Deliverable

60

Report on Confidentiality Clauses in VO contracts

WP9 Legal Issues

Dana Irina Cojocarasu,
NRCCL (ed.)

14.08.2006

Version

1.0

TrustCoM

A trust and Contract Management framework enabling secure collaborative business processing in on-demand created, self-managed, scalable, and highly dynamic Virtual Organisations

SIXTH FRAMEWORK PROGRAMME

PRIORITY IST-2002-2.3.1.9

Prepared for the European Commission under FP6 Contract No. 01945 as a deliverable form

LEGAL NOTICE

The following organisations are members of the Trustcom Consortium:

Atos Origin,
Council of the Central Laboratory of the Research Councils,
BAE Systems,
British Telecommunications PLC,
Universitaet Stuttgart,
SAP AktienGesellschaft Systeme Anwendungen Produkte in der Datenverarbeitung,
Swedish Institute of Computer Scence AB,
Europaeisches Microsoft Innovations Center GMBH,
Eidgenoessische Technische Hoschschule Zuerich,
Imperial College of Science Technology and Medicine,
King's College London,
Universitetet I Oslo,
Stiftelsen for industriell og Teknisk Forskning ved Norges Tekniske Hoegskole,
Universita degli studi di Milano,
The University of Salford,
International Business Machines Belgium SA .

Deliverable datasheet

Project acronym: TrustCoM

Project full title: *A trust and Contract Management framework enabling secure collaborative business processing in on-demand created, self-managed, scalable, and highly dynamic Virtual Organisations*

Action Line: 6

Activity: Analysis of Legal Issues

Work Package: 9

Task:

Document title: Confidentiality clauses in VO contracts

Version: 1.0

Document reference:

Official delivery date: 31 July 2006

Actual publication date:

File name:

Type of document: Report

Nature: Public

Authors: Jon Bing, Dana Irina Cojocarasu, Tobias Mahler, NRCCL

Reviewers: CCLRC and Atos Origin

Approved by:

Disclaimer

This document is the result of research work carried out in the TrustCoM Project. It is not intended to be legal advice and is not to be construed or understood as legal advice. Persons interested in applying any information in this document to their specific needs are recommended to seek relevant professional legal advice regarding their specific needs/requirements.

Neither the authors of this document, nor the TrustCoM Consortium, nor the European Commission shall be liable for any use made of this document. This document does not represent the opinion of the European Community nor is the European Community responsible for any use that might be made of the content of this document.

Forum

Any dispute arising out of or in connection with this document shall be submitted to the exclusive jurisdiction of the Norwegian Courts.

Table of Content

1 Executive summary

This report summarizes the research performed in TrustCoM Work Package 9 in the first half of 2006. The objective of the legal work package in TrustCoM is to study selected legal issues in relation to trust, security and contract management for virtual organisations

This study addresses confidentiality issues in virtual organisations' (VO) contracts. Legal issues in virtual organisations were previously discussed in D 15 (Report on Legal Issues) and D 17 (Legal Risk Management for Virtual Organisations). The TrustCoM contract model for VOs is presented in the TrustCoM framework deliverable.

This report focuses only on a subset of clauses in VO contracts. Confidentiality related clauses will arguably play an important role in VO contracts in the TrustCoM context, since the collaboration of VO partners in many cases will require participants to communicate confidential information. Confidential information will need to be protected both though technical means – as addressed in other TrustCoM deliverables - and through the use of appropriate clauses in the contract or contracts established to operate a VO.

This study aims at providing a framework for identifying what may legitimately described as confidential information, and what action can be taken if the this type of information is improperly disclosed. A special emphasis was therefore placed on identifying risks to information that VO partners have access to, with respect to (i) illicit access to confidential information by VO members or third parties, (ii) illicit dissemination of confidential information to entities that are not entitled to access the information.

The first part of the study identified and discussed the criteria in the light of which one can evaluate the confidential character of certain information. Having article 39.2 of the TRIPs Agreement as a starting point, we were able to conclude that the legal protection for “secret commercial information” depends on its relative novelty and exploitability and that it relies to a high extent on the implementation and documentation of “reasonable steps to maintain that information as secret”[1]. This requires that the management first of all identifies the relevant information assets and ranks them according to their level of sensitivity. This is by no means an easy task, since the competitive advantage provided by certain strategic information might become evident only after it has already been lost to a competitor.

One obvious solution would be to implement a high degree of security for ALL the information that is generated or exchanged by the organisation. On the other hand, proper allocation of resources as well as prevention of overreaching closure of the organisation to various business opportunities would make more appropriate a dynamic access management approach.

Depending on the applicable law in the particular context, the identification of confidential information will take into account with more or less accuracy the will of the contractual partner(s) disclosing the confidential information, as it is expressed in the agreed contractual arrangements. Over and above the manifested intention of the parties, the statutory limitations of the applicable law will decide the extent to which the contractual provisions are enforceable. Various legislations provide one or more criteria to qualify information as confidential and one or more formalities to be complied with by the parties once such designation of confidential information occurs.

[1] See TRIPs Agreement article 39.

Moreover, regardless of the way in which certain information was designated as confidential, statutory legal norms, enforcement of contractual provisions or criminal sanctions can deter someone from misusing it. These legal means of protection of confidential information provide possible treatments for mitigating the risks arising from the disclosure of confidential information. Their features, as well as the opportunity of their use are examined in Section 4 explaining the legal protection of confidential information.

The risks arisen during or following the disclosure of confidential information are most frequently mitigated through non-disclosure agreements. They can be regarded as the most proactive legal means of protection for the party disclosing confidential information. The proactivity stems from the fact that the potential business partners can negotiate and agree in detail on the extent of their mutual rights and obligations regarding the access to one or another's confidential information. Furthermore, if the terms of the non-disclosure agreement are not abided, its clauses can be enforced and adequate remedies can be provided to the party suffering a loss.

The enforcement of contractual provisions does not actually hinder the unlawful disclosure and the misuse of the confidential information in the manner in which a high standard security system might. However, once such an unwanted incident occurs, they become a powerful tool (maybe the only one available) in stopping further misuse or in obtaining damages for the harm caused. The rights and obligations guaranteed/ imposed through contractual arrangements on the contractual partners are analysed in Section 5 of the Deliverable.

Confidentiality is not, however, an absolute obligation. It has long been established that just cause or public interest action are defences to an action for breach of confidence. In practice this means that information imparted in confidence can in exceptional circumstances be disclosed regardless of the terms of the confidentiality agreement.

For example, the defence extends to all those judicial or administrative procedures where disclosure is imposed by the public administrative or judicial authorities.

Moreover there are some information about the organisation (internally designated confidential information) that the organisations shouldn't hide from potential business partners under the umbrella of confidentiality, either in the negotiation- identification phase of the Virtual Organisation lifecycle or during the execution of the contracts/ operational phase. In this case, it is not the disclosure that is sanctioned by the law, but the non-disclosure. Non-disclosure of such information may vitiate the collaboration contract with that business partner, making the agreement totally or partially unenforceable. This means that the party in good faith may have a just cause not to fulfill its duties (be it provision of a certain service of facility, performance of an analysis, or payment). This will of course hinder the attainment of the VO purpose and would activate additional policies, such as termination of collaboration, identification of new partners. Aditionally this might entail a decrease in the reputation score of the partner, modifications in the access authorisations and tokens. Section 6 of the Deliverable adresses these issues in more detail. In the context of TrustCom it is advisable that the parties disclose and discuss such information in the identification phase of the VO lifecycle in order to prevent risks relating to the invalidity of the colabloration agreement.

