the claim is for breach of a contractual or extra-contractual duty of care, the data subject will have to go further and produce evidence (a) that the defendant failed to exercise the required degree of care, and (b) that the failure caused the loss for which compensation is claimed.

The principles which a court will apply to decide this question have been explained in previous A4Cloud research[84], but what is needed to prove breach of a duty of care is different in each individual case. At a high level, the claimant needs to establish the standard of care which should have been achieved, usually by putting forward evidence of industry best practice in the field, and then adduce evidence which shows a failure in the particular circumstances to meet that standard.

As an example, let us suppose that a cloud service provider discloses personal data to some person to whom it should not have been disclosed. The data subject is likely to have to obtain evidence about a number of issues:

- Evidence that the disclosure occurred.
- Evidence as to the cause – possibilities include hardware failure, software logic defects, human error, deliberate human action or third party interference (e.g. hacking).
- Evidence as to the standard which should have been achieved. It is important to note that an obligation to take care is not breached unless insufficient care has been taken. If, for example, the cause was human error, then the evidence will need to show what precautions *ought* to have been taken against such error, perhaps by reference to industry standards of training and system design.
- Evidence that the defendant failed to meet that standard, for example by requesting disclosure of training practices.

How far down this evidential chain the claimant needs to go will depend on the court's assessment of previous elements. Some failures will so obviously be likely to be the result of negligence, such as hackers gaining entry through known security flaws for which a fix is readily available, that the court will require little more than proof that this was the cause of the disclosure. Others, such as deliberate disclosure by a trusted employee, will require evidence that the defendant should have recognised the risk and guarded against it.

[83] See 3.2 above.
[84] Reed, Vranaki, Cropper, Zabudkova & Dalla Corte, n 68.

4 Use case scenarios

This section describes a set of use cases for incident management and response in the cloud. They reflect typical classes of incidents and hence are appropriate for developing and testing IMT and RRT. The discussion provides a short description for each use case explaining how it is supposed to be detected. Furthermore, it sets out what information can be communicated about the incident to the involved stakeholders and indicates the incident category.

4.1 Virtual Machine (VM) Migration

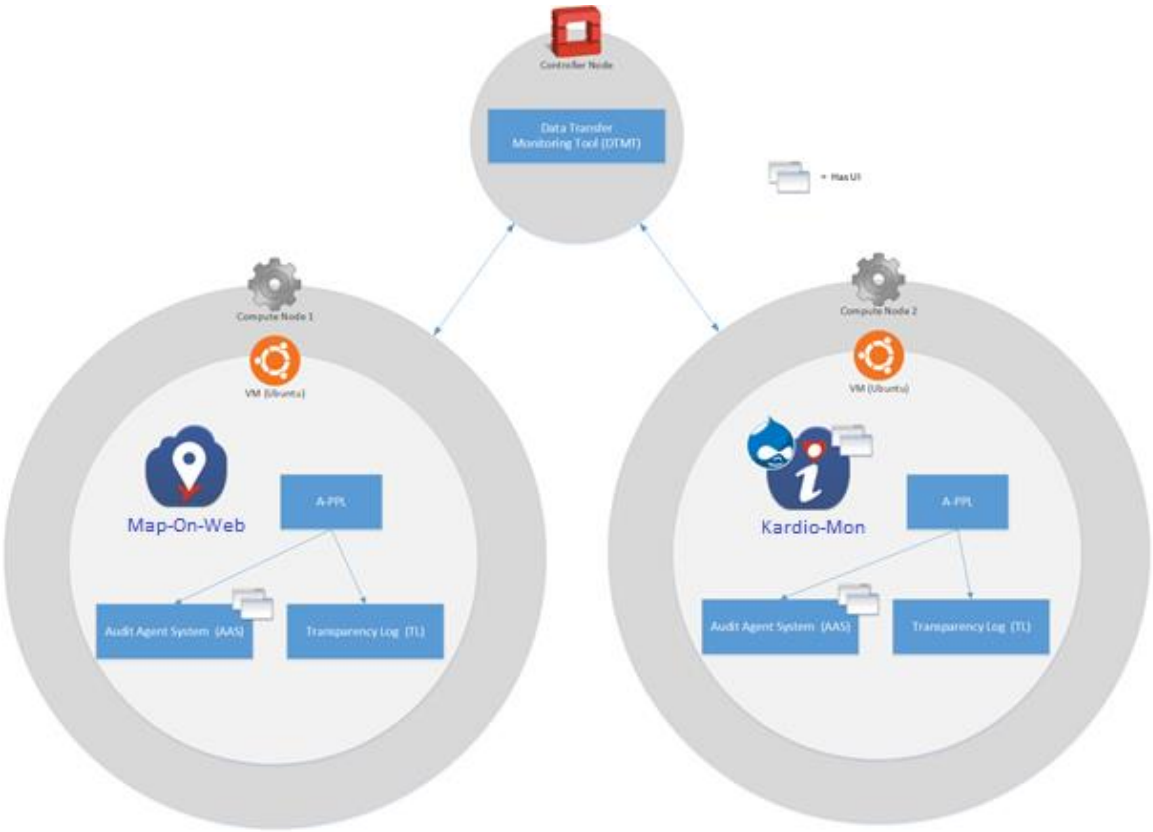


Figure 1: Wearables use case architecture, borrowed from D7

We consider here the demonstrator use case of A4Cloud[85].The Wearable Use Case has been designed to demonstrate the accountability framework and the respective tools developed by the A4Cloud project in a real world example of a cloud service supply chain. WearableCo is a cloud customer (data controller) offering services to cloud subjects (data subjects), by using a SaaS service offered by Kardio-Mon, which in turn uses another SaaS service by Map-On-Web; both SaaS services (incidentally) run on top of the same IaaS service.

An Infrastructure as a Service (IaaS) provider has the power to perform sensitive operations on the virtual assets owned by its tenants (for instance, in the Wearable's use case, this is the role of Wearable-Co). Usually such operations are transparent to the cloud customers because they have no implications to the compliance of the tenants with respect to policies and regulations. However, some operations may affect compliance with regulations and standards, for instance data transfer and duplication. Automated

[85] Giotis et all, "D:D-7.1: First system and use case prototype'' to be published on www.a4cloud.eu.

processes run by the infrastructure provider (in the running use case, the role of “IaaS Cloud Provider”, in D7 called DataSpacer) can transfer resources to data centres located in different jurisdictions. Such operations in many cases are agreed and expected in order to create data redundancy and thus resilience for the cloud consumer, but in some cases, this may represent a violation of the contract and policies in place. In most cases, it is possible to detect such data movements at runtime, but at the same time, it is very hard to determine if the data transfer is authorised or not, given the very complex nature of the regulations and the dynamicity of the cloud landscape.

4.1.1 How the incident are detected by A4Cloud tools

In order to provide transparency to its customers, the cloud provider agrees to run a monitoring tool (the Data Transfer Monitoring Tool, or DTMT) capable of analysing the infrastructure data flows to detect potential violations. The tool receives as input an APPL policy from which it extracts the permissible location of data and the identification and contact details of the data controller. It also receives as input a configuration file provided by the cloud provider about the physical location of its servers, and the endpoint for the A-PPLE (Accountability Policy Engine) running on the behalf of that tenant (Wearable-Co). Such input needs to be audited by an independent party to assert its correctness. The tool uses a set of inference rules over the stream of events on the cloud infrastructure Application Programming Interface (API).

Figure 1 depicts the environment set up in work package D7. The controller node runs Openstack and is under control of the IaaS provider. It will analyse Hypertext Transfer Protocol (HTTP) requests to the controller node concerning creation and instantiation of virtual disks and machines, backups, and server migrations in order to determine potentially invalid data flows – Figure 2 illustrates the message sequence diagram for DTMT.

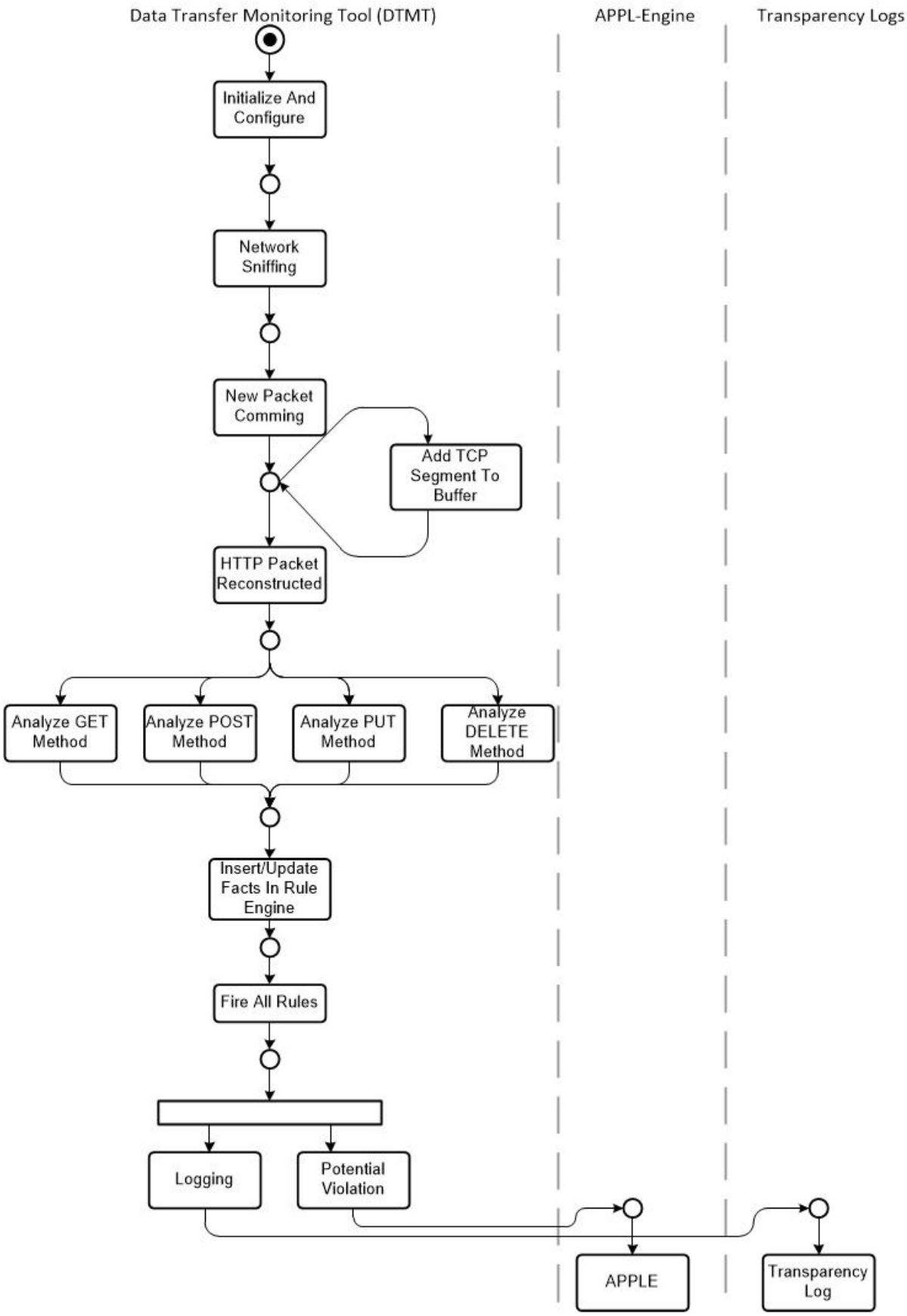


Figure 2: DTMT sequence diagram, taken from D3

Upon detection of a potential violation, the DTMT tool will log the details about the incident in the transparency log (TL), including time, the concerned dataset, the originally allowed location, and the current location. It will fire a trigger in the APPLE endpoint to handle a policy violation event. The current deployment in the demonstrator transmits the incident information to the Incident Management Tool configured in the engine instance.

4.1.2 Communicated Information regarding the incident

The IMT tool, described in Section 5, allows coordinating how incident information is transferred across the cloud supply chain. In the case of the scenario explained here, distinct events logged during the process can be used to communicate about the incident, including the Openstack logs, the DTMT logs, the VM logs. Some configuration information may be also necessary, such as, what are the allowed locations for the tenant's virtual machines.

4.1.3 Incident category

It's a privacy incident, since it is a breach of the data protection regulation in place.

4.2 Data retention violation

An accountability policy may contain obligations concerning how long personal data is kept by the data controller. The A-PPL Engine will automatically delete from its database all personal data which reached the expiration date and time. However, this may not be synchronized with replication or backup storage system, which usually depends on infrastructure layer services. Therefore there may be an incident where the accountability engine removes data from the live system, whereas backups maintain previous versions of the database where the deleted items are still present. AAS is able to correlate A-PPL engine logs with storage system information in order to identify such undesired situations.

4.2.1 How the incident detected by A4Cloud tools

AAS requests A-PPLE's logs via TL. The A-PPL Engine also stores internal logs that can be useful for AAS. These logs are outsourced to the TL. Being added as additional recipient for the TL instance allows an agent (who is familiar with this TL endpoint and was set up as recipient including key pair) to check this TL periodically for new logs. If an incident occurs and is classified as violation, this element is transformed into a policy violation record (as defined in the Framework of Evidence[86]) and stored inside the AAS's local evidence store. The Figure 3 illustrates the process.

[86]Agrawal et all ''D:C-8.1 Framework of evidence'', available at: http://www.a4cloud.eu/sites/default/files/D38.1%20Framework%20of%20evidence.pdf

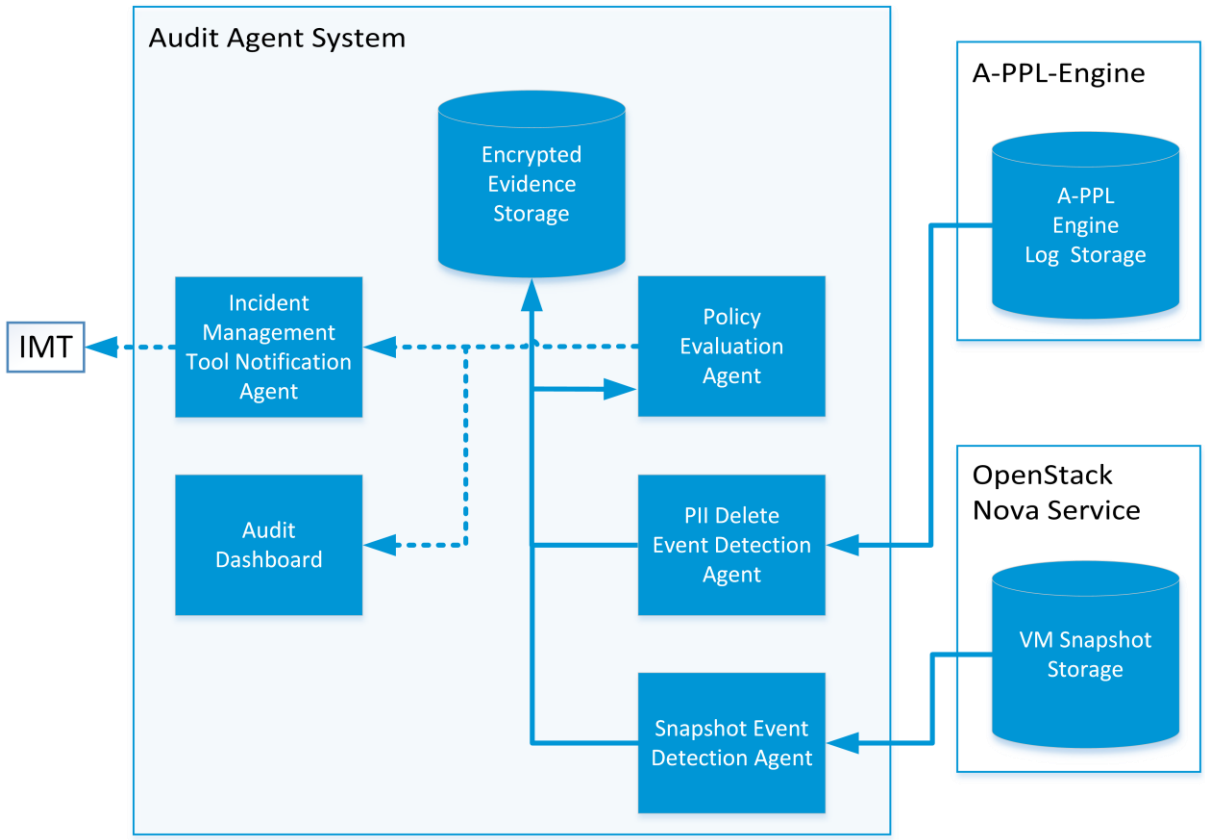


Figure 3: Data Retention Audit Task in AAS

4.2.2 Communicated information regarding the incident

The relevant information in this scenario are the concerned personal data type (for instance, home address, telephone number, etc.) that was supposed to be deleted, its expiration date, how long the item was kept after its expiration date, perhaps also if the backups were accessed or even restored after the expiration date. It may also include other events logged by the multiple architectural components. The Incident Management Tool Notification Agent, represented in Figure 3, transmits the aggregated incident information to the configured IMT instance.

4.2.3 Incident category

It is a privacy incident, since it is a violating a constraint in the privacy policy (more precisely, accountability policy) agreed with the data subject.

4.3 Lost laptop

A Kardio-Mon laptop containing sensitive info (e.g. production data) is lost (either by being forgotten at a bar or through theft from a parked car).

Severity depends on actual content on laptop, and whether or not the following security mechanisms are in place:

- Full Disk Encryption
- Database Encryption

4.3.1 How the incident detected by A4Cloud tools

This incident cannot be detected by A4Cloud tools. It must be detected by a human (presumably by the employee in possession of the laptop), and the incident must be entered/triggered manually into the IMT console by a Kardio-Mon operator.

4.3.2 Communicated information regarding the incident

WearableCo must be notified that their production data has been lost. Currently, this is done by manually informing the WearableCo Privacy Officer.