The results of the legal analysis performed in the main part of this Deliverable are tailored in Appendix A to the specificity of the TrustCom CE Scenario, as described in TrustCom Deliverables D 10 and D 41 and to the business models discussed in the socio-economic analysis discussed in D 59. Appendix A of this Deliverable provides an analysis of the CE scenario in the TrustCoM framework in the light of the legal requirements described above in order to identify the confidential information exchanges in the scenario and provide legal input in the design and deployment of policies governing the

access to confidential information. Moreover, we point out contractual solutions to mitigate the risks associated with the disclosure of confidential information during the VO lifecycle and after the dissolution of the VO where some business roles will have to be maintained. This analysis will be performed in accordance with the methodology provided in the first part of **Appendix A.**

Based on the legal and methodological input we provide, the parties may conduct a risk analysis evaluating up to what point they can prevent and manage conflicts internally and in what circumstances they have to rely on the legal authority of a third party (such as the judicial authorities for example). Moreover if the latter solution appears as necessary, due to the high degree of automation and to the delocalisation of the services in the TrustCoM framework, the parties may be constrained to monitor[2] certain elements with procedural relevance that go beyond simply ensuring the technical availability, integrity or confidentiality of the system. In order to lead credible evidence in courts it is essential to maintain a record of the measures taken by the organization on information security.

The findings of the legal analysis carried out in the main report have been summarized in a risk checklist (Section 8 of the Appendix) that uses the legal risk analysis of the CE scenario as described in Appendix A in order exemplify risks to confidentiality in the proposed scenario.

[2] Monitoring would need to be in accordance with evidentiary legal requirements.

2 Introduction

This report describes the research performed in TrustCoM work package 9 in the first half of 2006. The objective of TrustCoM's legal work package is to study selected legal issues in relation to trust, security and contract management for virtual organisations.

This study aims at identifying the risks to information that VO partners will have access to, with respect to (i) illicit access to confidential information by VO members or third parties, (ii) illicit dissemination of confidential information to entities that are not entitled to access the information. For a VO using the TrustCoM technology, the challenge was to integrate the access based on policies as defined in the TrustCoM framework with the legal protection of confidential information. In this context the legal protection of confidential information in selected statutory laws has been analysed and the need for additional contractual clauses was assessed. The Deliverable begins with an analysis of the notion of confidentiality according to several national laws (Section 3.1), including terminological distinctions to be made among confidentiality and related terms, such as secrecy, privacy, security (Section 3.2).

Once the conceptual framework of confidentiality is set, the legal analysis proceeds with the identification of the means through which the law safeguards the interests of the party disclosing confidential information (Section 4).

Section 5 explores in detail the confidentiality agreements, also known as non-disclosure agreements, since they represent the most frequent and the most proactive legal mean of protection of the party disclosing confidential information. Their proactivity stems from the fact that they enable the discloser and the receiver of the confidential information to negotiate both the manner in which this information will be identified, and the manner in which it will be handled. Some of the key issues discussed in this context are: how long the protection should last, the scope of the parties' mutual obligations, procedures for lifting the limitation and procedures for exceptional circumstances.

In principle, the receiving party is prohibited by law to reveal to third parties or to misuse information disclosed to it in confidence.

Information otherwise designated as confidential can in exceptional circumstances be disclosed regardless of the terms of the confidentiality agreement. For example they may be part of judicial or administrative procedures where the applicable law imposes disclosure to the state authorities. Similarly, there are some inforamtion about itself (internally designated confidential information) that the organisations cannot hide from potential business partners under the umbrella of confidentiality, either in the negotiation- identification phase of the Virtual Organisation lifecycle or during the execution of the contracts/ operational phase. In this case, it is not the disclosure that is sanctioned by the law, but the non- disclosure. In the negotiation phase for example, not only the parties have to make only true assertions, but sometimes they have the obligation to disclose certain information about themselves if they are relevant in the other parties' decision to enter the business

relation or not. Otherwise the collaboration agreement can be invalid. This situation where the law imposes disclosure and sanctions the secrecy will be analysed in Section 6.

The results of the legal analysis performed in the main part of this Deliverable are tailored in Appendix A to the specificity of the TrustCom CE Scenario, as described in TrustCom Deliverables D 10 and D 41 and to the business models discussed in the socio-economic analysis discussed in D 59. We integrate thus the access based on policies in the Trust Com framework with the legal protection of confidential information, in the context of different business models. The integration is achieved through providing input regarding the design of policies regarding access to confidential information as well as through suggesting appropriate contractual arrangements able to reduce the likelihood or the consequences of unwanted incidents involving confidential information. Section 7 of this Deliverable summarizes the results of Appendix A.

It is worth reminding also that enforcing contractual provisions in accordance with the applicable law represents an ex-post measure (to be taken after the damage- in this case misappropriation of confidential information- has occurred). Despite the fact that it may provide for equitable remedies for the confidentiality loss/ infringement of contractual rights and even criminal sanctions against the guilty party, the value derived from the restricted exploitation of the asset protected by confidentiality is lost forever as the information reaches public domain. This increases the need for adequate information systems managing access to confidential information.

3 Conceptual framework

Following the idea of an English court decision in 1987[3] we might distinguish three layers of information being produced or exchanged during commercial interactions between market players:

First, there is what can be described as "trivial information", that is in the public domain, easily available for anyone interested. The field of activity, as well as information made available on the website of an organisation would fit into this category.

Secondly there is information which an employee of the organisation should not disclose to anyone outside the organisation without prior authorisation, either because he is told that it is confidential or because its content makes it obviously confidential. Once learned, this information remains in the employee's head and will be regarded as part of his skill and knowledge, as part of his "professional expertise". While the employment lasts, the employee cannot use this information other than for the employer's benefit but when it ends he can use it as part of his professional experience, *absent a restrictive covenant.*

And finally there is information so sensitive that even though learned by heart it **cannot be used** for anyone's benefit even post-employment (other than the former employer's).

Obviously, the three categories are not static, one piece of information potentially being part of any of the three categories at one point in time. As it will be explained below, "confidentiality" is not the equivalent of "secrecy" although the latter notion functions as precondition for the first one. According to the ISO[4] , "*confidentiality"* would ensure that information is accessible only to those authorized to have access. Limited access excludes absolute secrecy: the information is known but only by authorised persons that are prohibited to transmit it further if this communications exceeds the limits of the authorisation he/she received. In a legal perspective, we are interested not only in finding out the treatment that confidential information is to receive (access based only on authorisation) but also what kind of information can be designated as confidential, how is that designation to be made, what kind of rights it ensures and what remedies are available once this information is unlawfully disclosed to unauthorised parties.

The first international legal instrument to provide for express "protection of undisclosed information" was the TRIPS Agreement[5] in 1994, up until now the most comprehensive international treaty on Intellectual Property. Before the coming into effect of the TRIPS Agreement, some protection to commercial confidential information was awarded through the application of the general rules regarding

---

[3] Faccenda Chicken v. Fowler [1987] 1 Ch.117, Goulding J ruling.

[4] International Organisation for Standardisation, http://www.iso.org/iso/en/ISOOnline.frontpage

[5] Agreement on Trade-Related Aspects of Intellectual Property Rights, available at: http://www.wto.org/english/tratop_e/trips_e/t_agm0_e.htm

unfair competition, especially Article 10 bis of the Paris Convention for the Protection of Industrial Property[6]. Paragraph 2 of article 10 bis contained a broad provision outlawing any acts contrary to honest practices in industry and commerce: "*Any act of competition contrary to honest practices in industrial or commercial matters constitutes an act of unfair competition*".

3.1 Definitions

The TRIPS Agreement in Article 39.2 does not require undisclosed information to be treated as a form of property (that is it does not guarantee exclusive rights for their owner, similar to patent rights for example), but it does require that a person lawfully in control of such information must have the possibility of preventing it from being disclosed to, acquired by, or used by others without his or her consent in a manner contrary to honest commercial practices:

> *Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices so long as such information*:
>
> (a*) 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 or readily accessible to persons within the circles that normally deal with the kind of information in question;*
>
> *(b) has commercial value because it is secret; and*
>
> *(c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.*

The three conditions comprised in article 39.2 of the TRIPs agreement can be regarded in fact as criteria in the light of which one can evaluate the confidential character of certain information. They will be explained in more detail below, also in the light of national applicable laws in the selected jurisdictions.

3.1.1 Content related requirements

As expressed by the first two conditions in article 39.2 of the TRIPs Agreement, not any information can be regarded as confidential: it has to go beyond the common professional knowledge in the field (relative novelty), and be commercially valuable to the rightful holder[7] (exploitable) provided it is kept out of the public domain.

It can be inferred from the text of article 39.2 that no information is worth keeping confidential when it is already in the public domain or easily inferable from the

[6] Available at: http://www.wipo.int/treaties/en/ip/paris/trtdocs_wo020.html

[7] I avoid using the term "owner" due to the fact that confidential information does not give property rights similar to for example copyrights or patents. As long as someone else finds it out through honest commercial practices (such as reverse engineering, independant research, or the information reaches public domain) the "confidentiality" protection is lost without the possibility for remedies. See more in Chapter 5.3

information to be found in the public domain. In this context, the doctrine[8], defines narrowly the "public domain", as "is not possible to state that everything that has been published anywhere in the world is destructive of secrecy - although it is destructive of novelty under patent law. It depends on the real ease of access to the publication […] The secrecy is defined relatively to those persons who normally deal with this category of information. As already noted, the requirement of only a relative secrecy allows the owner of a trade secret to obtain its legal protection although some other competitors keep the same matter confidential." Nonetheless, if every competitor is aware of that information, it is no longer secret in these circles. "The fact that newcomers to the industry would find it difficult to gain access to the information is of no relevance".

The second requirement in TRIPs seems to suggest that the commercial value of confidential information is derived from its limited accessibility. Since no agreed "book value" exists for most confidential information up to now, its appraisal by its legitimate holder will in practice determine its status. Most of the times however, the interest in keeping some information confidential arises from the competitive advantage that it provides. Basically, any kind of undisclosed information which is of commercial value has to be protected under Article 39 TRIPs. This means that technical and commercial knowledge alike will benefit of that protection.

Possible Trade Secrets

- **Business Related**

  Business strategies and plans, selective models of operations,marketing plans; clients lists, financial information, personnel records; work flow processses / schedules

- **Technical Related**

  R&D strategies and plans, Manuals, Designs, Formulae and know-how for producing products;
  - Manufacturing or repair processes, techniques and raw materials and specifications;
  - Drawings, Models, Prototypes blueprints and maps; Algorithms and processes that are implemented in computer programs, and the programs themselves; Architectural plans, Data compilations, proprietary databases and instructional methods; Document tracking processes.

[8] See for example Dr. François Dessemontet, "Protection of Trade Secrets and Confidential Information", http://www.unil.ch/webdav/site/cedidac/shared/Articles/Protection%20Trade%20Secrets.pdf

Table 1 Some examples of confidential information

(Source: "Leveraging Business / Trade Secrets for Competitive Advantage: Examples and Case Studies")

It is difficult to find concurring opinions in the doctrine regarding the terminology. Most confidentiality agreements that have been examined for the purpose of this study aim at protecting "trade secrets and other confidential information". The dichotomy between the two categories is not very clear since, as shown also by Table 1 trade secrets are broadly defined. Trade secrets may comprise "*any information, including but not limited to technical or non technical data, formula, pattern, compilation, program, device, method, technique, drawing process, financial data, or a list of potential customers or suppliers*"[9]

Examining some national applicable laws may provide useful guidance:

In **Italy**, the terms "trade secrets" and "know-how" are used interchangeable and they encompass commercial, industrial and technical information which is secret, not patented, and which "rise above the level of information which is merely confidential, i.e. it has value and the requisite level of novelty in the meaning that it is not readily accessible by the competitors"[10]. Article 14 of the Decree 198/1996[11] refers generally to "business information" including "commercial information lawfully within a competitor's control" without distinguishing different degrees of confidentiality afforded by different types of commercial information. The case law

[9] see "The legal protection of trade secrets" , article published by IPR Helpdesk at: http://www.ipr-helpdesk.org/documentos/docsPublicacion/pdf_xml/8_LegalprotectionofTradeSecrets%5B0000002422_00%5D.pdf

[10] See Elena Ossipova & Fadwa Eltayeb, "Trade Secrets", available at: http://www.wipo.org/academy/en/research_pub/papers/Turin2001/pdf/ossipovaetal.pdf

[11] Article 14 of the Industrial Property (TRIPS), Decree, 19/03/1996, No. 198 reads:

1. The following article shall be inserted after article 6 of Royal Decree no. 1127 of 29 June 1939, as subsequently amended:

'Article 6-bis. -

1. Without prejudice to the provisions of article 2598, no. 3, of the Civil Code, the disclosure of business information to third parties, including commercial information lawfully within a competitor's control, or the acquisition or use of such information by third parties in a manner contrary to fair professional practices shall constitute an act of unfair competition, where the said information:

a) 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 or readily accessible to experts and operators in that sector;

b) has commercial value because it is secret;

c) is subject to reasonable steps under the circumstances, by the persons lawfully in control of such information, to keep it secret.

2. Disclosure to third parties of test data or other secret data, the processing of which involves a considerable effort, or the acquisition or use of such data by third parties in a manner contrary to fair professional practices, where the submission of such data is a condition of approving the marketing of chemical, pharmaceutical or agricultural products utilising new chemical entities, shall be also considered an act of unfair competition.' (see http://www.wipo.int/clea/en/fiche.jsp?uid=it024 for the full text of the Decree).

however[12] made use of criteria such as the "ability to keep in memory" the relevant information in order to distinguish between the employees own professional experience, as accumulated during employment (which can freely be used after employment period has elapsed) and trade secrets that "belong" to the employer and thus cannot be disclosed without his authorization.

Norway on the other hand refers in Section 7 of the Marketing Control Law to "trade secrets" (*Bedriftshemmeligheter*)[13] prohibiting the unlawful use of a trade secret that was obtained due to employment or trust or as part of a business relationship.

In **Spain**[14], it is the rightful holder of the information who has the faculty of designating as confidential any document or information that according to his best judgment is commercially relevant. Such documents or information may comprise business strategies, know-how, contracts entered into, intellectual property, patents and plans for new products.

A similar situation is to be found in **France,** however the doctrine distinguishes more clearly between trade secrets (secrets de fabrique[15]), know -how ("savoir faire[16]") and other confidential business information. While the know-how can be transmitted to those willing to pay for it (and who would therefore have no interest in revealing it further), the trade secrets have to be kept secret if they are to benefit

---

[12] See for example: G. and M.Pizzi v.M.Tiezzi (1998), Trib. Di Modena 26 Marzo 1998, in *Giurisprudenza annotata di diritto industriale*, 1998, 3912.

[13] See The Marketing Control Act - Act No. 47 of 16 June 1972 relating to the Control of Marketing and Contract Terms and Conditions (Lov om kontroll med markedsføring og avtalevilkår (markedsføringsloven) LOV-1972-06-16-47) available at: http://www.lovdata.no/all/nl-19720616-047.html .In English:

"Section 7 **Trade secrets:** A person who has gained knowledge or possession of a trade secret in connection with a position of employment or trust or with a business relationship must not use the secret unlawfully in the conduct of business.