Severity evaluation (in increasing order, assuming that the encryption key was not stolen as well):

1. Data protected by full disk encryption AND database encryption
2. Data protected by full disk encryption
3. Data protected by database encryption
4. Data in plain text

WearableCo must determine which individuals are affected by data loss, based on the policies stored in Kardio-Mon's A-PPL Engine. In practice, they should notify all their customers, in particular if they cannot be sure who has been affected and who hasn't. For example, it is common practice to advice all users to change passwords even though only some of the passwords have been compromised.

Since data presumably is personal data in this particular use case scenario, all affected customers must be notified within appropriate time limits, as prescribed by regulations, regardless of severity.

Notification sent to A-PPLE, forwarded via TL to Data Track backend and finally to the RRT.

If data contains end user passwords (or password hashes), then the affected end users must be advised to change passwords, except if this data was encrypted (severity cases 1 to 3 described above).

4.3.3 Incident category

It is a security incident. This may lead to a privacy breach, as most security incidents.

4.4 Misconfiguration

Misconfiguration of services and failing to patch software quickly can lead to severe security problems such as being vulnerable to exploits and violating security requirements. Recent SSL vulnerabilities such as POODLE, BEAST and TLS vulnerabilities, like Heartbleed, are prime examples for the need to patch as soon as fixes become available. However, patching may not be enough in some cases. For instance, to mitigate the Heartbleed vulnerability, certificates need to be replaced, old certificates revoked and private keys changed. Besides that, problems can arise from service misconfiguration. The recently discovered POODLE vulnerability is closely linked to obsolete protocols being allowed (which is an SSL configuration problem). Also, in cases where strong cryptography is required, specific SSL configuration is required (protocol versions, available cipher suite, cipher order, algorithms, key length, certificate status…). AAS can be used to perform checks on both patch management (checking a server's installed packages and comparing versions against a known-good list) and configurations (checking previously described parameters in service configuration files). Additionally, in cases where files cannot be accessed directly, agents can perform vulnerability checks externally by using port scans, protocol validation and performing security scans/vulnerability checks.

4.4.1 How the incident detected by A4Cloud tools

- Internal service audit:
- File alteration monitoring and triggered configuration file audit (e.g., admin error)
- Keyword search, parameter checks in configuration files
- new/changed files (e.g., certification for file changes)
- Software version checks (checking critical patches ,using the packet management system)
- External service audit:
- Port scan (only secure configuration visible externally, e.g. no plain text connection possible)

- Protocol validation (valid certificates, valid/secure cypher suite, recommended key properties (size etc.), secure protocol versions)
- Vulnerability check: e.g., specific agent for detecting POODLE, BEAST, Heartbleed etc.

4.4.2 Communicated information regarding the incident

- Timestamp of incident detection
- Vulnerability assessment with respect to known attacks
- Details of configuration parameters in violation of security policy (config lines; software version mismatch; not who made the changes since this may not be known)

4.4.4 Incident category

It is a security incident. The cloud supply chain was unable to maintain security controls to their best performance, detecting the issue and taking due action in time. After detection, the CSP has obligation to notify.

4.5 Data access attempt for illegitimate purposes

Consider the demonstrator use case, where WearableCo is a cloud customer (data controller) offering services to cloud subjects (data subjects), by using a SaaS service offered by Kardio-Mon, which in turn uses another SaaS service by Map-On-Web; both SaaS services (incidentally) run on top of the same IaaS service.

4.5.1 How the incident detected by A4Cloud tools

If an actor tries to access data for a non-authorized purpose, then the access request is denied, raising a personal data access denied event in the policy engine. If there is an obligation in the obligation set of the policy associated with this personal data matching such event, then the corresponding action is executed. For instance, the action can be to log the access attempt, to notify the data subject and/or controller.

All access to personal data must be mediated by the policy engine, which will enforce the accountability policy it was configured with. A data controller will always adhere to this constraint in the case it wishes to easily demonstrate its accountability, in principle. The deployment of the engine in a given cloud landscape should be audited by an independent party in order to provide assurance to the cloud customers about this.

4.5.2 Communicated information regarding the incident

The policy must specify which fields should be included in the action log. That is, the information depends on what the data controller wants to have as part of the log. In the case of action notify we have type of the event (access permitted, deleted, unauthorized access attempt), the media for contact (e.g. email address), and the recipient.

4.5.3 Incident category

This case is actually not an incident, but an attempt (which is blocked by the policy engine).

4.6 Right to know vs. Need to know

Access rights on personal data are enforced in the A-PPL-Engine. However, there are cases, where an individual access request is granted (necessary privileges available) but context information (e.g., large number of access requests in a short period of time) indicates a violation (e.g., malicious insider, hacked account). Monitoring such scenarios is typical for intrusion detection systems (IDS). AAS agents can be used to interface with existing intrusion detection systems (e.g., register themselves as receiver of alarm events, polling for events) or implement intrusion detection mechanisms/tools themselves (e.g., log analysis component).

4.6.1 How is the incident detected by A4Cloud tools

- Intrusion detection (on database entries, API calls, network traffic monitoring)
- Behaviour analysis (learning data access patterns)
- Log analysis (specifically error logs)

4.6.2 Communicated information regarding the incident

- Timestamp
- Details of intrusion (who, what, reason for alarm etc.)
- Data subject
- Notification of a security incidents without details (won't understand it anyway)

4.6.3 Incident category

Breaching the principle of need-to-know is may also lead to breaching the data minimization principle put forward in the EU Data Protection regulation (and others). Such an incident is therefore considered as a privacy incident.

4.7 Unavailability

Cloud computing can be used to improve availability (by buying redundancy, qualified admins, distributing across data centres etc.). However, it is important that availability is clearly defined at the beginning (considering maintenance time, etc.) However, there can be service outages and hardware failures are quite common due to focus on consumer-grade hardware. In some cases, hardware failures can lead to lack of service availability. This is a common problem and is addressed by using redundant systems. When redundancy fails (e.g., whole data centre unavailable and no off-site) user's need to be informed accordingly. AAS can be used to gather availability information, performance counters etc. from various sources, such as the cloud management system (e.g., OpenStack), a dedicated server monitoring tool (e.g., Nagios) and from custom probes (e.g., simple ICMP probe, application level probe) to detect service availability incidents.

4.7.1 How is the incident detected by A4Cloud tools

- Infrastructure/hardware monitoring (server, network components…)
- ICMP probes/agents at network level (very low-level, initial indicator, but not adequate)
- Higher protocols probes/agents at application level (e.g., HTTP, automated service login)
- Hardware failure does not necessarily impact service availability immediately (redundancy), availability check on application level required

4.7.2 Communicated information regarding the incident

- Timestamp
- Duration of the outage
- "Component" availability incident details (only if it impacts service availability)

4.7.3 Incident category

It is a service incident, as the cloud supply chain was unable to fulfil the SLA.

5 Incident Management Tool (IMT)

The Incident Management Tool (IMT) is a tool targeted at organisations and teams that handle computer security incidents. In practise this means any organisation that provides or consumes an internet service. The targeted audience of IMT is not the cloud subject, but rather professional incident handlers and privacy officers that produce it. The contribution of IMT is a simplified incident format and a simplified incident exchange, making the solution usable for small companies as well as large. IMT provides support for cloud service provision chains, while maintaining traceability of the incidents and its way through the chain. Through the integration with the A4Cloud toolset, the incident handler is able to send notification directly to the affected cloud subjects.

5.1 Introduction

A problem experienced by incident handlers in the context of cloud computing is the lack of access to sufficient incident information throughout the cloud provider chain[87]. WearableCo would not necessarily receive the needed information from Kardio-Mon, nor Kardio-Mon from DataSpacer, etc. Furthermore, complicated cloud provider chains with multiple participants increase the need for more automated sharing of incident information, potentially allowing for automation of some response actions as well.

IMT operates in the direct context of multiple tools from the A4Cloud toolkit, namely DTMT, AAS and A-PPLE. IMT receives detected incidents from DTMT and AAS, and utilises A-PPLE to notify end users about incidents relevant for them. When a notification of end users occurs, IMT sends a notification to A-PPLE, A-PPLE provides this information to Transparency Log (TL), and Data Track fetches this information from TL in order to inform the end user about the incident. Subscribers – that is cloud customers who utilise services from a provider and have an IMT instance – can receive incident notifications from the provider's IMT to their own. IMT is also useable outside the context of A4Cloud tools as a way for organisations to communicate incident information and have this information propagate the cloud service provisioning chain.

The IMT interacts with other instances of IMT and other tools by a simple, extensible incident format and a publish-subscribe based API – making the solution usable for small companies as well as large. The integration with A4Cloud tools allows for easy notification of end users. The solution supports incidents propagating through the Cloud Service Provision Chain while preserving traceability. The IMT user interface targeting humans consists of a dashboard in which incident handlers and privacy officers can manage subscriptions, incidents and notifications of both other instances of IMT as well as A-PPLE instances capable of notifying end users.

5.2 General Concept

When using IMT, a human is involved in making the decision on whether or not to notify subscribers and end users. This is because few or no companies would agree to send their incidents directly to the cloud subjects or cloud customer subscribers without any filtering. Thus, the company can decide when to notify their subscribers and end users. A potential problem with this approach could be that the company might decide not to notify about some incidents, but this should be prevented by maintaining an audit trail.

When the Privacy Officer of DataSpacer first configures IMT, he adds the incident types – or incident categories – that Kardio-Mon is allowed to subscribe to. He also adds definitions of under which circumstances Kardio-Mon will be allowed to receive such incidents.

[87] Jaatun, Martin Gilje; Tøndel, Inger Anne, "How Much Cloud Can You Handle?," in Availability, Reliability and Security (ARES), 2015 *10th Int. Conference on*, pp.467-473, 24-27 Aug. 2015, available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7299953&isnumber=7299862

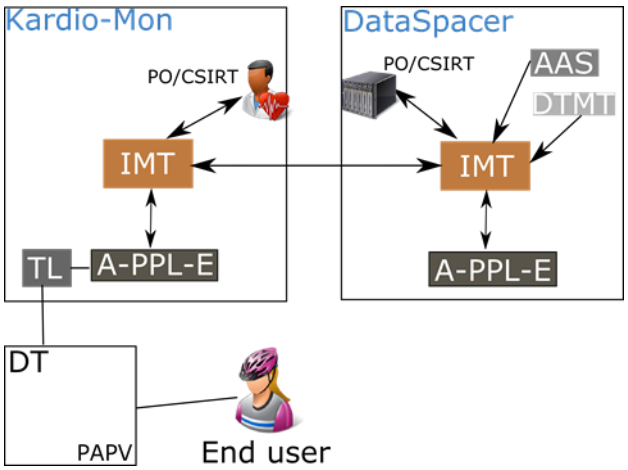


Figure 4: A simple Cloud Provision Chain

When Kardio-Mon becomes a customer of DataSpacer, the privacy officer of Kardio-Mon adds DataSpacer as a provider, which in turn makes the IMT of Kardio-Mon add itself as a subscriber to the IMT of DataSpacer. He then creates a subscription using the incident types made available by the privacy officer of DataSpacer, who also needs to approve the subscription.

The two instances of IMT are now configured to work together, as shown in Figure 4. The IMT of DataSpacer is configured as a provider for Kardio-Mon and the IMT of Kardio-Mon as a subscriber to DataSpacer. This means that DataSpacer is able to provide Kardio-Mon with relevant incident information.

When, e.g., the DTMT of DataSpacer identifies an incident, it creates a report and provides this information to IMT. An incident handler – in most cases a person– is notified about the received incident, examines it, obtains permission from the privacy officer and sends a notification to their subscribers – here exemplified by only Kardio-Mon. Kardio-Mon receives the incident from DataSpacer, an incident handler is notified and he examines the incident. If the incident relates to end-users they manage on behalf of WearableCo, he needs to get permission from the privacy officer of WearableCo before notifying end users – this demands that proper contracts are in place to assign the role of notifying end-users to a Kardio-Mon, and Kardio-Mon would probably need to identify themselves as WearableCo when notifying end-users. If the incident relates to end-users belonging to Kardio-Mon the incident handler needs to obtain the permission of the privacy officer of Kardio-Mon. After obtaining the permission/decision, he constructs a message that is understandable for end users and passes it to A-PPLE. A-PPLE logs the incident into Transparency Log, from which DataTrack fetches the information and presents it to the end user. The end user might now use RRT to perform remediation actions. If WearableCo had their own instance of IMT, Kardio-Mon would send the incident to WearableCo and leave the end-user notification to the incident handlers of WearableCo – in the exact same manner as DataSpacer did with Kardio-Mon.

5.3 User Interface

The Incident list is the centre of IMT, as this is where the incident handler gets an overview of the incidents in need of attention as well as his starting point for actually handling the incidents. Figure 5 shows how such an incident list could look and how it is currently implemented in IMT. The UI outline of the application has three areas:

- The blue bar on top gives the user access to messages, alerts and profile management
- The dark sidebar gives the user easy access to all the features of the tool
- The main (white) area is where new content appears on each page

The Incident list in Figure 5 displays information about incidents, in order to help the incident handler to prioritise which incidents to handle first. Both state and impact are colour coded, in order for the incident handler to easily get an overview of which incidents are resolved and which are not, as well as the degree

of impact of each incident. The impact of the incident is a high-level method for prioritizing the order in which to handle incidents, even though relying solely on that value means fully trusting the judgment of another incident handler – potentially at another organisation with another infrastructure and different threat situation.

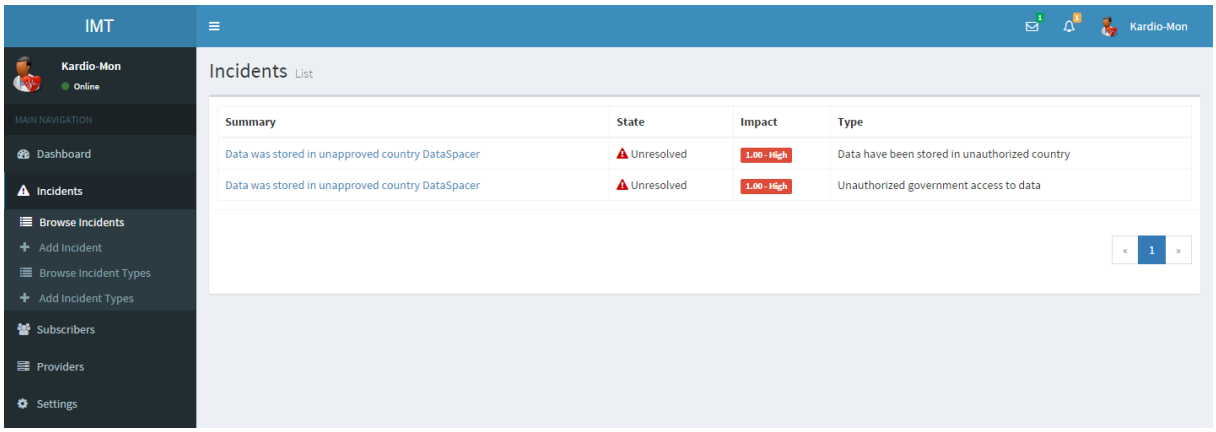


Figure 5: The Incident List

Figure 6 shows the detailed view of an incident, in which the incident handler is also able to add and manage attachments. The two-column layout holds multiple boxes of information and actions. The top left hand box contains information about the incident itself. The bottom left box holds attachments as well as allows the handler to add new attachments. Attachments are of predefined types in order to ease their handling. Above the attachments, custom fields and their values are shown, if the incident type has any associated custom fields.

The top right hand box presents information about who has the lead on the incident in question. This is important in order to avoid situations where different people believe someone else is responsible and the incident is never handled. By designating a specific lead for the incident, and giving this information a prominent place in the incident tracker, all involved parties can be sure that incidents are handled and by whom. This does not mean that the lead needs to work on the incident alone, but rather that he is responsible for the incident and its activities. The next box presents information about the incident's liaison - the person to contact if more information is necessary, to provide more information or any other matter. In this case, it is a support centre, but it might just as well have been a specific person. For example, for large customers it could have been their designated contact in the provider's incident management team.

The box titled “End user notifications*”* contains a list of notifications that have been sent to end users, who have been affected by this particular incident. The tool operator is also able to send new notifications to the end users by clicking on the “Send notification button’’, at which time he will be asked to write a message to the end user about the incident at hand.

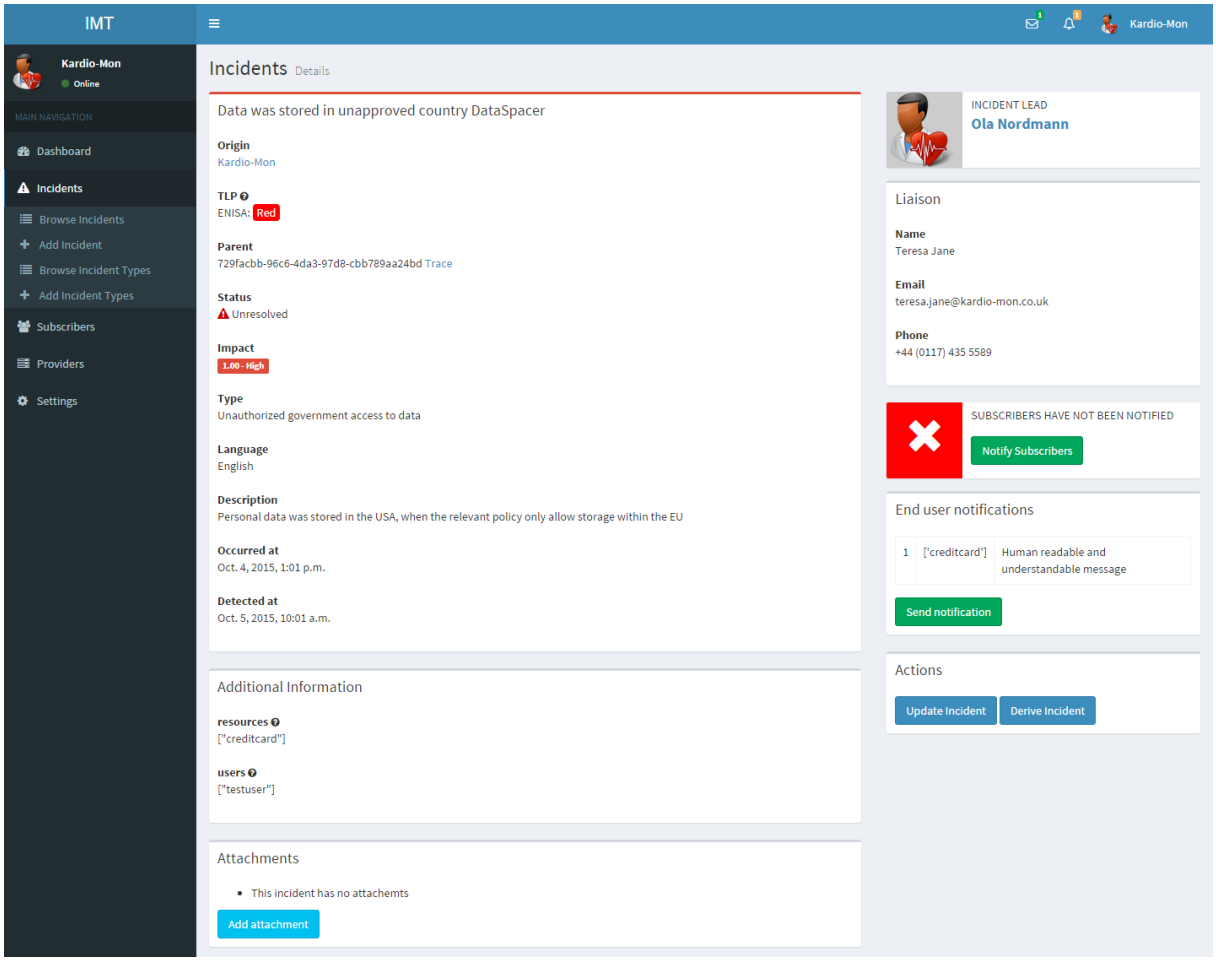


Figure 6: Detail view of an incident

The bottom right box holds the actions available to the incident handler. He is able to update the information in the incident, and notify the subscribers if the incident is created by his organisation. If the incident is received, the incident handler needs to derive it - create a new incident based on the received one - before being able to notify subscribers; this is done to preserve traceability. When a handler presses the button Notify Subscribers, all subscribers that subscribe to a notification involving the incident type and which fulfils the defined triggers, will be notified.

5.4 Incident Format

Schneier[88] claims that "Incidents aren't standardized; they're all different." The National Institute for Standards and Technology (NIST)[89] further states that each CSIRT must choose their own list of required data elements, based on factors like team model, team structure and how the team defines an incident. This raises the question of whether it is actually possible to represent every incident in one format, or whether it would be a better approach to allow multiple formats and thus allow for specialisation. By using only one format that is able to represent everything, one could, theoretically, know that all conforming implementations would be able to understand any incident received and be able to handle it automatically, if desired. On the other hand, the format would be very complex, as it needs to include mechanisms to represent all possible relevant information for any incident imaginable.

[88] Schneier, Bruce, "The Future of Incident Response" in *Security & Privacy, IEEE*, 2014,volume 12, pp.95-96, available at : http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=6924685

[89] Cichonski, Paul; Millar, Tom; Grance, Tim; Scarfone, Karen, "Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology, 800-61. Revision 2", 2012, available at: http://dx.doi.org/10.6028/NIST.SP.800-61r2

We have found the Incident Object Description Exchange Format (IODEF)[90] to be a comprehensive format for expressing incidents. While IODEF in practice can support any property included in other relevant formats, including Structured Threat Information Expression (STIX) format[91], eCrime[92], and Cyber Observable (CybOX)[93], it also brings along significant challenges. The format is severely complex, making it difficult to understand for humans, and a large amount of extensions would need to be created in order for the format to be fully usable for automatic handling of incidents.

On the other hand, an option can be to only transfer unstructured text messages between parties in the cloud supply chain. This would reduce the solution to be a secure "email" system, and thus in accordance with how incident information is mostly exchanged today[94]. The ability to provide free text would allow the parties to exchange any information required, but they would have to agree on a special formatting for the text if planning to support automatic handling of incidents. This would make it easier to implement the solution, and thus reduce initial adoption costs. Notable drawbacks of this approach include fragmentation in message formatting, leading to potential difficulties for humans in interpreting or encoding incident information.

The chosen middle ground is a small base format, with the ability to represent the most common information in a simple way and providing a structured solution for attaching other incident formats such as those mentioned above. This allows for reuse of existing incident formats, specialisation, incremental implementation, and flexibility to support newer formats.

Code 1 shows the content of the JSON file transferred between two IMT compatible instances when exchanging incident information. The structure is valid JSON, but the correct representation of data types has been set aside in favour of descriptive information. When constructing an incident representation in the format from Code 1, *STRING* must be replaced with, e.g., "Data Breach" for the name element.

[90] Danyliw, R; Meijer, J; Demchenko, Y, " The Incident Object Description Exchange Format" at IETF 2007, pp.1-91 available at: https://tools.ietf.org/html/rfc5070
[91] Barnum, Sean, "Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIX™)" 2012, pp. 1-20
[92] Cain, P; Jevans, D, "Extensions to the IODEF-Document Class for Reporting Phishing" at IETF 2010, pp.1-51
[93] The MITRE Corporation, "CybOX – Cyber Observable", available at: https://cyboxproject.github.io/
[94] Frøystad, Christian, "Exchange of Security Incident Information in the context of Cloud Services" Minor thesis report, 2014 pp.1-64

```
{
"id": UUID,
"parent":{
"id": UUID,
"provider": STRING,
"endpoint": URI
},
"type":{
"id": UUID,
"name": STRING,
"description": STRING,
"consequence": FLOAT,
},
"language": STRING,
"status": STRING,
"impact": FLOAT,
"summary": STRING,
"description": STRING,
"occurrence_time": ISO 8601,
"detection_time": ISO 8601,
"liaison":{
"name": STRING,
"email": EMAIL,
"phone": STRING,
"address": STRING,
"zip": STRING,
"city": STRING
},
"attachments":[
{
"format": STRING,
"uri": URI
},
],
"custom_fields":[
{
"id": UUID,
"value": STRING,
"type":{
"id": UUID,
"name": STRING,
"description": STRING,
"type": STRING
}
},
],
"tlp":{
"scheme": STRING,
"value": STRING,
"fields":[
{
"field": STRING,
"value": STRING,
},
]
},
"next_update": ISO 8601
}
```

Code 1 The Incident Exchange Format with named data types rather than actual representation of data

Further details about the incident exchange format can be found in the IMT handbook[95].

[95] Note that this handbook forms an internal project document addressing the Specification and API for IMT.

5.5 Incident Exchange API

At some point, the cloud provider experiencing an incident needs to notify its cloud customers, i.e. other providers in the cloud supply chain buying services from the CSP. One approach is to decide which notifications to send a-priori by mutual agreement between provider and customer, where each party makes sure that they exchange the necessary information to fulfil the relevant laws and provide sufficient data for information exchange to be useful.

Another approach could be that the provider decides which notifications to send, without the cloud customer's influence. This could include notifications with a core message like: "We have been breached, but your data was not compromised."

A hybrid, combining the two, would allow the mutual agreement to be created by the provider listing which types of incidents the cloud customer is allowed to access, and the cloud customer subscribing to the incident types he needs. In order to allow the cloud provider to fulfil any legal obligations to notify the cloud customer, he could, when obligated by law, send such notifications whether the cloud customer subscribes to them or not.

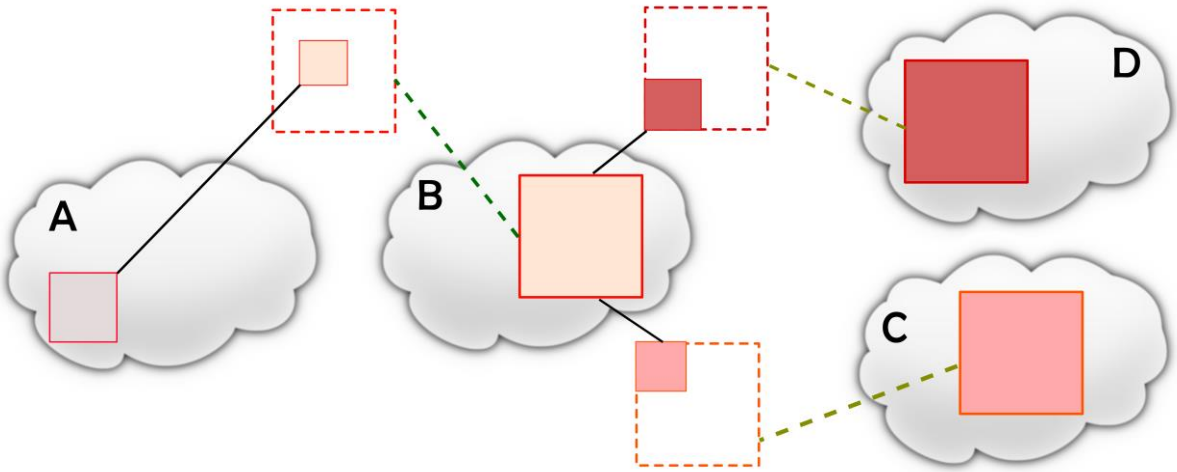


Figure 7: Data flow in supply chain

Figure 7 **Error! Reference source not found.**shows an example of the relationship between cloud providers and services used, and thus provides an example of the amount of unneeded or unwanted incident information a subscriber could receive if the defined triggers are not taken into account. Each cloud represents a service provider. Each coloured square represents the services used by the subscriber. The coloured square inside each stippled square, represents the data or parts of the services actually used by the subscriber. For example, in the case of cloud B, it only uses a fraction of the services offered by cloud C and D. If cloud B was notified about all incidents at C and D, this would include a large amount of unneeded information relating to services not in use by cloud B. Additionally if cloud D has thousands of customers, the overhead of negotiating and defining which incident information to share would become noticeable. Therefore, it is expected to be better to use the hybrid approach, where the subscriber defines what he wants to be notified about and the provider additionally pushes all information required by law to the subscriber by using mandatory notifications that could be defined for each subscriber.

Table 2: Complete REST interface for exchanging incident information

Resource	URI	HTTPS method
Incident types	/incidents/types	GET POST*
Incident type	/incidents/types/{id}	GET POST* DELETE*
Trigger types	/incidents/types/{id}/triggers/types	GET POST*
Trigger type	/triggers/types/{id}	GET POST* DELETE*
Subscriptions	/subscriptions	GET POST
Subscription	/subscriptions/{id}	GET POST DELETE
Subscription incidents	/subscriptions/{id}/incidents	GET POST
Subscription incident	/incidents/{id}	GET POST DELETE
Notification triggers	/incidents/{id}/triggers	GET POST
Notification trigger	/triggers/{id}	GET POST DELETE
Notification validation	/notifications/validate	POST
Provider identity	/identity	GET
Add subscriber	/subscriber	POST

* only the owner of the IMT instance can use these methods

Further details about the API can be found in the IMT handbook[96].

[96] n.95

6 The Remediation and Redress Tool (RRT)

The Remediation and Redress Tool (RRT) aims to assist cloud subjects in responding to (perceived) incidents in their cloud arrangement, and mitigate the difficulties that cloud subjects are reported to have in accessing judicial or administrative remedies.

6.1 Overview

RRT facilitates cloud subjects in receiving notifications about an exception happened in the cloud, which refers to their data disclosures. It is activated as a result of certain incidents reported by IMT to the relevant stakeholders or can be invoked by the user on the basis of information coming from other sources, such as a request for data disclosure from the Data Track (DT).

If the tool is triggered by an incident raised by IMT, then RRT knows what type of incident has occurred and what possible actions can be taken. Then, it will guide the user through these actions, which include getting targeted guidance, performing a number of corrective measures aiming at the mitigation of the incident, and obtaining an account to be used in case the subject decides, as a final measure, to seek judicial redress. In case the tool is consulted by the user without being triggered by IMT, it will engage in a dialogue with the user to establish their concern and next guide the user through appropriate actions. Where appropriate, the tool will take automatic action to communicate requests/complaints etc.

We underline that the tool is not aimed at providing legal advice strictu sensu, nor at automating or incentivizing any part of a possible legal action.

6.2 RRT functional specifications

As already elaborated above, RRT complements the incident management and remediation functional category of the A4Cloud tools to serve the need of cloud subjects to be notified about incidents that occurred in the cloud environment and affect the disclosure of their personal data to various cloud applications. In that respect, the tool is designed as a client side tool, which consumes the results of the server side logic of other accountability tools and responds to perceived incidents with the aim to mitigate risks, such as the loss of privacy, and support the implementation of corrective accountability mechanisms.

RRT is assigned with the following set of functionalities:

- Receive the incidents reported by IMT and targeted to data subjects, functioning together with IMT as a complete set of notification tools;
- Allow cloud subjects to download an account of the incident;
- Provide cloud subjects with a list of immediate corrective measures for a reported incident;
- Provide the cloud subject with targeted guidance concerning the incident reported and its legal consequences.

We elaborate more on the purpose of these functionalities to allow the reader to understand the rationale for implementing them as part of the RRT workflow.

Notification requirements are on the rise in the EU. The General Data Protection Regulation (GDPR), which will be uniformly applicable across all EU countries, foresees an obligation to notify both DPAs and cloud subjects of data breaches.[97] The tool allows data subjects receive any kind of incident, enabling cloud providers to easily demonstrate their compliance with the European data protection regulatory framework. Since the notification message is not limited to data breaches, but covers potentially more types of incidents (like an unavailability of a service), it allows cloud providers show higher accountability standards, by reporting more than the minimum requirements set in national legislations, thus differentiating themselves in the market.

[97] See the draft compromise adopted by the LIBE Committee on 17 December 2015, articles 31 and 32.

As far as data breaches are concerned, moreover, our intention would be to have the relevant reports sent e.g. to a dedicated repository or mailbox accessible by the concerned DPA, in order to anticipate what is foreseen by art. 31 of the GDPR proposal adopted by the LIBE Committee of the EU Parliament on 17 Dec 2015, according to which DPAs would have to be notified of data breaches.

The acquisition of an account for cloud subjects enables them have some degree of evidence[98] before seeking legal advice or lodging a complaint to the national DPA. As mentioned in section three, The burden of proof from national legislation is often a major obstacle in accessing the data protection-related remedies. What would be beneficial for data subjects is the possibility to be able to download both a human-readable, digitally signed and time-stamped file in a commonly used format (e.g., a .pdf file), and if feasible the relevant data in the "raw" form as logged by the tools reporting to IMT and stored in AAS as evidence. This would provide the user with an account of the incident appropriate to the audience of reference (e.g. a DPA receiving additional material in support of the cloud subject's complaint, or the lawyer tasked with representing the cloud subject), which would arguably mitigate the costs and difficulties associated with gathering evidence of an accident happening in a cloud environment.

Through RRT, the cloud subject should be able to access a list of immediate corrective measures (ideally directly and immediately actionable, without having the tool redirect the user to other pages) to address the incident notified (e.g. change login credentials, delete data, cancel or freeze/block account, remove payment details, contact customer service, etc.) depending on the cloud service's characteristics and the type of the incident notified. Obtaining legal redress is often a lengthy and complex process, even in cases that cloud providers have adopted the necessary precautionary measures, and there is generally the need to address incidents directly and immediately. While this, in some cases, might be trivial for the more savvy users, others would benefit from a way of doing so through the RRT accountability tool.

When incidents occur and are reported to cloud subjects, there is always a gap from the time that the data subject is notified of the incident up to the time that a legal representative undertakes the situation. An early guidance on the incident reported from a legal perspective is therefore a required function that should be made available from RRT. However, this needs to be generic enough, so that it is not considered as legal advice. On the one hand, the complexity and natural asymmetry of the cloud environment make it hard for end-users to understand which incidents can result in a violation of the applicable legal norms, and whether those norms have been actually violated or not; on the other hand, for both feasibility and liability[99] reasons, it would be better to avoid issuing opinions that can be framed as professional and/or formal advice, concerning the substance or procedure of the law with regards to a particular and specific factual situation. Aside from providing guidance to users, this functionality could also be useful for individuals' and SMEs' counsels; as highlighted by FRA, the lack of expertise in privacy and data protection matters by legal professionals is one of the major causes hindering access to data protection remedies in the EU.

6.3 The high level architecture of RRT

Figure 8 shows the high level view of the RRT architecture, which is designed to implement the functionalities in the section above. RRT gets as input the incident data (in the form of a type of incident, a time and a scope), some user related information (e.g., about the location, the allocated roles, the contact details, etc.), any contextual information that can assist in making proper decisions on remediation and the incident response model retrieved from a knowledge base. The latter may include a list of actions for the cloud subjects that relate to the type of generated incident.

The main components of the RRT architecture, as shown in Figure 8, are:

[98] The Italian Legislative Decree no. 196 of 30 June 2003, for instance, requires in this respect that plaintiffs lodging a complaint to "refer, with as many details as possible, to the facts and circumstances on which it is grounded, the allegedly infringed provisions and the remedies sought as well as to the identification data concerning data controller, data processor, if available, and claimant".

[99] An extensive discussion on liability regarding the A4Cloud Tools is included in Chris Reed, Asma Vranaki, Lorna Cropper, Petra Zabudkova & Lorenzo Dalla Corte, ''D-4.12: A4Cloud Tools, Liability and Compliance Investigations'' to be published on www.a4cloud.eu.