The same shall apply to any person who has gained knowledge or possession of a trade secret through breach by another person of his or her professional secrecy or otherwise through the unlawful act of another person"

[14] See María González Moreno de Manaca Consulting, S.L , "La importancia de la Protección de la Información Corporativa.Los Acuerdos o Pactos de Confidencialidad : "el empresario tiene la libertad de calificar como Confidencial, cualquier documento o información, que a su juicio, influya directa o indirectamente en el desarrollo del negocio: estrategias empresariales, métodos de negocio, documentos contractuales, propiedad intelectual, patentes, desarrollo de nuevos productos, etc.."

[15] Comme l'a écrit le Doyen ROUBIER (de la Faculté de Droit de Lyon) :"le secret de fabrique implique que la connaissance qui en forme l'objet ne soit pas à la portée de l'homme du métier et ne fasse pas partie des éléments qui doivent être connus de la généralité des personnes compétentes en la matière". http://www.progexpi.com/htm30.php

[16] habileté manuelle communicable", tout au moins communicable à des individus capables de l'assimiler. "Connaissances techniques, transmissibles, non-immédiatement accessibles au public et non-brevetées, et pour lesquelles quelqu'un serait serait disposé à payer pour en avoir connaissance ". See http://www.progexpi.com/htm30.php for more details.

form any legal protection or have value at all. The Labor Code contains in article L152-7[17] a prohibition to reveal trade secrets.

Article 26 of the Labour Code in **Romania**[18] stipulates that the employment contract has to contain express provisions regarding the information to be treated as confidential among the parties. The leader of the legal person can draw up lists of information that are to be included under the umbrella of professional secrecy[19].

Finally, the jurisprudence in **UK** led to the definition of different standards of protection for confidential information. For a duty of confidentiality to arise, the information:

- in itself must have the necessary quality of confidentiality (must not be known within the particular professional circle)

- must have been imparted in circumstances importing an obligation of confidence (must have been given in confidence)

- must have been used in an unauthorised manner (the confidence must have been broken)[20].

Lang (2003)[21] quotes the views of the Law Commission in 1997 regarding the criminalisation of trade secret infringements and identifies 4 categories of information susceptible of being included in the definition of trade secrets, and thus protected by confidentiality: formulae for highly specific products; technological secrets, strategic business information and collations of publicly available information (databases). Case law supports this view[22], trade secrets differing from "other confidential information" through their use in trade or business (as opposed to personnel files or medical records that need to be kept confidential although they do not ensure a competitive advantage), through the fact that they are subjected to special protection against widespread dissemination. Moreover, the person to whom they are communicated with the permission of their rightful holder cannot use them for the benefit of someone else than the rightholder even after the contractual relations (employment or otherwise) have ended.

Underlining the diversity in the criteria that can be used for the definition of confidential according to different applicable laws emphasises that the TrustCom contractual arrangements among the VO partners need to be flexible enough to accommodate their own confidentiality policies. Simply providing for "the protection

[17] Introduced through Law n° 92-1336 from 16.12.1992 art. 236, published in "Journal Officiel" of 23.12.1992 in force from 1er mars 1994.

[18] Law nr. 53/2003, published in the "Monitorul Oficial" nr.72/2003, available in Romanian at: http://www.dsclex.ro/coduri/cm.htm

[19] article 7 of Decision nr. 585 from 13 June 2002 regarding the National Standards for the Protection of Classified Information in Romania, published in Monitorul Oficial nr. 485/ 5 July 2002

[20] Coco v. AN Clark (Engineers) Ltd.[1969] FSR 415.

[21] Jon Lang: The protection of commercial trade secrets, [2003] E.I.P.R issue 10, p.462 – 471

[22] see Lansing Linde Ltd. v. Kerr, [1991] 1 W.L.R. 251

of confidential information" will not necessarily ensure that the partners will assume the same level of protection to the various sensitive documents or specifications. The protection afforded by law to confidential information can theoretically last forever (as opposed to the temporary patent or copyright protection), provided their secrecy is maintained.

3.1.2 Requirements pertaining to the access procedures involving confidential information

The final requirement for information designated as confidential to benefit from legal protection against unlawful disclosure or use is, according to article 39.2.c of the TRIPs Agreement that it is "*subject to reasonable steps… to keep it a secret".*

Unlike for patents, there is no automatic protection for trade secrets following a registration by an administrative body, since trade secrets are not subject to the grant of a title by the Patent Office or any other office.

From this point of view, the trade secret protection is more limited, in the sense that a third party which develops independently the same technology cannot be prevented to use it, even against competitors who did get hold of the trade secrets in a derivative way from the original owner. Therefore, adequate access control policies are a must.

Due to the fact that trade secrets are not registered, the costs involved in the protection of trade secrets stem mainly from the requirement to put in place an information security and protection policy and program in the company as well as from monitoring, surveillance, audit and legal measures against those who breach or try to breach the security system. So long as a company has made systematic efforts that are considered reasonable under the circumstances to preserve confidentiality or secrecy, legal remedies are available in case of misappropriation of almost any kind of information of competitive value.

In practice, a trade secret holder may still spend considerable effort and financial resources protecting the trade secret. The efforts are well worth exceeding the "reasonable care" requirement since the goal of a business enterprise is to avoid disclosure and subsequent loss of the trade secret rather than the minimum actions needed to prevail in a trade secret misappropriation lawsuit after destruction of the secrecy due to disclosure.

Some criteria that have been put forward in the literature[23] in order to determine if **reasonable efforts** were made to keep the access to the confidential information restricted on a need to know basis, are:

- the existence of an adequate program to ensure secrecy;

[23] Andrew Beckerman-Rodau Trade Secrets - The New Risks to Trade Secrets Posted by Computerization, published by Suffolk University Law School, available at:

http://lsr.nellco.org/cgi/viewcontent.cgi?article=1000&context=suffolk/ip

- the amount of resources invested by the company in the program meant to ensure secrecy (may suggest good faith even in case it failed to reach its goal);
- the limited access to the facilities where the information is stored or located;
- the means used to avert the employees that they are dealing with confidential information
- the compliance with existing industry standards or codes of practice

3.2 Terminological distinctions

This section is meant to introduce some basic distinctions between confidentiality and related notions.

3.2.1 Confidentiality and secrecy

A relation based on confidentiality ensures only a relative secrecy of certain information. If A is the rightful holder of some documents, he may choose to keep them only for himself (secret) or entrust them also to B under an agreement of confidentiality preventing B to communicate it further to C. At the same time, C cannot use unfair competition means to find out the information from either A or B, but nothing prevents him to conduct research and find it on its own effort.

However, once the information becomes common knowledge in the field (either because A releases it or because D discloses it) B is not bound by the confidentiality agreement even if its term has not elapsed yet. Therefore he can use and trade that information freely.

3.2.2 Commercial confidentiality and privacy

Although both of the notions describe a situation of limited access to information, the nature of the information as well as the values thus protected differ. Privacy is a right guaranteed to the individual with respect to personal information ensuring his integrity as a human being, autonomy, attentional self- determination. Commercial confidentiality, the focus of this study, targets that information used in trade and affording to the rightholder a competitive advantage and protects the effort invested in research or analysis.

3.2.3 Confidentiality as part of information security

In a legal perspective confidentiality is a binding relation that constrains the behaviour of the humans dealing with some types of information. That binding relation can be consensual (the result of a contractual agreement) or imposed by law (where the law imposes on certain professionals obligations of confidentiality). From the perspective of information security, confidentiality is an intrinsic property of the system, requiring that only those designated to have access to the system can enter the system.

In a legal perspective, we are interested not only in finding out the treatment that confidential information is to receive (access based only on authorisation) but also what kind of information can be designated as confidential, how is that designation to be made, what kind of rights it ensures and what remedies are available once this information is unlawfully disclosed to unauthorised parties.