- The Response Listener, which listens for new notifications coming from the incident management process.
- The Response Logger, which logs the information about the actions decided and taken by the data subjects.
- The Dialogue Manager, which is the graphical component of RRT and enables for the interaction with the data subject in order to conclude on the appropriate remediation or redress action.
- The Response Generator, which processes the received incidents to propose appropriate actions.
- The Remediation Queue Sender, which handles the processing of the selected response actions.

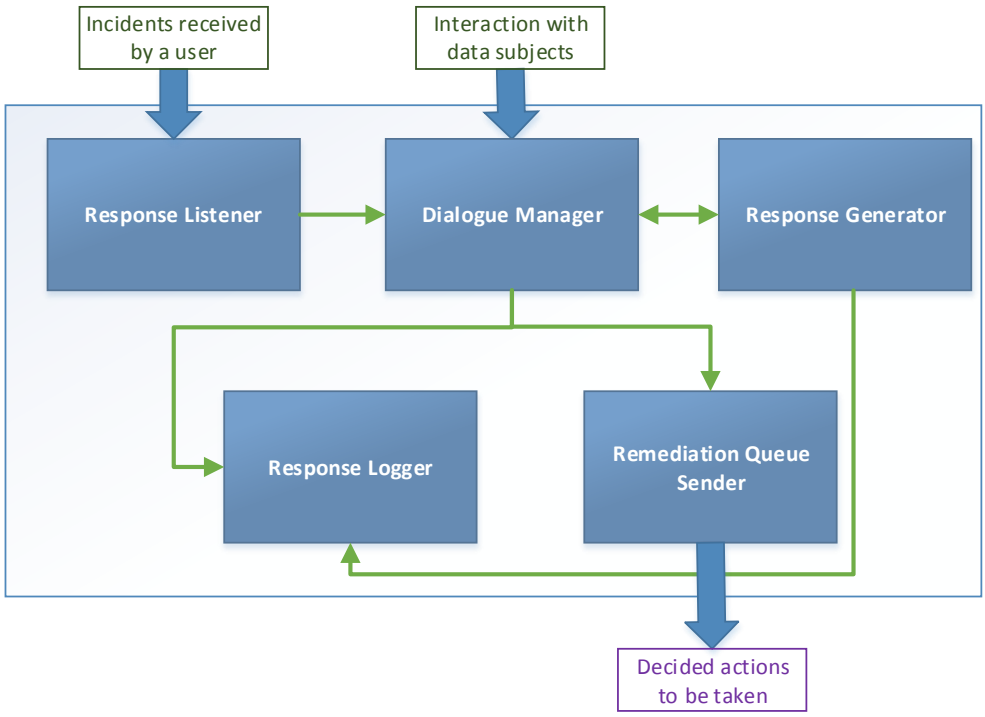


Figure 8: The high level architecture of the Remediation and Redress Tool.

Thus, RRT integrates mechanisms for analysing the incoming incident information and providing explanations, mapping the user concern or incident to the knowledge base, synthesizing the response and producing the relevant response. The output of the tool is a list of potential remediation and/or redress actions, including pre-completed (standard) forms for complaints/request etc. It also educates the respective stakeholders on incidents and potential actions and procedures to be taken.

6.4 Current implementation aspects

In the current prototype implementation delivered in the context of the A4Cloud project, RRT is developed as a client side Web application, which integrates with other cloud subject controls tools. This is the case of Data Track (DT). As such, RRT is offered as a User Interface container of the DT implementation, however it is functionally decoupled from it. The main reason is that RRT targets cloud subjects and the functionalities offered by this tool are agnostic to the particular process of any cloud application used by these cloud subjects to disclose their personal data with cloud providers. The same applies for DT, which enables cloud subjects to access their disclosures in the cloud in a transparent way. In that respect, A4Cloud integrates both DT and RRT in a single installation package for the cloud subjects.

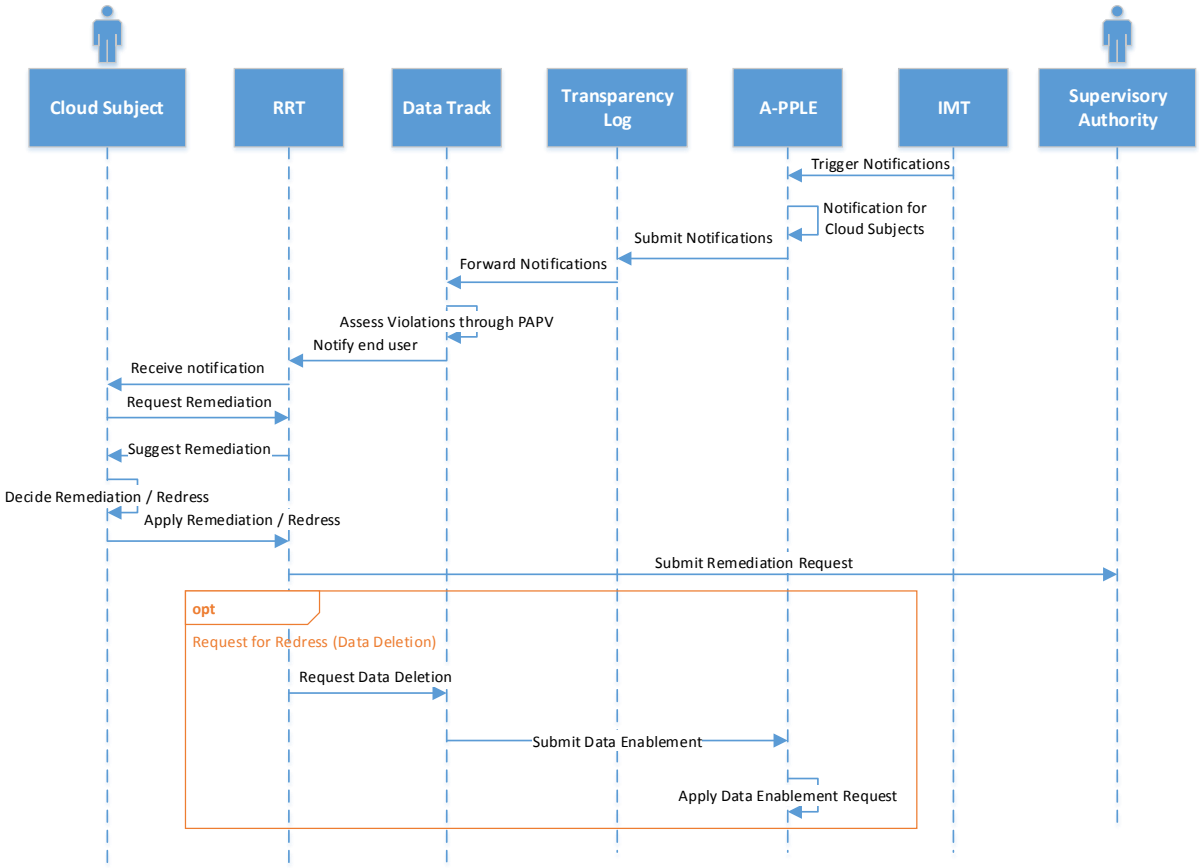
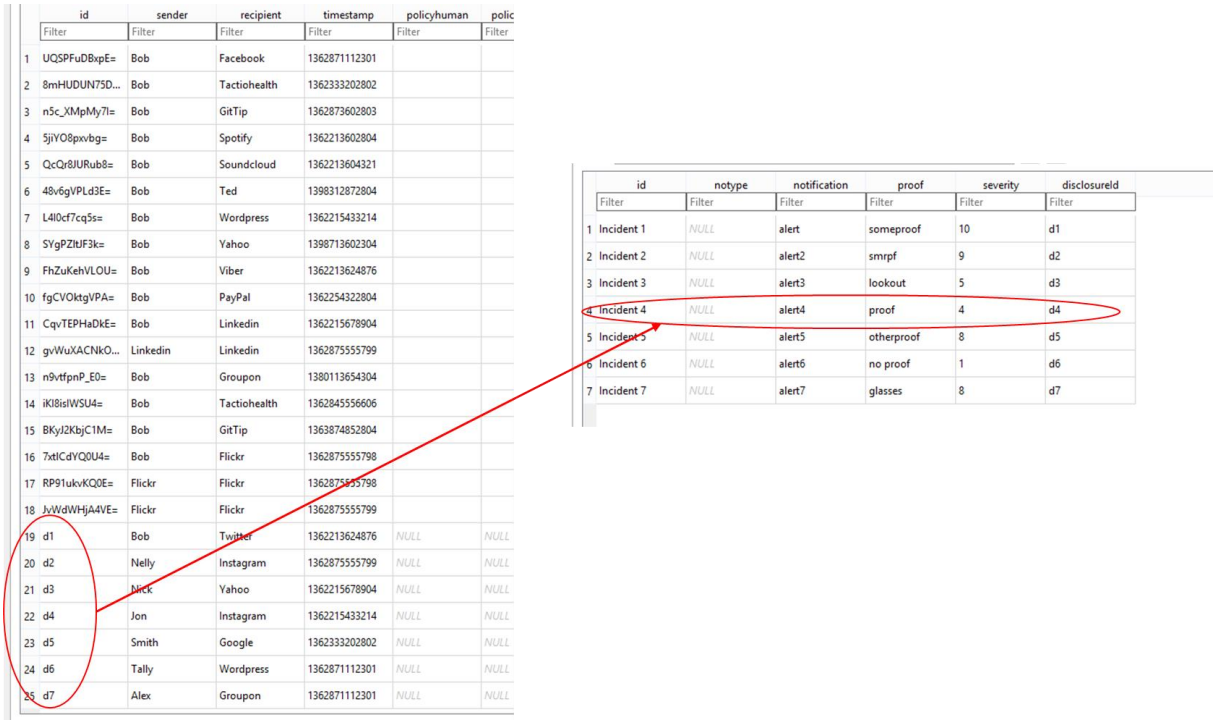


Figure 9: The remediation and redress interaction diagram supported in A4Cloud

Figure 9 shows the interactions between the different accountability tools and the relevant cloud stakeholders. As shown there, the process starts when IMT has processed an incident (detected by the various accountability tools). This IMT instance refers to the one being installed in the data controller side, which also operates the instance of the policy enforcement engine A-PPLE. The notifications, which have been marked by the IMT operator as suitable ones for being forwarded to the affected data subjects, are communicated to A-PPLE. The latter is responsible for handling these notifications according to the rules part of the A-PPL policy format (this has been already explained in WP:D-3). The policy enforcement engine is aware of the way for reaching data subjects through the A4Cloud specific secure and encrypted communication channel (which is the Transparency Log tool). In that way, the notifications faced towards a specific data subject are securely maintained in the respective TL channel.

Once a cloud subject launches their DT instance locally in the Web browser, the notifications from the TL are propagated to the internal datatrack.db database of DT. In this case, a dedicated database table has been created to maintain the incidents for this cloud subject. These incidents are associated with a particular disclosure action of this cloud subject with the data controller of reference. This association is better reflected in the example shown in Figure 10. An incident is registered to a data disclosure action, which in turn refers to the disclosure of the senders' personal data to the recipient data controller.



	id	sender	recipient	timestamp	policyhuman	polic
1	UQSPFuDBxpE=	Bob	Facebook	1362871112301		
2	8mHUDUN75D...	Bob	Tactiohealth	1362333202802		
3	n5c_XMpMy7I=	Bob	GitTip	1362873602803		
4	5jiYO8pxvbg=	Bob	Spotify	1362213602804		
5	QcQr8JURub8=	Bob	Soundcloud	1362213604321		
6	48v6gVPLd3E=	Bob	Ted	1398312872804		
7	L4l0cf7cq5s=	Bob	Wordpress	1362215433214		
8	SYgPZItJF3k=	Bob	Yahoo	1398713602304		
9	FhZuKehVLOU=	Bob	Viber	1362213624876		
10	fgCVOktgVPA=	Bob	PayPal	1362254322804		
11	CqvTEPHaDkE=	Bob	Linkedin	1362215678904		
12	gvWuXACNkO...	Linkedin	Linkedin	1362875555799		
13	n9vtfpnP_E0=	Bob	Groupon	1380113654304		
14	iKI8islWSU4=	Bob	Tactiohealth	1362845556606		
15	BKyJ2KbjC1M=	Bob	GitTip	1363874852804		
16	7xtlCdYQ0U4=	Bob	Flickr	1362875555798		
17	RP91ukvKQ0E=	Flickr	Flickr	1362875535798		
18	JvWdWHjA4VE=	Flickr	Flickr	1362875555799		
19	d1	Bob	Twitter	1362213624876	NULL	NULL
20	d2	Nelly	Instagram	1362875555799	NULL	NULL
21	d3	Nick	Yahoo	1362215678904	NULL	NULL
22	d4	Jon	Instagram	1362215433214	NULL	NULL
23	d5	Smith	Google	1362333202802	NULL	NULL
24	d6	Tally	Wordpress	1362871112301	NULL	NULL
25	d7	Alex	Groupon	1362871112301	NULL	NULL

	id	notype	notification	proof	severity	disclosureId
1	Incident 1	NULL	alert	someproof	10	d1
2	Incident 2	NULL	alert2	smrpf	9	d2
3	Incident 3	NULL	alert3	lookout	5	d3
4	Incident 4	NULL	alert4	proof	4	d4
5	Incident 5	NULL	alert5	otherproof	8	d5
6	Incident 6	NULL	alert6	no proof	1	d6
7	Incident 7	NULL	alert7	glasses	8	d7

Figure 10: An example of the Data Track database hosting the incident information.

The incident records consist of information, which can be used by RRT to easily present these incidents to the cloud subjects. When a new incident enters the DT database, RRT retrieves it and displays a preview of the incident information in a dedicated widget, which is made available in the menu bar of DT (see Figure 11). Through this widget, the cloud subject can navigate through the RRT UI and browse the whole set of functionalities for remediation and redress.

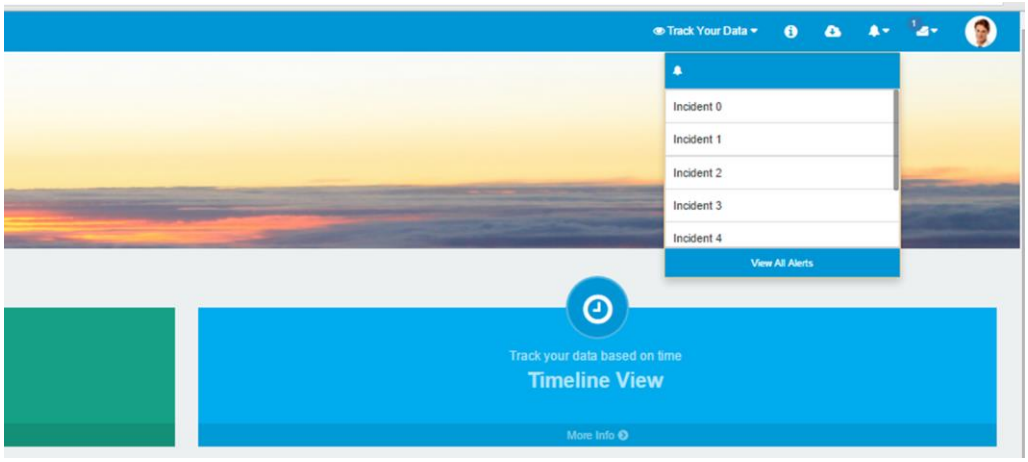


Figure 11: Populating incidents in the widget of Data Track UI.

A screenshot of the RRT view is shown in Figure 12. The UI is split into three main parts. On the top left part, the list of incidents is presented. Currently, this view shows only the incident id, but in the future the tool will be further developed to present more fields from the incidents tables (of Figure 10), like the incident description and the severity level. The top right hand side part of the RRT UI is enabled once the data subject clicks on one of the incidents in the incidents' list on the left. This view presents the details of an incident, like the timestamp of the incident occurred, detected and notified to the cloud subject, the affected disclosure details, the respective data controller reported the incident and a link to the applied policy. Again, this is the current view of the incident information window, which can be expanded to include more information from the incident characteristics.