4 Legal protection

The legal protection of confidential information is ensured through a mixture of statutory obligations, contractual means and criminal measures.

4.1 Contractual means

Most of the time a duty not to disclose confidential information stems from a contractual relationship between the rightful holder of a trade secret and the person(s) to whom the trade secret is disclosed. Due to the fact that the limited availability to the confidential information is a prerequisite for their legal protection, the disclosure occurs under strict terms regarding its access, use followed by destruction or restitution.

The confidentiality or non-disclosure agreement represents the agreement reached between the rightful holder of the confidential information and a receiver, in which the two parties decide on the information that is to be regarded as confidential, the scope of their mutual obligations and the time period in which confidentiality obligations subsist. Section 5 of the main report provides detailed explanations regarding the terms and conditions to be found in such an agreement.

While it can be a stand-alone document, the non-disclosure agreement is rarely the only contract governing the business interactions between the parties. Smaller operations, where the amount of confidential information exchanged is limited, or is not the main asset involved in the trade do not even require a stand-alone act dealing in detail with the scope of the parties' confidential exchanges. It would be enough to have a confidentiality clause in a broader collaboration or employment contract.

Larger operations involving numerous informational assets require in addition to a very broad collaboration agreement (a licensing agreement, a commissioning agreement, consultancy, joint-venture, partnership) a non-disclosure agreement expressing the agreement on the partners' management and security standards regarding the confidential information exchanged. Similarly, if the field of activity or the position requires it, in addition to the employment contract (that could make a short reference to the employee's obligation of confidentiality towards his employer) the parties may enter into a separate confidentiality agreement that defines in detail the scope of the employees' obligation of confidentiality.

In that sense, the non-disclosure agreement can be regarded as an auxiliary act of the collaboration, an act that guarantees rights and imposes obligations that may survive even after the collaboration between the parties has ended (See Section 5.2.1 for details). Contractual arrangements do not stop the infringement; however they create rights and provide the legal basis and mechanisms for redress in case adequate remediesfor infringements need to be insured. Contractual provisions must certainly be doubled by more active prevention mechanisms. But if these technical measures fail, the contract is to be enforced *ex-post* (after the unlawful act took place).

While they ensure legal certainty regarding the obligations of the contractual partners, the contractual means of protection of confidential information offer limited or no protection at all in case a third party is at the origin of the disclosure. Not only the contract between A and B cannot be invoked when C is the one responsible for the confidentiality loss, but once the information reaches public domain because of C (absent a behaviour contrary to honest commercial practices), the confidentiality agreement will have no value since either of the parties will be able to use the information as they please.

4.2 Statutory obligations of confidentiality

Such obligations of confidentiality are imposed by law or by statute on certain professionals by virtue of the field in which they act. "Professional secrecy" constrains the behaviour of doctors, psychologists, lawyers to maintain confidential the information they receive from their patients or clients, even though a confidentiality agreement is not signed each time. Similarly the information supplied to the Inland Revenue[24] , information supplied to the Child Support Agency, etc is to be kept confidential.

Moreover, national laws[25] may regard the obligations of confidentiality of the employees as obligations intrinsic to the employment, and therefore not require reference to express clauses of confidentiality in the employment contract.

The common law doctrine of "breach of confidence"[26] finds a "duty not to disclose information" in the specific circumstances in which the information was received which would make it unacceptable for the receiver to disclose the information in a way the giver has not authorised, even if the agreement in this regard is lacking. Such an exception can be invoked in order to deny access to certain information where there is "*a justifiable need or desire on the part of the giver of the information to keep the information confidential, e.g., if disclosure of the confidential information might cause substantial detriment to the giver, or to the giver's commercial interests*".
Similarly, confidentiality is a part of a fiduciary relationships (eg. doctor-patient, solicitor-client, employee-employer) that the fiduciary must keep confidential any confidential information given or obtained, unless there is express or implied consent to disclosure[27]. The same notion can be found in the Swiss law of trade secrets[28]. For employees, the Swiss Code of Obligations specifies that they have to

[24] See section 182 of the Finance Act 1989 and section 6 and Schedule 1 to the Taxes Management Act 1970 in the UK

[25] See for example " Estatuto de los Trabajadores" (work duties), article 5 in Spain. In opposition, the Romanian Labor Code (Codul Muncii) requires that the confidentiality clause be express in the work contract in order for an obligation to arise.

[26] See Information Sheet - Breach of confidence exemption (s.46(1)(a) of the Freedom of information Act), Office of the information commissioner, UK

[27] See Tate v Williamson [1866] LR 7 Ch App 55 YB 02.589 at 61

[28] See François Dessemontet, op.cit.

keep the trade secrets of their employer, notwithstanding the absence of a mention to that effect in the employment agreement[29] or in the dealership agreement[30] .

4.3 Criminal sanctions

A trade secret misappropriation may also attract criminal liability for the perpetrator. This may prove useful where there is no contractual or implied (statutory) obligation of confidentiality on the perpetrator. In most of the cases, the acts undertaken in the course of acquiring the trade secrets of another might represent criminal offences like burglary, fraud, illegal access[31], illegal interception[32] or data interference[33].

Although the criminal sanctions, such as fines on imprisonment do not actually compensate the rightful holders of confidential information for their loss, it is no less relevant that they outlaw and serve as a disincentive for certain behaviours that result in a loss for a rightful holder.

[29] Art. 321 a al. 4 Swiss Code of Obligations

[30] Art. 418 d al. 1 Swiss Code of Obligations

[31] According to article 2, Title 1 of the Budapest Convention on Cybercrime, illegal acces represents ”the access to the whole or any part of a computer system without right” possibly ”committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system”

[32] According to article 3, Title 1 of the Budapest Convention on Cybercrime, illegal interception represents the intentional ”interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data”.

[33] Data interference (according to article 4, Title 1 of the Budapest Convention on Cybercrime) represents the intentional “damaging, deletion, deterioration, alteration or suppression of computer data without right” possible resulted in serious harm.

5 Confidentiality agreements

We have analysed in the previous section the means through which VOs can ensure legal protection of confidential information. It was pointed out that business partners whishing to participate in such exchanges, prior to any disclosure of confidential information, enter into confidentiality agreements. These agreements can be reached between businesses or between an employer and an employee..

In addition to stating expressly the rights and the obligations of both the partner entrusting information and the partner to whom they are entrusted, these agreements give also indication of the presence of the sensitive information being exchanged and might even serve as a disincentive to recklessness leading to disclosure.

This section aims at looking into the statutory norms and the business practice in selected jurisdictions in order to illustrate the typical clauses of a non disclosure agreement as well as the rights and obligations guaranteed to the contractual partners, and just as important, the limits of their applicability and enforceability. The selected issues will call attention to legal requirements for confidentiality policies in the TrustCoM framework.

Depending on the nature of contractual relation envisaged by the parties (employment, collaboration, outsourcing, etc), confidentiality clauses can be incorporated within larger and more general agreements, such as employment contracts or collaboration agreements or can represent agreements per se, usually known as CONFIDENTIALITY or NON-DISCLOSURE AGREEMENTS (NDAs). These agreements describe in more detail the scope of the obligations of confidentiality assumed by the parties.

In the event of a legal action for trade secret misappropriation and absent a clear designation of confidential information, the court will examine as a minimal requirement whether or not there is at least a confidentiality clause in the agreement between the rightful holder of the information and the party to whom it is disclosed. This would represent an indication that the right holder took at least “reasonable steps” to maintain that information secret.

5.1 Typical clauses

5.1.1 Identification of the parties

Just like any contract, a non-disclosure agreement identifies firstly the parties to which the contractual provisions will apply. Since an implied obligation of confidentiality exists only in limited cases,[34] and the rightful holder of the

[34] See Section 4.2 of this Deliverable

confidential information can only claim his rights against those bound to confidentiality towards him, it is very important to identify those parties from the start.