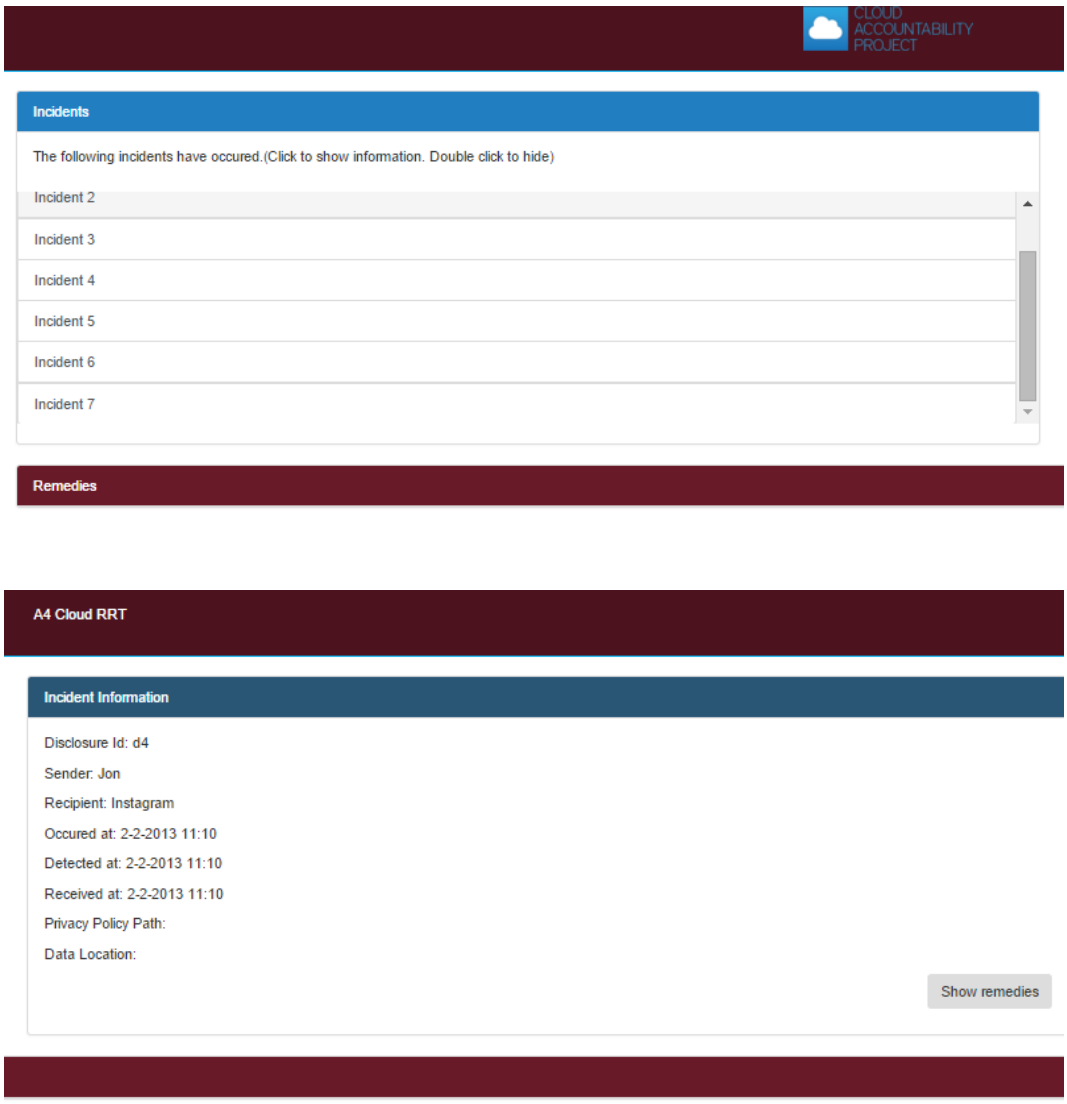


Figure 12: Screenshot of the RRT UI

Finally, the bottom part of the RRT UI includes the remedies view, which relates to a specific incident selected from the previous view. Thus, the remedies view is enabled by clicking the "show remedies" button in the incident information window. This view is presented in Figure 13. As shown there, the remedies views lists the available proposed actions towards remediation and redress, by offering the following information to the data subjects:

- A title and description to the proposed action to enable the cloud subjects understand the scope of the suggested remedy to be applied.
- An "Action" area, which includes actionable buttons for the selection of the proposed actions.

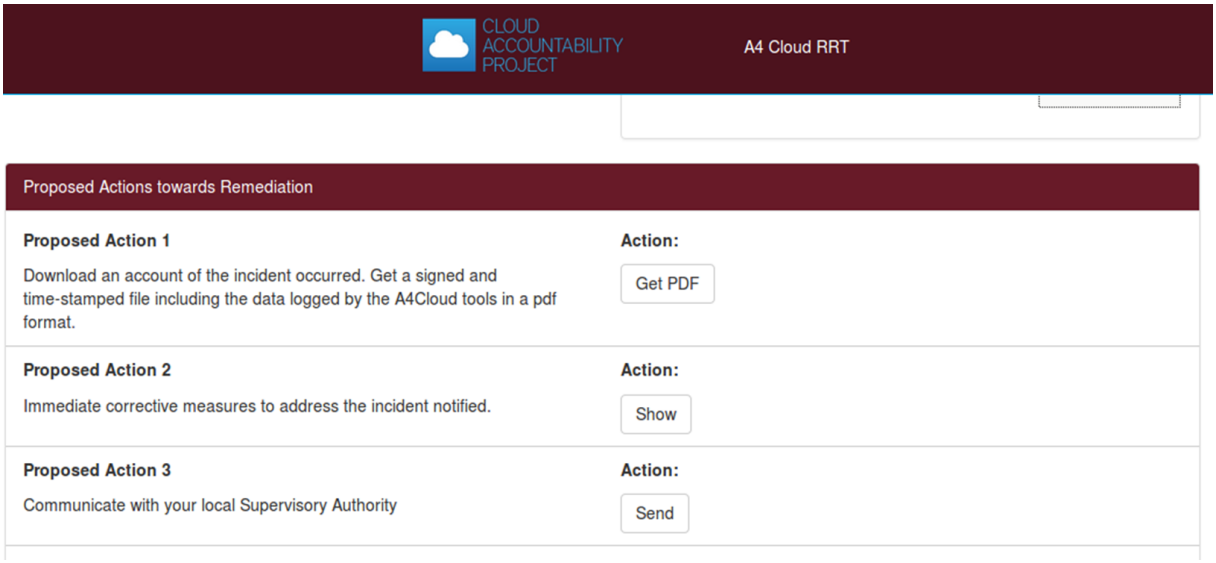
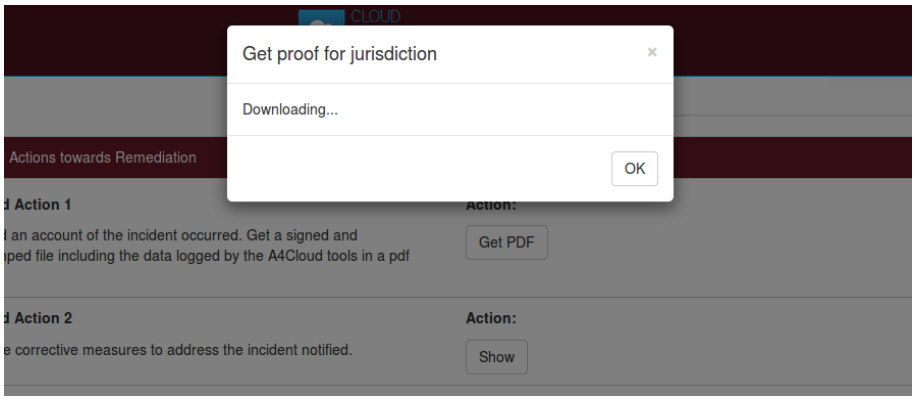


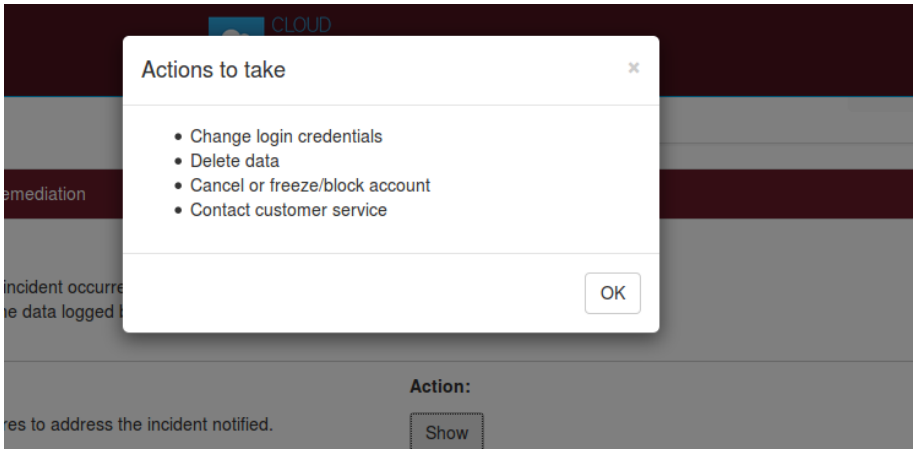
Figure 13: Screenshot of the RRT remedies window

The proposed actions may refer to:

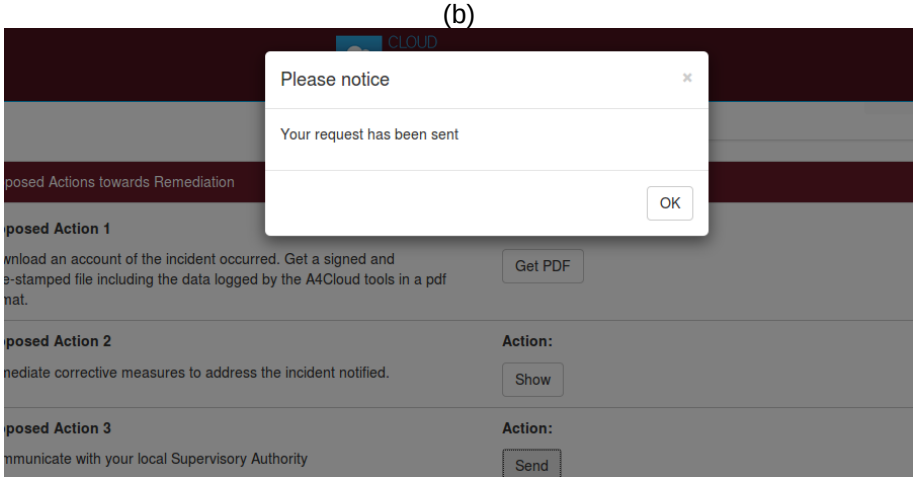
- Download a digitally signed and stamped PDF of the account relevant to the reported incident (see Figure 14 a), which can subsequently be used by cloud data subjects for jurisdiction purposes. This PDF file can be requested from the cloud providers, through a dedicated Web service.
- A list of corrective measures to be manually adopted by the cloud subject through accessing the cloud application, referred to by the incident (see Figure 14b). In this case, and depending on the selected corrective action, RRT has to communicate with the DT and request the implementation of the selected actions on the data disclosed in the respective data controller. Such actions (i.e. data deletion, account deletion) are to be implemented mainly through A-PPLE, as shown in Figure 9.
- Communication with the local Supervisory Authority by composing the incident details received from the cloud into a form (e.g. email, etc.) that can be used by the data subject to establish this contact (Figure 14c). This is an action that requires the offline interaction of the cloud subject with the relevant cloud stakeholder to submit the output received from RRT, as shown in Figure 9.



(a)



(b)



(c)

Figure 14: Example of proposed actions for remediation from the RRT remedies view

Currently, the remediation and redress actions cover a subset of the remedies described in section three, but the RRT implementation is a proof of concept prototype and further implementation is planned for the future.

RRT has been implemented as an HTML Web application, which uses JavaScript for developing backend logic and access to the datatrack database.

7 IMT and RRT as accountability tools

At a high level, we classify accountability functions as being preventive, detective and corrective. As explained in section one, preventive functions focus on mitigating the occurrence of an unauthorised action. Detective functions refer to the identification of the occurrence of an unauthorised action. The current section describes the components of the A4Cloud toolset that implement corrective functions: those used to fix an undesired result that has already occurred and has been detected by the detective functions. These components focus on managing incidents, providing notifications and facilitating redress. Thus, in this section, we discuss the roles of IMT and RRT both within the A4Cloud toolset and in other environments.

7.1 IMT and RRT as accountability tools in the cloud environment and other future Internet services

Independently of the A4Cloud toolset, accountable cloud providers follow the general accountability life cycle, displayed in Figure 15, which is directly derived from the Cloud Accountability Reference Architecture document [100].

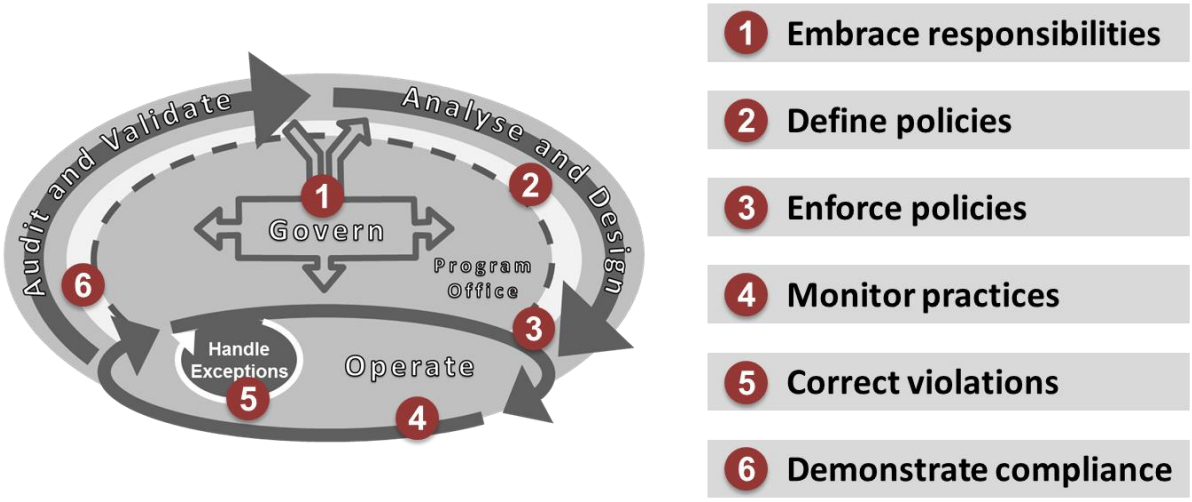


Figure 15: Accountability Lifecycle and Practices

In this lifecycle, which consists of various phases, the sub-cycle “5 Correct violations/handle exceptions” comprises activities, which relate to exception handling procedures. It is a sub-cycle because it interrupts the normal operational cycle and a particular exception/incident should be handled before normal operations (based on what happened prior to the incident) can continue. The sub-cycle includes all processes for the handling of complaints and breaches related to obligations following from the accountability framework (which derive from law, contract, social norms, etc.). Processes need to be in place to take corrective action and/or provide a remedy for any party harmed in case of failure to comply with its governing norms.

The expected behaviour from organisations in these phases of the cycle is to:

- Receive, handle, track, and respond to complaints and information requests from stakeholders in a timely manner as required by internal policies or legal requirements. Have a Frequently Asked Questions (FAQ) to anticipate the most frequent information requests.
- Create a classification for requests and complaints. Define standard procedures for the handling of requests in each of the classes. Have defined escalation procedures.

[100] Cloud Accountability Reference Architecture – Preliminary Release, available online at www.a4cloud.eu.

- Ensure the organisation is ready to handle incidents related to obligations for which it is accountable (incident response). Ensure Preparedness for handling exceptional events (processes and procedures, allocate responsibility, deploy the staff, define a contingency plan, get retainer for external resources (e.g. forensics expertise), insure against risks, define metrics then track and report performance, test the system based on simulated incidents.

The basic functionality of IMT and RRT partly support the goals expressed above. The current prototypes demonstrated in A4Cloud needed to introduce some level of integration and dependency with respect to the A4Cloud toolset. However, it would not take considerable effort to adapt them to other realities.

More specifically, IMT supports the implementation of two relevant accountability support services and processes, namely the incident management and the notification. In the incident management case, IMT receives those incidents that are raised as a result of the analysis of machine-generated logs and evidence records from the various detective accountability tools as well as manual triggers. In the case of the A4Cloud project prototype implementation, the automatically detected incidents are raised by the DTMT, the AAS, and the A-PPLE tools (see Figure 16).

- DTMT is used by IaaS Cloud Providers in their cloud environment to log network traffic and raise incidents in case of data transfers,
- AAS is used by all cloud deployment types (IaaS, PaaS and SaaS) providers to raise incidents related to data use or retention, as well as security breaches and encryption leakages.
- A-PPLE is used by cloud providers to produce logs on the decisions made by the policy enforcement engine with respect to data access, use and retention actions. This tool can subsequently raise incidents on excessive authorised requests.

All these tools have a significant contribution to the monitoring of the cloud status and operations, as well as they develop or collect evidence records from the various protocol stack operations and are able to raise specific notification alerts to the IMT tool.
IMT also enables the registration of incidents that are manually detected by the respective IMT operations, such as IT security managers or privacy officers, who are responsible for assessing the status of the runtime operation of their business with respect to established and agreed contracts and policies. Thus, IMT facilitates exception handling both through an automatic detection of potential policy violations and security breaches or via manual registration of system anomalies and misbehaviours after an end-user assessment.

Further to the incident management service process, IMT executes notification operations that enable the communication of verified incidents to other cloud providers, or cloud customers and cloud subjects. The communication of the incidents is in the form of notification reports, which describe the type of the detected incidents, the occurrence timestamp and other incident specific information, which can support proper assessment of the incident from the recipients.

RRT, in turn, serves the requirements and functions of the same accountability lifecycle phase 5 for handling exceptions and correcting violations. This tool refers to the remediation and redress actions and it can be triggered as a response to the notification accountability support service or even when a cloud provider fails to correctly demonstrate compliance with the legal framework and/or the agreed accountability policies. RRT assists cloud end users in responding to real or perceived data handling incidents, either by guiding them in inquiring about capitalising the provisions of an already agreed insurance (this is not implemented at this version of the A4Cloud tools) and compiling claims or by supporting the actual implementation of redress actions.

Figure 17 summarises the set of cloud stakeholders that are intended to be the users of the IMT and RRT tools in the implementation of the accountability lifecycle.

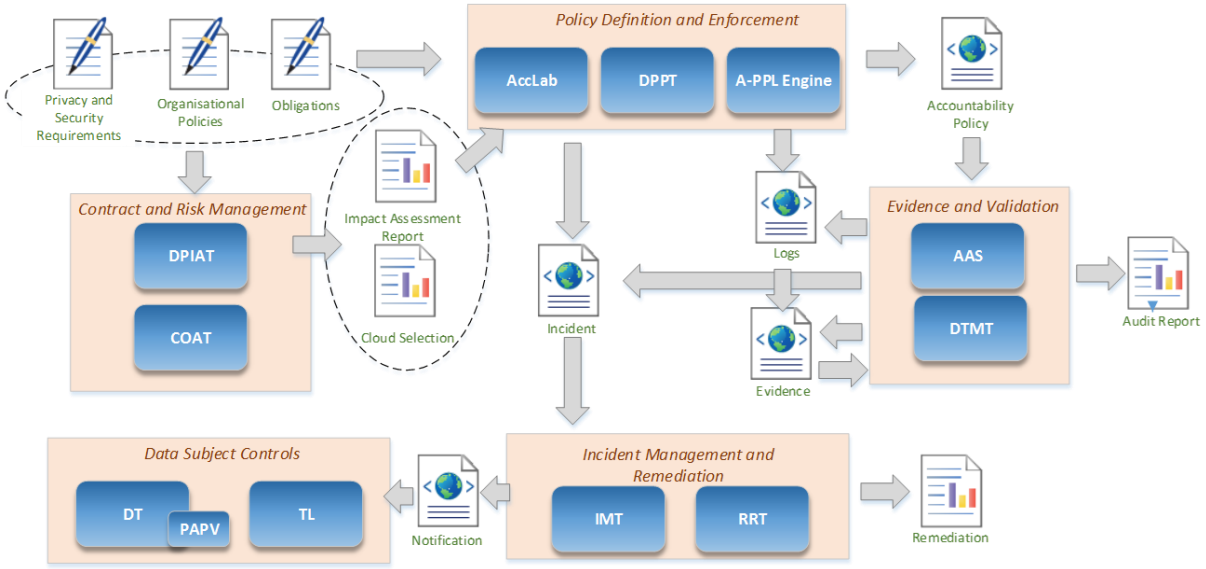


Figure 16: The position of IMT and RRT in the tool interaction diagram of A4Cloud

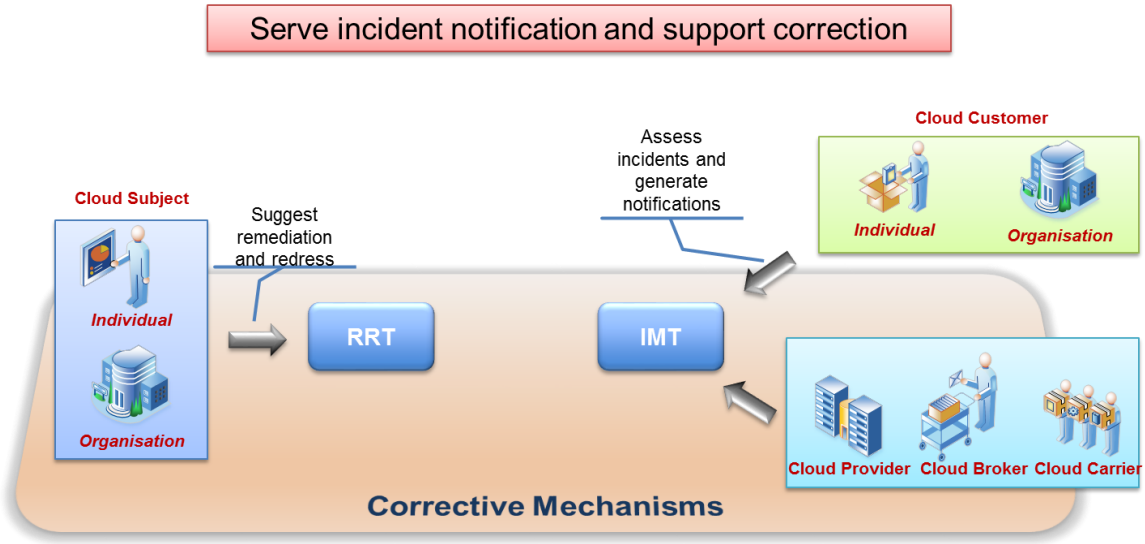


Figure 17: Overview of the incident management and remediation tools

An extended interaction diagram between the A4Cloud tools is presented in Figure 18, which is adopted from WP:D-2, as shown there, IMT sits in the centre of the notification process and governs the incidents that should be notified to cloud providers, customers and data subjects, according to the accountability policies enforced by A-PPLE. RRT is the recipient of the incident notifications, which is implemented as part of DT.

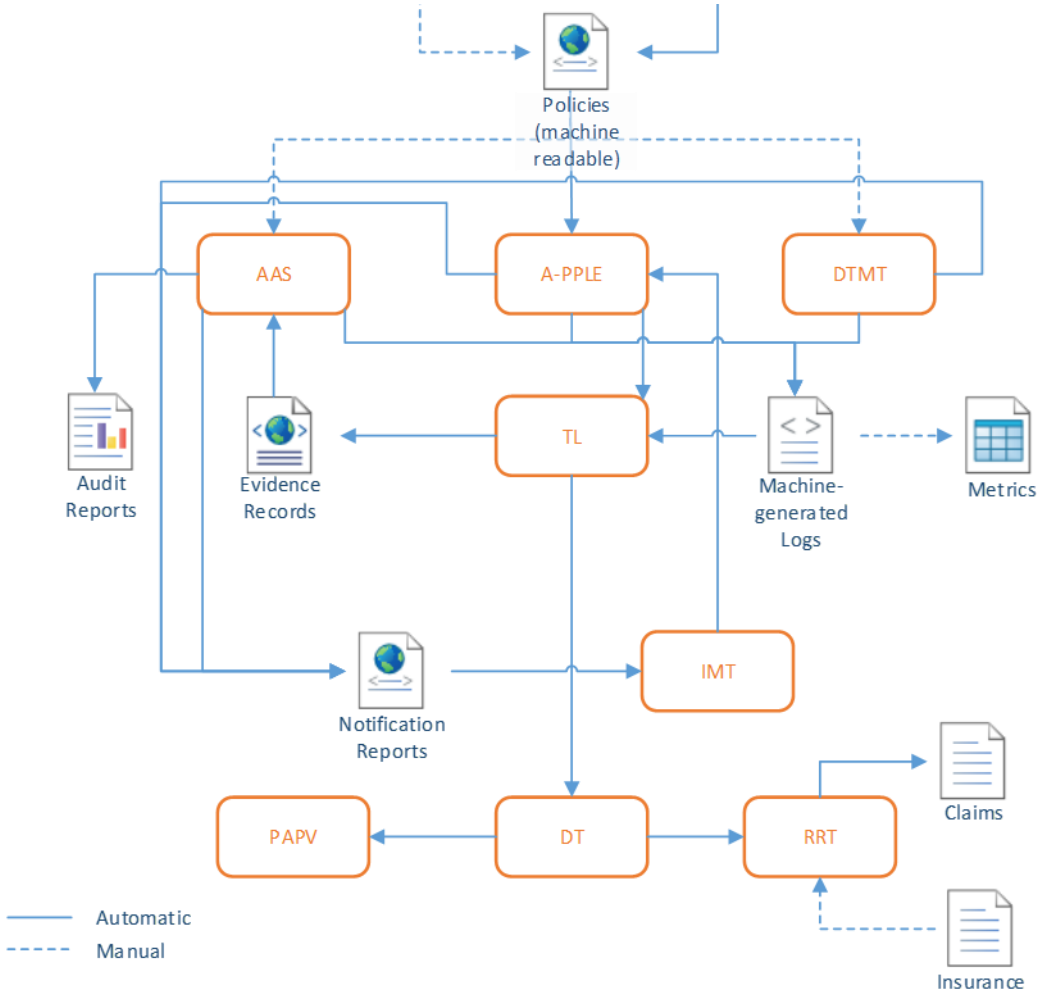


Figure 18: Detailed interaction diagram among the A4Cloud tools

8 Conclusions

Achieving accountability in the cloud ecosystem is important and includes being transparent and accountable regarding incidents. Incidents can never be completely prevented and therefore procedures need to be in place to remedy the consequences. Informing relevant stakeholders about incidents and what to do once they occur is part of good stewardship of data. Providing transparency about incidents provides a significant challenge as we discovered while developing the IMT and RRT tools. The realm is full of trade-offs. For instance, assuming transparency implies delivering information in an understandable manner also regarding highly technical issues. This requires choices to be made regarding level of information in relation to audience (lay-people versus regulators versus service operators). Or, if all incidents need to be reported, then notifying cloud subjects every time an incident occurs – including, for example, attempting to move a virtual machine, which happens often in cloud environments —would lead to incident fatigue; people would no longer care about the incidents. Overwhelming non expert users with big amounts of technical information would then miss its purpose.

Another issue presents itself in the remediation stage. Guiding cloud subjects through possible remedial options by providing them with all technical evidence on the same screen at once surely would count as being transparent. However, in reality, this could confuse and overwhelm lay people acting in their capacity as cloud subjects and, therefore, potentially hamper their decisions to pursue remedies. One solution to this problem is to categorize the information provided through RRT and provide it gradually and upon end-users' requests. Moreover, the choice to introduce "remediability" — instead of remediation—as an accountability attribute in the A4Cloud project[101] is further supported by the fact that technical failures can be addressed through appropriate corrective actions but the harms suffered as a consequence of data protection breaches cannot always be adequately remedied by monetary damages.

The research reported on in this deliverable shows that RRT can be a future-proof technical tool. Incident management tools will develop and increase in sophistication. The logic of such tools, guiding individuals through clear and concrete steps and navigating through the possible procedures or other legal actions s/he might take, remains valid. This would also be true for areas outside the domain of data protection, for example, in applications related to consumer protection law. IMT and RRT provide a general framework to cope with incident management provided there are triggers (automatic and manual) and clear actions to be taken.

Despite the prospect of IMT/RRT there are business and legal considerations that affect the adoptability of the tools in practice. For instance, although accountability could be a market differentiator, it is questionable whether cloud providers would adopt a tool such as IMT, which in combination with the client side RRT would help their customers (and their users/customers) to take action for violations of contractual and regulatory obligations at this moment in time. On the other hand, any responsible organisation provides their customers with (electronic) complaints forms that do the same thing. For instance, the Dutch railroads (NS) allow their customers to file claims in case of delays (more than 30 mins) online that lead to financial compensation within a few weeks. The scale at which this is being used by train travellers may be orders of magnitude smaller than cloud based incidents (although the damages for individuals in these cases may be much smaller than in the NS case). In any case, it remains to be seen in the context of project research[102] on the socio-economic impact assessment investigating whether cloud providers would be willing to adopt these tools on a voluntary basis.

Nevertheless, in the event, of a personal data breach, for example, IMT and RRT could assist CSPs in proving supervisory authority their efforts to do the "right thing", or even detecting incidents and taking measures to mitigate the associated harms, therefore reducing the possibility of a fine. In addition, IMT would allow cloud providers to potentially demonstrate that the incident happened in another link of the cloud supply chain, thus, putting the responsibility for the incident with another actor of the supply chain. It is also possible that the new General Data Protection Regulation provides a regulatory push in adopting IMT/RRT like technologies. Either through the privacy-by-design provisions (art. 23), the breach notification provisions (art. 31 and 32), or just through the general accountability provision (art.22). To what extent reporting incidents will become mandatory, and to whom, us unclear at the moment of writing this deliverable, but will be clearer in 2016.

[101] n 1.
[102] WP A-4.1 Socio-economic impact assessment

Overall, incident response, including the implementation of corrective actions, is a complex issue that cannot be solved merely by employing technical solutions. On the contrary, as it is the case for accountability in general, effective incident response follows from embedding mechanisms and practices within organizations. NIST illustrates this clearly by pointing out the dependencies within organizations and the series of departments that need to be involved in incident handling: "Every incident response team relies on the expertise, judgment, and abilities of others"[103]. The need for cooperation is even more imperative in the cloud, since multiple departments within a single organization need to co-operate amongst themselves, but also with the departments of other organizations across the supply chain. Furthermore, our research reveals that the incidents detected should generate notifications to the "appropriate'' employees, who are then to decide whether a certain incident should result in notification to the competent authorities and the affected individuals.

Finally, it is important to note that the role of incident handling is crucial even outside the domain of cloud computing. Indeed, technologies like "Big Data" and the "Internet of things" that allow for large scale processing of personal information increase the economic and social impact of potential incidents. It is, therefore, up to decision makers to decide how high the issue of digital security will rank in the policy discourse and take necessary action.

[103] National Institute of Standards and Technology, Special Publication 800-61 Revision 2 Natl. Inst. Stand. Technol. Spec. Publ. 800-61 Revision 2, 79 pages (Aug. 2012) CODEN: NSPUE2

9 References

Article 29 Working Party, Opinion 05/2012 on Cloud Computing WP 196, adopted on the 1st of July 2012

Barnum, Sean, "Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIX™)" 2012

Cain, P; Jevans, D, "Extensions to the IODEF-Document Class for Reporting Phishing" at IETF 2010, pp.1-51

Christopher Dabrowski, Kevin L. Mills: VM Leakage and Orphan Control in Open-Source Clouds. IEEE CloudCom 2011: 554-559

Christopher Kuner, Transborder Data Flows and Data Privacy Law, Oxford University Press, 2013

Cichonski, Paul; Millar, Tom; Grance, Tim; Scarfone, Karen, "Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology, 800-61. Revision 2", 2012

Cloud Accountability Reference Architecture – Preliminary Release, available online at www.a4cloud.eu.

Danyliw, R; Meijer, J; Demchenko, Y, " The Incident Object Description Exchange Format" at IETF 2007, pp.1-91, available at : https://tools.ietf.org/html/rfc5070

De Oliveira A.S et all, ''D:C-6.1: Risk and trust models for accountability in the cloud'', available at: http://www.a4cloud.eu/sites/default/files/D36.1%20Risk%20and%20trust%20models%20for%20accountability%20in%20the%20cloud.pdf

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178/1, 17 July 2000.

European Agency for Fundamental Rights (FRA), Access to data protection remedies in EU Member States, 2013

European Commission, 'Proposal for a 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)' COM 2012 (011) final

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data', OJ L 281, 23 November 1995.

European Parliament, Cloud computing Study, section 5.2.3, available at http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO_ET(2012)475104_EN.pdf

Frøystad, Christian, "Exchange of Security Incident Information in the context of Cloud Services" Minor thesis report, 2014

Geoffrey C. Hazard Jr, "Discovery and the Role of the Judge in Civil Law Jurisdictions" (1997-8) 73 Notre Dame LR 1017.

Hassan Takabi, James B. D. Joshi, Gail-Joon Ahn: Security and Privacy Challenges in Cloud Computing Environments. IEEE Security & Privacy 8(6): 24-31 (2010)

Information Commissioner's guidance about the issue of monetary penalties prepared and issued under section 55C (1) of the Data Protection Act 1998 (ICO 2015), https://ico.org.uk/media/for-organisations/documents/1043720/ico-guidance-on-monetary-penalties.pdf.

Jaatun, Martin Gilje; Tøndel, Inger Anne, "How Much Cloud Can You Handle?," in *Availability, Reliability and Security (ARES), 2015 10th Int. Conference on*, pp.467-473, 24-27 Aug. 2015 available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7299953&isnumber=7299862

Meiko Jensen, Jörg Schwenk, Nils Gruschka, Luigi Lo Iacono: On Technical Security Issues in Cloud Computing. IEEE CLOUD 2009: 109-116

OECD (2015), Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/9789264245471-en

Siani Pearson, "Accountability in Cloud Service Provision Ecosystems'' Secure IT Systems, 19th Nordic Conference, NordSec 2014, Tromsø, Norway, October 15-17, 2014, Proceedings, ed. Springer

Siani Pearson, Azzedine Benameur: Privacy, Security and Trust Issues Arising from Cloud Computing. CloudCom 2010: 693-702

Schneier, Bruce, "The Future of Incident Response" in *Security & Privacy, IEEE*, 2014, volume 12, pp.95-96, available at: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=6924685

Tetley, William. "Mixed Jurisdictions: Common Law v. Civil Law (Codified and Uncodified)." *La. L. Rev.* 60 (1999): 677

The MITRE Corporation, "CybOX – Cyber Observable" available at: https://cyboxproject.github.io/,

Thomas Ristenpart, Eran Tromer, Hovav Shacham, Stefan Savage: Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. ACM Conference on Computer and Communications Security 2009: 199-212

Tjong Tjin Tai, T.F.E., Op Heij, D.J.B., e Silva, K.K., Skorvanek, I. and Koops, B.J. (2015). Duties of care and diligence against cybercrime, Tilburg University, available at: https://www.gccs2015.com/sites/default/files/documents/Bijlage%202%20-%20Duties%20of%20care%20and%20diligence%20against%20cybercrime%20(1).pdf

Yinqian Zhang, Ari Juels, Michael K. Reiter, Thomas Ristenpart: Cross-VM side channels and their use to extract private keys. ACM Conference on Computer and Communications Security 2012: 305-316

10 Appendices

Appendix 1

Network and Information Security at EU level[104]

On the 7th of February 2013 the European Commission published its "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace[105]" ("the Cybersecurity Strategy") along with a proposal for a Network and Information Security (NIS) Directive.[106] The Directive is a minimum harmonization[107] one, which aims at ensuring a higher level of data security across the whole EU by setting a threshold that national laws must meet, while still having the possibility to exceed the minimum mandatory level.

The proposal represents the EU's first attempt to enact a comprehensive set of cybersecurity related norms that are not restricted to a particular area or regulatory sector. It is a polar shift towards a mandatory framework for cooperation and incident notification, which sharply differentiates itself from the voluntary cooperation, and data breach reporting mechanisms with which the EU is familiar.[108]

Despite the widespread view that cybercrime and the lack of cybersecurity represent a major threat[109] for public safety, economic well-being and national security, the legislative proposals generated a significant amount of concern, both from economic actors and Member States. Some actors indeed worry that this proposed top-down, cross-sectorial, mandatory form of regulation could ultimately hinder European businesses. The imposition of burdensome and static administrative requirements and the increased coefficient of reputational risk all companies bound by mandatory data breach notification requirements would be subject to led the European Parliament – guided by the Internal Market and Consumer Protection (IMCO) Committee – to significantly amend and water down the original NIS Directive proposal. Ultimately, a final parliamentary version was voted on the 13th of March 2014.