The contractual provisions of an NDA apply first and foremost to the parties entering the agreement (The HOLDER and the RECEIVER of the confidential information). They will also appear as the signatory parties of the agreement.

However, parties may choose to extend the provisions of the confidentiality agreements to "affiliated companies", as defined in the national law, including for example companies or corporations that are directly or indirectly controlled by one of the parties, a company or corporation that directly or indirectly controls a party, or a company or corporation that is directly or indirectly controlled by a company or corporation that also directly or indirectly controls one of the parties.

Since these companies or corporations are not *per se* part of the initial agreement, it can sometimes be difficult to qualify them either as parties bound by the agreement or as third parties to whom the confidentiality obligations will not apply. A differentiating criterion might be the extent to which one of the signatory parties had the legal (as in the case of subsidiaries or daughter companies without legal personality) or practical ability (as in the case where it holds a majority of shares) to control or supervise their activity or access control policies.

5.1.2 Definitions of relevant terms

The parties should be able to clearly identify what they mean by "***confidential information***". Depending on the applicable law, this could be done through express listing of the information (or subject matters) that is to be regarded as confidential, or through describing the way the information is to be marked as confidential. The latter approach is especially useful in cases where new confidential information is created and disclosed to the other party after the entry into force of the agreement.

Depending on the particular context in which the agreement is reached, the definition may or may not include also "negative know-how", that is the information regarding failures in production processes, incomplete or erroneous data, irrelevant or unfavorable factors, that is information about "how not to do". This will prove relevant for example in the TrustCoM's CE scenario where the confidential information exchanges among the VO partners are highly dynamic and dependant on the results of the simulations and conclusions of the analysis reports performed.

It is also advisable to state the circumstances in which, irrespective of the nature of information exchanged, confidentiality obligations do not exist. They can refer to Information, knowledge, data and/or know-how which are:

- already known to the receiving party at the time of the disclosure;

- publicly known without the wrongful act or breach of the confidentiality agreement by the receiving party;

- rightfully received by the receiving party from a third party on a non-confidential basis;

- approved for release by written authorization of the disclosing party;

- required to be disclosed by law or judicial action;

- independently developed by employees or affiliated companies of the receiving party without any knowledge of the disclosure that is about to be made.

Some confidentiality agreements provide that confidential information may be included also in oral communications; however national legislation has to be checked in order to see whether or not this provision could be enforced in the end.[35]

Other terms might also be defined, such as "affiliated companies", "subject matter of information", "authorized person" (it is possible to indicate just the contractual provision that stipulate the access authorization policies). It would be better for the certainty of the rights and obligations assumed to consensually define more terms than to leave their interpretation to the general principles regarding the interpretation of the contacts, normally dependant on the provisions of the applicable law.

5.1.3 Rights and obligations

The most extensive part of an NDA addresses the rights and obligations of the contractual parties. The content as well as the degree of enforceability of these clauses are dependant on the chosen jurisdiction, however the typical obligations entailed by a confidentiality agreement are:

5.1.3.1 The obligation not to disclose

The commercial value of confidential information (be it trade secrets, know-how or other confidential information) stems from their secrecy. Their legal protection is conditional on their limited availability. Therefore, the party with whom the confidential information is shared has to agree not to disclose them without the authorization of the rightful holder. In case both contractual parties exchange confidential information, this obligation is reciprocal.

In employment contracts, such an obligation could be seen as part of the employees' obligation to professional secrecy and good faith towards the employer and some jurisdictions would recognize such an obligation even if it is not stated expressly in the contract[36].

In business contracts however, where the parties do not owe each other anything that is not agreed to[37], it would be safer to state expressly the duty not to disclose. This is especially relevant in the pre-contractual stage. During negotiations, the parties need to share certain information relevant in assessing the other's availability, competence, expertise in fulfilling the collaboration objectives. Since at

---

[35] In Romanian law, such provisions would typically not be enforceable (Article 26 of the Labor Code).

[36] See for example the English Law. On the other hand, in the Romanian law, it is compulsory to have a duty of confidentiality stated expressly in the employment contract if such an obligation is to apply.

[37] In the limits of fair competition

this point the outcome of negotiations is uncertain (it is uncertain if the parties will become contractual partners), it is recommendable for parties to agree at this early stage on the procedures involving each other's confidential information.

Although one party cannot force the other to disclose certain sensitive information during negotiations[38] all it is said at this point needs to be true, otherwise the party that was "tricked" by the false allegations of the other party may declare the contract null and void.

Since the main interest protected through non-disclosure is the secrecy of confidential information, this obligation lasts for as long as the information is still secret. If a third party (other than an "affiliated company") is at the source of the disclosure and the information reaches public domain, there should be no further constraints on the receivers that were previously bound to confidentiality. They would be free to disclose or use the misappropriated information[39] (though the decrease in its value is obvious having now reached public availability).

Even in such a case, the initial holder of the information may ask from its contractual partner to notify his intention to disclose or use the information that was otherwise part of the confidentiality agreements reached.[40]

It is possible that the confidentiality agreements itself be protected by a duty not to disclose[41].

When disclosure of certain information seen by the parties as confidential is imposed by judicial or state authorities as part of legal proceedings, it is possible for parties to agree on a notification procedure and to require support in contesting such procedures (where possible)[42] in addition to the notification.

5.1.3.2 The obligation to use for determined purposes

This clause can be stipulated either as a positive obligation (to use only for determined purposes) or as a negative obligation not to use for certain purposes (the others being allowed). As a rule, and as an obvious consequence of the first

---

[38] This assertion is true in the limits of what will be explained in the next section as disclosure that vitiates the contract (there are certain information that have to be disclosed by the parties and cannot be hidden by claming confidentiality).

[39] See Dr. François Dessemontet, op.cit.

[40] for example, "Recipient shall have no obligation under this Agreement with respect to Confidential Information which is or becomes publicly available without breach of this Agreement by Recipient; is rightfully received by Recipient without obligations of confidentiality; or is developed by Recipient without breach of this Agreement; **provided, however, such Confidential Information shall not be disclosed until thirty (30) days after written notice of intent to disclose is given to Owner along with the asserted grounds for disclosure**."

[41] for example the parties agree that "all matters relating to the existence and content of this Agreement are confidential and agrees that he shall not disclose such matters to any person or entity except his counsel, financial advisors and immediate family, but only if those individuals agree to keep such matters confidential"

[42] for example "If A receives a subpoena or other legal process seeking disclosure of Confidential Information belonging to B, A shall immediately notify B and cooperate fully with B in contesting such disclosure."

obligation, the receiver will have the obligation not to copy, not to make available, reproduce, or use for commercial purposes for his own interest or for others the information imparted in confidence. Depending on the objectives of collaboration, these obligations may differ from a confidentiality agreement to the other. Therefore, we cannot provide a list of "possible allowed uses". The TRIPs Agreement outlaws any use "contrary to honest commercial practices"[43].

Several situations could be distinguished: Considering that B receives in confidence from A confidential information, B cannot use for himself or for the benefit of a third party A's confidential information, even if B incorporates it into a more extensive product or analysis that it performs for a third party.

Furthermore B has to make available that information to its employees only on a need to know basis, in accordance to the roles assigned to them in fulfilling the purpose of the collaboration. This implies that if other units of B that did not have access to A's confidential information independently discover the same information (duplicates or reaches similar conclusions) regarding a compilation of data in a database, a market forecast, a product, a method of production, etc. the existent confidentiality agreement between A and B will not impede B to use as he sees fit (including through making it public) this information. Reverse engineering or independent derivations are not seen as improper means of handling confidential information[44]. B will have to make sure that in the event of legal proceedings brought by A against him, he will be able to prove the severability between the research conducted by the two teams.