Setting the scene

The Cybersecurity Strategy enumerated the priorities of the EU,[110] amongst which NIS naturally assumes a prominent position. The Commission's proposal for a NIS Directive, published along with the Strategy, addresses this priority pursuing a triple order of objectives:[111]

[104] The discussion below is based on the analysis for the internal milestone report: MS:D-4.3 produced in March 2015, under the T:D-4.5: Regulatory update.
[105] European Commission, joint communication to the European Parliament, the council, the European Economic and Social Committee and the Committee of the Regions, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", JOIN (2013) 1 final, Brussels, 7.2.2013.
[106] European Commission, "Proposal for a Directive of The European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union", COM (2013) 48 final, 2013/0027 (COD), Brussels, 7.2.2013.
[107] See Art. 2, Commission's proposal for a NIS Directive. See also European Commission, "Proposed Directive on Network and Information Security – frequently asked questions", Memo, Brussels, 7.2.2013.
[108] "The current situation in the EU, reflecting the purely voluntary approach followed so far, does not provide sufficient protection against NIS incidents and risks across the EU. Existing NIS capabilities and mechanisms are simply insufficient to keep pace with the fast-changing landscape of threats and to ensure a common high level of protection in all the Member States": European Commission, "Proposal for a Directive of The European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union", Ibid., p. 3.
[109] A research conducted on U.S. companies by the Ponemon Institute in 2012, for instance, framed the cost for a single lost or stolen record in the order of $194, the average size of breached records being 28,349 in the sample considered: Ponemon Institute LLC, "2011 Cost of Data Breach Study", March 2012. Another research conducted by PwC U.K. quantified the mean cost of the single most expensive breach in a single year's span: between 15.000 and 30.000 Pounds for a small business and between 110.000 and 250.000 Pounds for a large organization, totalling billions in damages for the whole U.K.'s PLCs: PwC, "Information security breaches survey", PwC U.K., 2012.
[110] Achieving cyber resilience, reducing cybercrime, developing cyber defence policy and capabilities and industrial and technological resources for cyber-security, establishing a coherent international cyberspace policy for the European Union and promoting core EU values: European Commission, "EU Cybersecurity plan to protect open internet and online freedom and opportunity", press release, Brussels, 7.2.2013.
[111] See Art. 1, par. 2, Commission's proposal for a NIS Directive.

1. Having the Member States reach a high[112] level of national information security capabilities "by establishing competent authorities for NIS, setting up Computer Emergency Response Teams (CERTs), and adopting national NIS strategies and national NIS cooperation plans[113]"
2. Stimulating cooperation at a communitarian level "within a network enabling secure and effective coordination, including coordinated information exchange as well as detection and response at EU level […] to counter NIS threats and incidents on the basis of the European NIS cooperation plan.[114]"
3. Mandating operators in critical sectors[115] and public operators to adhere to stringent risk assessment and management practices, adopting appropriate and proportionate security measures and reporting the NIS incidents that are deemed sufficiently serious.

Those objectives reflect on the proposed Directive's structure. The proposal is divided in five chapters, respectively titled "General Provisions", "National Frameworks on Network and Information Security", "Cooperation Between Competent Authorities", "Security of the Networks and Information Systems of Public Administrations and Market Operators" and "final provisions". The Directive contains also two annexes, containing respectively a list of tasks and requirements for CERTs and a (non-exhaustive) list of market operators covered under the scope of the Directive.

As to the first area, which regards future Member States' frameworks for NIS, Article 5 would mandate Member States to adopt a "national NIS strategy,"[116] comprising a "NIS cooperation plan[117]", to be communicated to the Commission within one month from its adoption. Member States, according to the following Article 6, would also have to designate a competent national NIS authority tasked to monitor the Directive's application and contribute to its coherent implementation across the EU. Moreover, Article 7 sanctions Member States to setup a CERT "*responsible for handling incidents and risks according to a well-defined process*" under the supervision of the Authority *ex* Art. 6; the CERT would need to have enough technical, financial and human resources to be effective in responding to incidents as set out in its tasks, and Member States would need to allow it to rely on a secure information-sharing system as set out in Article 9 of the NIS proposed Directive.

The second objective of the NIS Directive – the development of a solid cooperation system between the competent authorities mentioned above – is tackled by its third chapter. Setting up a cooperation network would logically be the first step, and indeed Article 8 states "*the competent authorities and the Commission shall form a network ("cooperation network") to cooperate against risks and incidents affecting network and information systems*". The network's members shall:

(a) Circulate early warnings on risks and incidents in accordance with Article 10;
(b) Ensure a coordinated response in accordance with Article 11;
(c) Publish on a regular basis non-confidential information on on-going early warnings and coordinated response on a common website;
(d) Jointly discuss and assess, at the request of one Member State or of the Commission, one or more national NIS strategies and national NIS cooperation plans referred to in Article 5, within the scope of this Directive.
(e) Jointly discuss and assess, at the request of a Member State or the Commission, the effectiveness of the CERTs, in particular when NIS exercises are performed at Union level;

[112] See Art. 4, Commission's proposal for a NIS Directive.
[113] European Commission, "Proposal for a Directive of The European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union", Ibid, p. 4.
[114] Ibid.
[115] As defined and enumerated by the proposed Directive and its annexes.
[116] The NIS national strategy shall address, as a minimum: The definition of the objectives and priorities of the strategy based on an up-to-date risk and incident analysis; A governance framework to achieve the strategy objectives and priorities, including a clear definition of the roles and responsibilities of the government bodies and the other relevant actors; The identification of the general measures on preparedness, response and recovery, including cooperation mechanisms between the public and private sectors; An indication of the education, awareness raising and training programmes; Research and development plans and a description of how these plans reflect the identified priorities.
[117] The NIS cooperation plan shall address, as a minimum: A risk assessment plan to identify risks and assess the impacts of potential incidents; The definition of the roles and responsibilities of the various actors involved in the implementation of the plan; The definition of cooperation and communication processes ensuring prevention, detection, response, repair and recovery, and modulated according to the alert level; A roadmap for NIS exercises and training to reinforce, validate, and test the plan. Lessons learned to be documented and incorporated into updates to the plan.

(f) Cooperate and exchange information on all relevant matters with the European Cybercrime Center within Europol, and with other relevant European bodies in particular in the fields of data protection, energy, transport, banking, stock exchanges and health;
(g) Exchange information and best practices between themselves and the Commission, and assist each other in building capacity on NIS;
(h) Organize regular peer reviews on capabilities and preparedness;
(i) Organize NIS exercises at Union level and participate, as appropriate, in international NIS exercises.

A secure information-sharing infrastructure, like the one national CERTs have to be provided by Member States, is foreseen in Article 9, in order to allow the members of the cooperation network to communicate through a secure system.

The Directive highlights also the importance of early warnings (Art. 10) and coordinated responses (Art. 11), clearly signalling the weight coordination mechanisms have during the whole lifecycle of the incident – from its detection to the response phase.

The setup of such a network would imply a high level of cooperation and information sharing throughout the EU and possibly on a global level as well, due to the transnational, borderless nature of NIS threats and incidents. In order to achieve such a cooperation level, Article 12 empowers the Commission to adopt a "Union NIS cooperation plan", no later than one year after the Directive's adoption, which aims to coordinate Member States' NIS action; Article 13, on its hand, affirms that the EU may conclude international agreements with third countries or with international organizations partly or fully integrating them in the Union's cooperation plan.

The Directive's fourth chapter deals with public administrations' and market operators' NIS requirements and incident notification. Both are to undertake appropriate technical and organisational security measures[118] in order to manage the NIS risks relating to their operations. Those measures are to be appropriate in relation to the state of the art, and guarantee a level of security tuned to the risks foreseen: "*In particular, measures shall be taken to prevent and minimise the impact of incidents affecting their network and information system on the core services they provide and thus ensure the continuity of the services underpinned by those networks and information systems[119]*". Both, moreover, shall notify to the competent authority incidents having a significant impact on the security of the core services they provide[120]. Neither the NIS mandatory measures nor the notification requirement foreseen in Article 14's first two paragraphs apply, though, according to its last paragraph, to micro-enterprises, as defined in Commission Recommendation 2003/361/EC of 6 May 2003. Moreover, Article 1, paragraph 3, clarifies that "*(t)he security requirements provided for in Article 14 shall apply neither to undertakings providing public communication networks or publicly available electronic communication services within the meaning of Directive 2002/21/EC, which shall comply with the specific security and integrity requirements laid down in Articles 13a and 13b of that Directive, nor to trust* service providers".

The Parliament, mainly steered by its IMCO Committee, in its first reading[121] significantly amended the Commission's proposal for a NIS Directive, arguably watering down its scope and effectiveness.

As mentioned, the security and reporting requirements of the Directive would have applied, according to the Commission's version, to public administrations and market operators, defined as either (a) providers of information society services which enable the provision of other information society services" or (b) operators of critical infrastructure that are essential for the maintenance of vital economic and societal activities in the fields of energy, transport, banking, stock exchanges and health. Annex II concretely

[118] "'Security' means the ability of a network and information system to resist, at a given level of confidence, accident or malicious action that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data or the related services offered by or accessible via that network and information system":Art. 3 point 2, Commission's proposal for a NIS Directive.
[119]Art. 14, par. 1, Commission's proposal for a NIS Directive.
[120]Art. 14, par. 2, Commission's proposal for a NIS Directive.
[121]European Parliament,"Legislative resolution of 13 March 2014 on the proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union", (COM(2013)0048 – C7-0035/2013 – 2013/0027(COD)).

specifies, albeit in a non-exhaustive way, which categories of undertakings qualify as market operators for the purposes of the Directive.

The Parliament's version removes public administrations from the scope of the Directive, and amends the list of market operators excluding providers of information society services (as defined by the e-Commerce Directive) such as e-commerce platforms, internet payment gateways, social networks, search engines, cloud computing services and application stores, focusing instead on energy, transports, financial markets infrastructures, water and food production and supply, and internet exchange points[122]. A new Article 13a, moreover, allows Member States to determine the level of criticality of market operators, taking into account an array of considerations, such as the specificities of sectors, the importance of the particular market operator for maintaining a sufficient level of service, the number of parties supplied by the operator, the time period until the discontinuity of the core services of the market operator has a negative impact on the maintenance of vital economic and societal activities, and so on.

The Parliament also clarifies the incident reporting obligation set in Article 14. The notification, it specifies, shall be done *without undue delay* when incidents dent the *continuity* of the core services in a significant manner[123]; the significance of the incident shall be determined taking into consideration the number of users affected, its duration and its geographic spread. A newly introduced paragraph 2a specifies moreover that the authority to be notified is the one of the country of the affected core service. Finally, Article 1a's fifth paragraph states that the incident notification foreseen in Article 14 shall be without prejudice to the provisions regarding personal data breach notifications set out in Article 4 of Directive 2002/58/EC and in Regulation (EU) No 611/2013.

Despite narrowing the scope of the original Commission's proposal, the Parliament's text highlights the connection between NIS measures, notification to the competent authority and individuals' rights to privacy and data protection introducing Article 1a, titled "*Protection and processing of personal data*", that binds the processing of personal data in the NIS context to the respect of Directive 95/46/EC, Directive 2002/58/EC, Regulation (EC) No 45/2001, and Decision 2009/371/JHA. The same article specifies that "*(t)he processing of personal data shall be fair and lawful and strictly limited to the minimum data needed for the purposes for which they are processed*" and that the data "*shall be kept in a form which permits the identification of data subjects for no longer than necessary for the purpose for which the personal data are processed*".

The text supported by the Parliament would need approval by the Council before it could be converted into law, since they both must back proposed EU legislation before it can be introduced through the ordinary procedure. Discussions on how to balance the Commission's proposal with the Parliament's amendments are currently being held by Member States representatives[124]. It seems possible – even likely – that the Directive will be finalized before the end of the year.

The impact of on the A4Cloud toolset

The NIS Directive, overall, is expected to create a positive impact for EU cybersecurity in general and for the A4Cloud project in particular. The shift from a generalized voluntary approach to a mandatory framework is timely and opportune; the main issue, rather than the opportunity of the Directive's enactment, seems to be balancing the Directive's scope and obligations in order not to unreasonably hinder economic operators' ordinary activities, burdening them with too many obligations. As for the Project's scope, the adoption of a mandatory data breach notification mechanism and the imposition of a stricter minimum level of security measures could boost the usefulness – and therefore, potentially, the demand – of the A4Cloud toolset. The concordance between the NIS Directive's ratio legis and the A4Cloud's tools results clearly from the Project's definition of accountability, "defining governance to comply in a responsible manner with internal and external criteria, ensuring implementation of appropriate

[122]Ibid., Annex II.

[123] "Incident having a significant impact' means an incident affecting the security and continuity of an information network or system that leads to the major disruption of vital economic or societal functions": Art. 3 point 8a of the NIS Directive as amended by the Parliament.

[124]See for instance Council of the European Union, "Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union – progress report", Inter-institutional File:2013/0027(COD), Brussels, 22.5.2014. See also Council of the European Union, "3318th Council meeting. Transport, Telecommunications and Energy", Luxembourg, 5/6.6.2014

actions, explaining and justifying those actions and remedying any failure to act properly[125]". The Council is now discussing the proposed Directive. Some of the provisions on which it will have to reach an agreement with the Parliament closely relate with the Project's scope, aims and context.

In the first place, the scope of the NIS Directive would be significantly restricted if the final version will turn out to adhere to the Parliament's amendments: as for the Projects' interest, maintaining information society services – cloud services included – in the list of operators bound by NIS obligations would increase the relevance of the project's tools, making them go along with hard-coded legal obligations. In particular, having CSPs mandatorily subject, on one hand, to the security requirements set out by the Directive, and on the other to the notification obligation would significantly boost the tools' usefulness. In any case, the adoption of the A4Cloud toolset by the economic operators to whom the Directive will eventually apply is likely to be a meaningful help in compliance practices, and even if public administrations and some economic operators will be eventually excluded from the scope of the Directive, the Project's tools could still be adopted on a voluntary basis.

On the other hand, the Parliament's amendments show a closer connection and integration with both the existing data protection framework and the upcoming General Data Protection Regulation (GDPR) – a welcome approach, considering how the obligations set out in the NIS Directive could turn out to have a stark privacy-invasive side.

As the Commission's version, moreover, the Parliament's one keeps being characteristically technology-neutral: as Recital 25 of both the Commission and the Parliament's text highlights, the Directive's provisions "*should not require that a particular commercial information and communications technology product be designed, developed or manufactured in a particular manner*"; furthermore, its very wording allows its application irrespectively of the particular information and communication technology considered.

The substance of the provisions regarding the cooperation between authorities has been left untouched, and is likely to remain in the final version of the Directive: tool systems like the one prototyped by the A4Cloud consortium could turn out to be a valuable instrument in fostering incident reporting, notification and communication between the affected stakeholders, if further refined, developed and implemented in this direction. In this regard, a critical issue worth mentioning is that the cooperation and information sharing model sketched by both texts – the Commission's and the Parliament's ones – seems be strictly a top-down, unidirectional one: from the industry to the authority. A bi-directional approach could be ultimately better suited in improving European digital threat understanding and incident response[126]: information regarding incidents flowing both ways would arguably help the relevant actors sketch a clearer and more complete picture of what happens with respect to EU NIS; incident and threat-related information communicated by the relevant authorities to the concerned industries, moreover, could potentially improve the latter's responsiveness and effectiveness when dealing with information security incidents.

[125] n 1.

[126] Information Technology Industry Council, "ITI Position Paper on the Proposed "Directive of the European Parliament and of the Council Concerning Measures to Ensure a High Common Level of Network and Information Security Across the Union"", June 24, 2013.

Appendix 2

Remedies and redress mechanisms for business sensitive information[127]

Although the field data protection regulation is to some extent harmonised across the EU countries, when it comes to protection of business sensitive information, redress mechanisms and remedies vary from country to country bringing about the additional differences between civil law and common law jurisdictions. This section offers a first overview of remedies and redress mechanisms for business sensitive information focusing especially on the breach of contractual obligations, while the full analysis on remedies and redress mechanisms for business sensitive information will be a continuous task within WP44(D-4) to examine unfair competition practices and remedies in different criminal procedures.

Prior to examining those different aspects, it is first worthwhile to examine the regulatory framework provided by the World Trade Organisation's 1994 TRIPS Agreement (Agreement on Trade-Related Aspects of Intellectual Property Rights). Article 39 focuses on "undisclosed information" and establishes minimum requirements for the protection of such information. Its provisions generally provide that undisclosed information will be protected where:

1. The Information is secret (in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among person within the circles that normally deal with such information)
2. There is commercial value because the information is secret
3. Reasonable steps have been taken to maintain the secrecy of the information

As will be seen below, these basic parameters have been adopted by both the civil law and common law jurisdictions through the development of the applicable codes and case law. Also notable is that oftentimes there will be contracts among the party holding the rights to the trade secrets or confidential information.

On 28 November2013, the European Commission published a Proposal for a Directive "*on the protection of undisclosed know-how and business information* (trade secrets) *against their unlawful acquisition, use and disclosure*"[128]. The Proposed Directive aims to harmonise national civil law remedies against the misappropriation of trade secrets and rules on preservation of confidentiality of trade secrets during and after legal proceedings.[129]The Proposed Directive will be sent to the Council of Ministers and the European Parliament for adoption. Once approved, it will make it easier for national Courts to deal with the violations of business sensitive information and for victims to receive remediation. Furthermore, the proposal is in full alignment with the TRIPS Agreement obligations: it will largely align the protection of business sensitive information within the EU with that of the US. Additionally, harmonised EU rules will contribute to influencing a global level of protection of business sensitive information, within the spirit of the TRIPS Agreement.

Civil law jurisdictions

At present, there is no EU framework for business sensitive information. Across EU, national laws on redress against misappropriation of business sensitive information differ significantly.[130] For instance, some Member States like "Austria, Bulgaria, the Czech Republic, Estonia, Germany, Finland, Greece, Hungary, Italy, Latvia, Lithuania, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden have specific legislation on misappropriation of trade secrets, although some of them fail to define what trade secrets are (examples: Germany, Finland, Greece, Denmark, Spain).In others, like Belgium, France,

[127] The discussion below is based on the analysis for the internal milestone report MS:D-4.1 on legal analysis and redress mechanisms.

[128]Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure 2013/0402 (COD), http://ec.europa.eu/smart-regulation/impact/ia_carried_out/docs/ia_2013/com_2013_0813_en.pdf.

[129] p. 6 Proposed Directive on trade secrets.