The obligation "to use only for determined purposes" has also another dimension. It imposes on an employer a duty not to encourage or otherwise determine a new employee to use for his benefit confidential information belonging to the former employer. According to the TRIPs Agreement (art.39), this situation is seen as a dishonest commercial practice, both for the employee himself (since he infringes someone else's confidentiality rights) and for the employer ("inducement to breach"). Although the direct infringer is the employee, the employer's liability could be engaged if such an "inducement to breach" is proven.

In order to prevent this liability, the confidentiality agreement reached between the employer and the employee could include a clause stating that the employment relation does not and will not breach any agreements with or duties to a former employer (in case the employee is bound by a non-competition clause still active from the previous employment).

Moreover, the contract could state that the employee or the business partner will not disclose or use confidential information belonging to others and will not bring on the premises of the company confidential information belonging to someone else unless that party consented to it in writing.

---

[43] footnote 10 connected to article 39 of the TRIPs Agreement describes as "a manner contrary to honest commercial practices" at "least practices such as **breach of contract, breach of confidence and inducement to breach**, and includes the acquisition of undisclosed information by third parties who knew, or were grossly negligent in failing to know, that such practices were involved in the "acquisition" (emphasis added).

[44] See "The legal protection of trade secrets", article published by IPR Helpdesk, op.cit.

5.1.3.3 The obligation to take measures to protect the confidential information received

Article 39 of the TRIPs Agreement states that one indication that the rightful holder wishes to keep certain information confidential is the fact that he takes "*reasonable steps… to keep it a secret"*. When the disclosure of such information to selected business partners is dictated by commercial reasons, the secrecy requirement is transferred to the business partner, who has not only the obligation "not to disclose" himself but also to take measures to hinder or better yet to impede unauthorized access to the information entrusted by the other. The measures could be both legal (contracts) and technical.

The parties could negotiate on one or more of the following clauses:

- the obligation to implement a certain security system for the protection of confidential information;
- the obligation to ensure the same standard of protection for the confidential information received from the contractual partner as for his own confidential information;
- the obligation to impose confidentiality obligations on the employees of the receiver (to have the employees sign confidentiality agreements)
- the obligation to keep the confidential information from different business partners in different locations
- the obligation to notify when a confidentiality breech has occurred and to disclose the identity of the infringing party.

Therefore, before signing a confidentiality agreement, it would be prudent to investigate the recipient's practices in maintaining secrecy of its own information. If those practices are substandard or even nonexistent, and still the rightful holder wishes to do business with that partner, the confidentiality agreement should contain specific provisions concerning the standard of protection for its information and become involved in the receiver's definition of access to confidential information policies.

5.1.3.4 The obligation to return or destroy the documents referring to the confidential information upon completion of the tasks

Since the confidential information is disclosed by the rightful owner in strict connection with the other party's performance of specific tasks, once these tasks are fulfilled it is common to request the return or the destruction of the "documents" making reference or otherwise incorporating them. The practical manner in which such an obligation will be executed depends on the medium in which confidential information is embedded. This involves also a progressive and dynamic access management and monitoring in accordance with the different phases of the project.

When paper documents or otherwise tangible goods contain confidential information it may be more convenient to request their physical destruction. The receiver may additionally be placed under an obligation not to duplicate such documents or goods and moreover, to provide a certificate attesting their destruction within an agreed period of time. Although these clauses will not de facto impede the receiver to act in bad faith, including them in the agreement would

provide additional safeguards to the rightful holder of the confidential information once an infringement took place. He will be able to point out exactly the contractual provision that was not respected as well as the receiver's untruthful declaration.

When the confidential information is in electronic format, the security system put in place by its rightful holder will carry the burden of ensuring that the receiver is no longer able to get access to it or further use it or incorporate it into work done for his own interest or for a third party's.

It may be more difficult to deny the access or obstruct the access to confidential information once it is incorporated into oral communications (in those legislations or business sectors where such an approach is allowed). It is obvious that the receiver or his employees cannot be constrained to forget the information they came across during the fulfillment of their duties. It will be therefore a matter of narrowly defining the notion of "confidential information" and listing those data cannot be interpreted as "professional expertise". Information designated as confidential should be sufficiently novel and stand-alone to be susceptive of a special treatment: the absolute prohibition of its use outside the specific duty for which it was disclosed, even after the end of the business relations and regardless of the employee's ability to memorize it.

5.1.4 Other clauses

In addition to the contractual clauses that guarantee the above analyzed rights and the corresponding duties, a confidentiality (non-disclosure) agreement may contain also other provisions that pertain more to the management of confidentiality rights than to the rights they confer.

5.1.4.1 "No implied license" clause

This clause provides further guarantees for the rightful holder against the misuse of information imparted by him in confidence. It basically states that nothing contained in the confidentiality agreement is intended or shall be construed as conveying to the respective other party any license, intellectual property rights or other rights in the information imparted. The rightful holder reserves all rights to the disclosed information, in particular the right to apply for patents and other protective rights. The receiver has therefore only the right to temporarily use it for specified purposes and cannot profit from the use of that knowledge outside the terms of the confidentiality agreement.

5.1.4.2 Severability

The severability clause ensures the relative independence of one contractual clause towards the other. In contract law, there are cases in which the nullity of one contractual clause invalidates the whole contract. If the contractual clauses are severable one from the others, the fact that one or more provisions become fully or in part invalid, illegal or unenforceable under any applicable law will not affect the validity, legality, and enforceability of the remaining provisions. Invalid, illegal or unenforceable provisions could be replaced by provisions which best meet the purpose of the replaced provisions. The same applies in case of an omission.

5.1.4.3 Jurisdiction and choice of law

The purpose and the principles of jurisdiction and choice of law clauses has been explained in detail in another TrustCoM Deliverable[45]. In this context it is just worth pointing out the importance that such a clause exists (considering especially the conceptual differences among the definitions of "confidential information")

5.1.4.4 Article published based on research, inventions

The parties will have to agree further on the dissemination of the research involving the confidential information, and decide whether or not academic publications might indirectly jeopardise its intrinsic secrecy. Most of the times, what is produced in the course of the contractual relations (for example analysis reports performed in relation or upon confidential information) belongs to the rightful holder of the confidential information. In very strict confidentiality agreements, further use of the results or the conclusions reached by the analysis team would be allowed only with the authorisation of the rightful holder[46].

5.1.4.5 Modification of contractual provisions

Considering that it expresses the consensus of the parties regarding the policies of access and use of confidential information, the Confidentiality Agreement will have to be mutually agreed according to a pre-approved procedure.

---

[45] see Appendix B of TrustCom Deliverable D15.

[46] One such strong confidentiality clause I came across in the literature is: "*In the event Employee desires to publish the results of Employee's work for Company through literature or speeches, Employee will submit such literature or speeches to the Board of Directors of Company at least 10 days before dissemination of such information for a determination of whether such disclosure may alter trade secret status, may be highly prejudicial to the interests of Company, or may constitute an invasion of its privacy. Employee agrees not to publish, disclose or otherwise disseminate such information without prior written approval of the Board of Directors of Company. Employee acknowledges that Employee is aware that the unauthorized disclosure of Confidential Information of Company may be highly prejudicial to its interests, an invasion of privacy, and an improper disclosure of trade secrets*".

5.2 Enforceability of the clauses

The issue of enforceability of the clauses in a confidentiality agreement arises when for one reason or another one of the contractual parties culpably does not fulfil his obligations. One of the general principles of law[47] is that agreements produce effects (that is, giving rights and imposing obligations) only to the contractual partners[48]. As such, the provisions of the confidentiality agreements can only be imposed on those that are parts of the agreement, for as long as the agreement is considered to be in force. Other parties- that somehow infringe the rights of a legitimate rightholder of confidential information while not being bound to confidentiality towards him- could be stopped from doing so through legal means (remedies) that lie outside the contract.