[130]http://ec.europa.eu/internal_market/iprenforcement/docs/trade-secrets/120113_study_en.pdf

Ireland, Luxembourg, Malta, the Netherlands, there are no specific provisions on trade secrets in civil law"[131].

Nevertheless, it is important to consider a set of civil remedies (that trade secret holders can seek for breaches of confidence) that will be addressed through the terms and conditions of the contracts among the various actors, whenever they suffer from trade secret misappropriation. Most States provide for the protection of trade secrets by contractual obligations. Considering that most claims involving acts and/or omissions involving trade secrets fall under the umbrella of a claim for breach of confidence/breach of contract, bellow are discussed the main aspects of civil law jurisdictions concerning remedies and remediation mechanisms for breach of contract where the violation consists in the improperly use or disclose of business sensitive information.

Remedies and remediation in case of breach of contract across the European Union

In all legal systems are provided appropriate remedies in case of breach of contract. According to civil law jurisdictions, the term "breach of contract" refers not only to the cases in which (i) the performance of a binding agreement is not honoured and, therefore, totally lacking, but also to those in which the performance actually carried out is (ii) late, (iii) defective or is (iiii) not the same, in some respects, to that originally provided for in the contract. Under the traditional approach of the German Civil Code (BGB), breach of contract occurs even in the event of impossibility of performance. When a breach of contract occurs, the following options are offered:

a) Specific enforcement/performance

It is an order by the Court requiring one party to perform their contractual obligation. When entering into a bilateral contract, each party acquires a legal right to the performance of the contract and at the same time assumes a legally recognised and enforceable obligation to perform it. In civil law jurisdictions, specific relief, particularly in the form of an order for specific enforcement/performance or an injunction, is the preferable remedy imposed by Courts.

Under common law, granting specific performance is an extraordinary remedy, granted in very limited circumstances and the specific performance would be ordered only if the Court thought it suitable, while the general principle for the assessment of breach of contracts is compensation for damages. This is the most striking difference between the civil and common law approach to remediation for a breach of a contract.

b) Termination

Termination is an order by the Court, which ends whatever remains to be performed according to the contract. The Court will have to verify that the breach of the contract is relevant and that the contract will be unable to fulfil the interest of the debtor. The innocent party has the option of terminating the contract only if the breach is a serious (or fundamental) breach of a term or the party totally fails to perform the contract.

c) Compensation for damages

Whenever trade secrets are misappropriated (e.g. stolen or misused) by a third party, the trade secret owner will suffer losses. Compensation is intended to "compensate" for the injured party for damages suffered as a result of the breach of contract and it is a monetary sum fixed by the Court to compensate the injured party. It may bear no relation to the actual loss suffered; even exceed the amount of loss caused by the breach of contract.

The civil law system adopts the rule that the debtor is released from the obligation of compensation only in cases where the breach (default or the defective performance) has depended on an external cause for his behaviour. In particular, Articles 1147-1148 French Code civil and Article 1128 Italian Civil Code provide that the debtor is ordered to pay damages and interest when he fails to prove that

[131]http://europa.eu/rapid/press-release_MEMO-13-1061_en.htm

the failure (or delay) is due to a cause unrelated to his behaviour: that no damage or interest is due if the breach of contract has resulted by unforeseeable circumstances or force majeure.

In the **French civil code** and in the **Italian civil code**, the general rule is that when a party fails to perform, precisely and exactly, his obligations under the contract, the other party *may choose* between the specific performance or the termination of the contract, leaving unabated compensation of damages. More specifically, Article 1184 of the French Civil Code provides that with respect to each contract a tacit termination clause is implied, for the case in which one of the parties fails to meet a contractual obligation. The second paragraph of the same article also establishes that the party who has suffered the breach may choose to force the other party to the specific performance - if this is possible - or to request termination of the contract and damages. At the same time, Article 1453 of the **Italian Civil Code** states that in contracts when one party does not fulfil its obligations, the other may, at his own discretion, ask the specific performance (adempimento in forma specifica) or termination (risoluzione) of the contract, leaving unabated compensation for damages. The termination is pronounced by the Court upon request of the parties (judicial termination).In the Franco-Italian model neither option has the priority. The contractor may request the specific performance or the termination of the contract and the compensation of the damages.

In some other civil law systems exists, on the contrary, the principle that the party may redress to Court to seek for termination of the contract only if specific performance has become impossible.

In Germany, the § 241 **BGB** states that the creditor is entitled to demand specific performance from the debtor, with the exception only of the case in which the obligation itself has become impossible. Only in this case, the party may ask for termination and compensation.
In other words, "the specific performance" is the main remedy that must be applied for all the times in which it is still possible to perform the obligation and only in the case of impossibility the creditor may instead act for termination and compensation.

In the **Dutch Law**, the Wet van 6 maart 2003 amended Article 7:22 BW, stating that a party can seek for termination (*ontbinden*) only when the breach is essential. Alternatively, the party may request a reduction of the price with respect to what was agreed.

In the **Greek Law**, Article 540 of the Civil Code, as amended by Law no. 3043, of 21 August 2002, governs the rights of the consumer. There is no priority among remedies and all are intended to be equivalent. When one party does not fulfill its contractual obligations, the other may, at his own discretion, ask the specific performance or termination of the contract, leaving unabated compensation for damages. The consumer may act for a reduction of price if the breach is not essential.

Common law

As referenced above, many of the redress/recourse mechanisms and the remedial actions for breaches of confidence will be addressed through the terms and conditions of the controlling contracts among the various actors. Nevertheless, it is important to realise that oftentimes the contracts will not address such situations and/or a remedy may be needed against a non-party to a contract who improperly uses or discloses business sensitive information (which is also referred to at times as confidential information and/or trade secrets).

United Kingdom

The common law of the United Kingdom is perhaps the best illustrative of how trade secrets and confidential information are protected under common law in the European Union and is well-developed with many illustrative cases and nuances.

In particular, most claims involving acts and/or omissions involving trade secrets fall under the umbrella of a claim for breach of confidence. While this is technically a claim for equitable relief, courts have applied it more like a tort claim. The term trade secret is believed to have first been used in a court decision in Newberry v. James (1817) 2 Mer. 446, 35 Eng. Rep. 1011, 1013 (Ct. Ch. 1817).The basis for a claim for breach of confidence thereafter was established in *Morison v. Moat* (1851) 9 Hare 241, per Turner V-C, where it was held:

In some cases, it [the jurisdiction of the court] has been referred to property, in others to contract, and in others, again, it has been treated as founded upon trust or confidence, meaning, as we conceive, that the court fastens the obligation on the conscience of the party, and enforces it against him in the same manner as it enforces against a party to whom a benefit is given the obligation of performing a promise on the faith of which the benefit has been conferred; but, upon *whatever grounds the jurisdiction is founded, the authorities leave no doubt as to the exercise of it*.

Coco v. A.N. Clark(Engineers) Ltd. [1969] R.P.C. 41 is widely considered the leading modern case on a claim for breach of confidence and provides that three elements must be established to prevail on such a claim:

1. The information must be confidential
2. The information must be disclosed in circumstances giving rise to an obligation of confidence
3. There must be actual or anticipated unauthorised use or disclosure of information

There are some other important requirements in regard to a claim for breach of confidence. First, in order to bring such a claim, the claimant must establish that it is the person to whom the duty of confidence is owed. *Fraser v Thames TV* [1984] QB 44.A duty of confidence arises out of the relationship between two entities, and so it is quite possible that for any piece of information person A would owe the claimant a duty of confidence while person B does not.

Second, there is no need to show any detriment from the breach of confidence when it involved personal or commercial information (diversion of potential business suffices to show damages), though detriment is required to be shown when the confidential information is government information. *Attorney General v Guardian Newspapers Ltd* [1990] 1 AC 109; see also, *R v. Department of Health ex parte Source Informatics* [2001] QB 424 (CA).

Finally, the determination as to whether there has been a breach of confidence will be contextually dependent. For example, in a contract situation, the determination will depend on the contract; in an implied situation it depends on the purpose of why the information was disclosed; and in other cases, an objective test is applied as to the confidant's own conscience, i.e., would a reasonable confidant, under the same circumstances, think that his action amount to a breach of confidence?

English courts have also examined the first two elements in greater detail (with the third element largely speaking for itself and either happening or not happening).As to the first element of whether the information is confidential, in determining whether the information is confidential, courts have held that the information must be sufficiently developed, i.e. the information must be fairly specific, rather than a mere idea, and the kind of information that the relevant industry would deem involved protectable concepts. Fraser v Thames TV [1984] QB 44.Courts have also held that the information must be inaccessible or maintained in relative secrecy (absolute secrecy is therefore not necessary for information being deemed as confidential).Cantor Fitzgerald International v Tradition (UK) (2000) RPC 95; Mars UK Ltd. v Teknowledge Ltd. (2000) FSR 138.In further examining this requirement, courts have generally looked to commercial considerations, including whether appropriate security measures have been taken to protect the information such as managing information flows and access, whether and what sort of restrictions have been placed on the use and disclosure of the information (generally through purpose limitations), whether there has been active policing and enforcement of the measures taken in respect to maintaining the confidentiality of the information, and whether there are any non-compete provisions required from those to whom the information is disclosed.

Finally, the information must not already be in the public domain. For example, the information must not be well-known to the section of the public that has an interest in knowing the information.*Ryan v Capital Leasing* (High Court of Ireland, 2 Apr. 1993).However, where confidential information is shown to a limited set of people, eg friends, families, and co-venturers – depending on the circumstances, the information will still be deemed to be confidential.*Prince Albert v Strange* (1849) 2 De G & Sm 652.But information which has been published, even if it is not easily accessible to the public at large, will have lost its confidential nature – see e.g. *Franchi v Franchi* [1967] RPC 149 where the information was published in a foreign patent application.

As to the second element, whether the disclosure gives rise to an obligation of confidence, there are two general categories of such circumstances. The first category is where there is an express obligation imposed on the confidant through an agreement. Such obligations are generally found in non-disclosure agreements or in larger contracts such as outsourcing agreements, data processing contracts, or similar type contracts. In reviewing and applying such contracts, the terms must be reasonable and there remain exceptions where the obligation will not be applied despite the parties' agreement, such as where the information has come into the public domain, a party was in possession of information before agreement was entered, or where the information is acquired from a third party. There is also an exception where the disclosure is justified in the public interest, such as a disclosure of unlawful behavior by the confider. Initial Services v Putterill [1967] 3 All ER 145, [1968] 1 QB 396.This defense is not just limited to cases of wrongdoing by the plaintiffs, i.e. the inequality rule; but there are also limitations where someone does not need to disclose to the whole world where lesser disclosure may suffice. And, importantly, these protections have been codified in the UK in the Public Interest Disclosure Act 1998.

The second category is where the obligation is implied by law. Typical situations where a duty of confidence will be implied by law include where a fiduciary duty exists, eg, officers or directors of a business entity, business partners, attorney-client relationship, etc. Outside such inherently confidential relationships, as the court held in *Coco v. Clark*, a party is bound to respect the confidentiality of information which has been disclosed to him if he either knew or ought in the circumstances to have known that the information was communicated to him in confidence. Examples might include where information is disclosed in a business-like relationship, with a joint venture in mind, or in relation to the manufacture of articles. An implied duty will often apply in other relationships, such as in the employment context. Courts have even found an implied duty where there was no direct relationship between the parties, imposing the duty on a third party learning of confidential information and knowing it to be confidential. Attorney-General v Guardian Newspapers (No.2) [1990] AC 109; see also, English & American v. Herbert Smith (1988) FSR 232 (holding a third party coming by confidential information innocently, but subsequently discovering the information to be confidential, will be bound by a duty of confidence).Finally, a duty of confidence has even been extended to strangers where the stranger had knowledge that the information they were disclosing or otherwise using without authorisation was confidential. Shelly Films v Rex Features (1994) EMLR 134.

There are generally four remedies available for breach of confidence. None of these are exclusive and all will generally be ordered if there has been a breach of confidence. The first is injunctive relief[132], where a party can be ordered not to make further use or disclosure of the confidential information. The second remedy is the compulsion of an account for profits, where the offending party will be compelled to account for all uses and disclosure of the confidential information, as well as any monies received as a result of such use and disclosure. The third remedy is the delivery up/destruction of the confidential information, where the offending party will be required to deliver all confidential information to the party owning the information and/or otherwise destroy any remaining copies of the confidential information. Finally, the fourth remedy is monetary damages, which can be determined by the market value of the information, a fair remuneration of what licensing fees would have been, and/or the loss suffered by the claimant (including loss of potential profits) from the unauthorised use or disclosure of the information.

There are three other related concepts worth mentioning in respect to trade secrets. The first is what has come to be known as the springboard doctrine as adopted in *Terrapin Ltd v. Builders' Supply Co (Hayes) Ltd [1960] RPC 128*, where that court held that "a person who has obtained information in confidence is not allowed to use it as a springboard for activities detrimental to the person who made the confidential communication, and springboard it remains, even when all the features have been published or can be ascertained by actual inspection by any member of the public." The basis of this concept is that, although the information has now ceased to be confidential, the confidant wrongly used it while it was still confidential. This gives the confidant a commercial lead in the market, and fairness and justice requires that the advantage be taken away. This doctrine has resulted in courts sometimes imposing what are known as "springboard" injunctions to prevent any unfair advantage from a breach of confidence, though

[132] Injunctive relief is an equitable remedy available to courts which empowers them to prevent certain acts or to compel certain acts. Such relief can be preliminary and temporary in nature, for example to preserve the status quo while a case is pending, or can be permanent in nature, whereby courts may prevent certain acts permanently, even after the case before it is otherwise resolved.

such injunctions will not last for an unlimited period of time and only for the period of time where the unfair advantage is expected to last.

United States

Many cloud computing contracts among cloud actors contain forum selection provisions choosing courts in the United States as the only venue in which to litigate any disputes arising from the contract and/or choice of law provisions providing the law of a certain state, oftentimes California, as the governing law. See generally, Bradshaw, Simon, Millard, Christopher, and Walden, Ian (2013), Standard Contracts for Services, Cloud Computing Law, ed. Millard, C. 37 – 72.However, the United States proves to be a more difficult study in light of its federal laws, state laws, and the development of case law, all of which can vary across those the federal circuit courts and the fifty states. Nevertheless, there are some common features to generalise the typical approach to how trade secrets are approached.

First and foremost, in 1979, the Uniform Law Commission, National Conference of Commissioners on United States Laws[133] proposed a uniform law on trade secrets known as the Uniform Trade Secrets Act. With the exception of New York and Texas, which still rely on common law, all other states have adopted the act. See Study on Trade Secrets and Confidential Business Information in the Internal Market, Final Study, April 2013, Prepared for the European Commission, Contract Number: MARKT/2011/128/D at p. 10.For our purposes, and because many cloud computing contracts are governed by California law, our examination will be of the Uniform Trade Secrets Act as enacted in that state in its Civil Codes Sections 3426 through 3426.11, inclusive.

> Under the Uniform Trade Secrets Act, a trade secret is defined as:
>
> Information, including, without limitation, a formula, pattern, compilation, program, device, method, technique, product, system, process, design, prototype, procedure, computer programming instruction or code that:
> (a) Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by the public or any other persons who can obtain commercial or economic value from its disclosure or use; and
> (b) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

California Civil Code, § 3426.1(d).

> "Misappropriation" means:
>
> (1) Acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or
> (2) Disclosure or use of a trade secret of another without express or implied consent by a person who:
> (A) Used improper means to acquire knowledge of the trade secret; or
> (B) At the time of disclosure or use, knew or had reason to know that his or her knowledge of the trade secret was:
> (i) Derived from or through a person who had utilised improper means to acquire it;
> (ii) Acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or
> (iii) Derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or
> (C) Before a material change of his or her position, knew or had

[133] This organisation is not empowered to make laws, but rather regularly meets to discuss the harmonisation of laws across the United States and proposes uniform laws to be adopted. States are not required to adopt such laws, but normally do so, oftentimes with slight changes from the proposed language by the Uniform Law Commission.

> reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake.

California Civil Code, § 3426.1(b).

The Uniform Trade Secrets Act provide remedies similar to those provided in the United Kingdom, including injunctive relief, damages, and licensing fees. California Civil Code, § 3426.2 and 3426.3.Perhaps the biggest difference between UK and US law is that the Uniform Trade Secrets Act provides for an award of exemplary damages not exceeding two times the amount of compensatory damages awarded, but only if there has been wilful and malicious misappropriation. See California Civil Code, § 3426.3(c).

Finally, and notably, the Uniform Trade Secrets Act specifically provides that it does not supersede any contractual remedies agreed to between the parties, other civil remedies available to a party, or any criminal remedies that may also exist. See California Civil Code, § 3426.7(b).

11 Index of Figures

Figure 1: Wearables use case architecture, borrowed from D7 27
Figure 2: DTMT sequence diagram, taken from D3 29
Figure 3: Data Retention Audit Task in AAS 31
Figure 4: A simple Cloud Provision Chain 36
Figure 5: The Incident List 37
Figure 6: Detail view of an incident 38
Figure 7: Data flow in supply chain 41
Figure 8: The high level architecture of the Remediation and Redress Tool. 45
Figure 9: The remediation and redress interaction diagram supported in A4Cloud 46
Figure 10: An example of the Data Track database hosting the incident information. 47
Figure 11: Populating incidents in the widget of Data Track UI. 47
Figure 12: Screenshot of the RRT UI 48
Figure 13: Screenshot of the RRT remedies window 49
Figure 14: Example of proposed actions for remediation from the RRT remedies view 50
Figure 15: Accountability Lifecycle and Practices 51
Figure 16: The position of IMT and RRT in the tool interaction diagram of A4Cloud 53
Figure 17: Overview of the incident management and remediation tools 53
Figure 18: Detailed interaction diagram among the A4Cloud tools 54

12 Index of Tables

Table 1: CSA incident categories and A4Cloud categories, examples taken from [D7] 10
Table 2: Complete REST interface for exchanging incident information 41