Three issues will be analysed within this section of the study:

- how long the obligations in a confidentiality agreement can last;
- remedies available for the legitimate rightholder of confidential information in case the infringement comes from a contractual partner;
- remedies available for the legitimate rightholder of confidential information in case the infringement comes from a third party;

5.2.1 Duration of confidentiality obligations

The rights and obligations arisen from a confidentiality agreement last all throughout the time period in which the main contractual relations between parties survive. For example, if the exchange or the disclosure of confidential information occurred within employment, the corresponding obligations last all throughout the duration of the employment relation. Similarly, if the disclosure of confidential information occurred as part of a collaboration or consultancy relation between two business entities, the above analyzed obligations survive all throughout the lifetime of this collaboration. In this respect, we may consider the confidentiality obligations as auxiliary to the main legal relationships between the parties (employment, collaboration…etc…).

In addition to this default rule, the parties may agree on instances in which the confidentiality obligations end prior to the termination of the main business relationships between them.

Similarly, the parties may agree on a period of time in which the confidentiality obligations survive after the main contractual relations ended.

---

[47] See for example Principles of European Contract Law (1995) available at: http://www.jus.uio.no/lm/eu.contract.principles.part1.1995/

[48] With some distinctions that are beyond the scope of this analysis.

Although the confidentiality agreement is still in force and the employment or the collaboration relationship still exists, the parties cannot escape their obligations towards the public judicial authorities or other authoritative administrative bodies in case these bodies would compel them to reveal certain information (that could otherwise *per se*, according to the agreement, be protected by confidentiality). The procedural requirements of such a state intervention differ from jurisdiction to jurisdiction. The important point to be noted is that confidential information can be revealed without the prior authorization of the rightholder if such an intervention occurs in accordance with the national law.

It was argued above that the confidentiality obligations exist as long as the information remains secret (so that the legitimate holder can benefit from its scarcity and use it as a commodity). However, depending on the parties' will, early termination of the confidentiality obligations can occur also due to the impossibility of one of them to fulfill its obligations in accordance with the terms of the employment or the collaboration agreement. The bankruptcy, receivership, assignment, attachment or seizure procedures for one of the parties, though do not lead directly to an impossibility for them to maintain confidentiality as agreed, may lead to an early termination of the confidentiality agreement.

If the parties consent to an extension of the confidentiality obligations beyond the lifetime of the main business relationships (when the goal of the collaboration has been attained) it is advisable that they specify the time period during which disclosures will be made and the period during which confidentiality of the information is to be maintained.

It is in the best interest of the party disclosing confidential information that it makes clear to the receiver, for example, that he is to maintain the confidentiality of the information received for X months (years) after its disclosure. In this case, the access policies for each of the confidential documents disclosed would have to be maintained and monitored separately, as the beginning and the end date of the confidentiality requirements will differ.

Another option would be to stipulate that regardless of the business relations in which the parties will find themselves in X month (years) from the entering into effect of the agreement, certain information disclosed (as defined) is to be kept confidential. In this case, the access policies will be active until that end-date, even if some confidential information is disclosed just a few days prior to that end –date.

In addition to the practical and technical implications opting for one solution or for the other, there are in general no constraints imposed by the national legislation regarding the time length of the confidentiality obligations. In case of a disagreement, if the parties were ambiguous about the duration of their obligations, the court will be called to apply its own criteria in determining a reasonable duration for the obligations assumed, which may be shorter that what the parties could get via negotiations.

5.2.2 Enforceability among the signatory parties

According to article 2.1.16 of the UNIDROIT[49] Principles of international commercial contracts (2004)[50], "*where information is given as confidential by one party in the course of negotiations, the other party is under a duty not to disclose that information or to use it improperly for its own purposes,* ***whether or not a contract is subsequently concluded****. Where appropriate, the remedy for breach of that duty may include* ***compensation*** *based on the benefit received by the other party" (*emphasis added*).*

Article 2.1.16 of the UNIDROIT Principles points out that regardless of the outcome of the negotiations, the parties owe each other confidentiality regarding the information exchanged at this point. All the more reason, when parties already agreed on the scope of their confidentiality obligations[51], they are entitled to remedies. What might those remedies be?

The main obligations owed by a party bound to confidentiality towards another are negative obligations (not to disclose, not to use for its own interest or for the interest of a third party). In this case, non fulfilment of obligations assumed via a confidentiality agreement would in fact represent illegitimate disclosure or to illegitimate use. Non fulfilment of obligations occurs as well when the receiver fails to return or does not destruct the confidential documents as agreed.

The first step to be made by a legitimate rightholder is **to notify** the contractual party in case that by the non fulfilment of obligations he is actually infringing its rights. The legal relevance of this notification may differ depending on the identity of the parties in the given case. In civil law relations (such as between an employer and an employee) the infringing party owes damages from this point onwards (from the date of the notification, and not necessarily from the date the infringement took place[52]). In commercial law, even if damages are owed directly from the date of the infringement, such a notification is no less important as it may constitute the turning point in the subjective position of the receiver of information. If up until now he could have claimed he took all reasonable steps in protecting the confidentiality of the information entrusted towards third party (that is he is in good faith), once notified he will be considered to be in bad faith if he does nothing to prevent further intrusions. Consequently, the amount of compensation to be paid would differ.

In practice, the extent of the damages awarded to the rightful holder of confidential information would depend on the nature and the extent of the prejudice he claims to have suffered. In case that prejudice is contested by the defendant, the plaintiff (in this case the rightful holder) would have the burden of proving both that he suffered a loss due to the behaviour of the other party and its extent. However, since as

---

[49] See http://www.unidroit.org/english/members/main.htm for a list of UNIDROIT's Member States.

[50] The full text of the Principles is available at:

http://www.unidroit.org/english/principles/contracts/main.htm

[51] This implies that the confidentiality agreement is validly concluded, for the circumstances in which non-disclosure vitiates the contract see Section 6 of this study.

[52] Of course, various national laws may differ on this point, so their provisions should be consulted on this particular issues.

discussed earlier in this study, the economic value as well as the competitive advantage conferred by holding confidential information is difficult to evaluate beforehand, proving that the prejudice is equivalent to a certain amount of money could be a cumbersome process.

Therefore it is advisable that the confidentiality agreement concluded by the parties includes a **clause of agreed payment for non performance**[53]**.** In this case, a party who does not perform is to pay a specified sum to the aggrieved party for such non-performance irrespective of its actual harm. Therefore, the rightful holder of information will be entitled to claim from the receiver the agreed sum of money whatever the extent of the actual prejudice he suffered[54].

5.2.3 Third party infringements

The third party commits an unlawful act only when he misappropriates the trade secret of another, and not when he invests resources and discovers it through independent means. With respect to the actions of third parties, the rights afforded by the confidentiality of trade secrets are frailer than those conferred by patents.

If the confidential information is embodied in an innovative product, it is legal for others to reverse engineer it and discover and use the secret. Trade secret protection of an invention in fact does not provide the exclusive right to exclude third parties from making commercial use of it. Only patents and utility models can provide this type of protection. Moreover, a trade secret may be patented by someone else who developed the relevant information by legitimate means.

Contractual liability cannot arise when the infringing party is not bound to confidentiality via a non-disclosure agreement. However, once a third party is responsible for the confidentiality loss, other remedies may become available in accordance with the national law.

For example, in those cases where there is a statutory obligation of confidentiality[55], the statute or the law governing the activity of the respective professional body will stipulate also the sanctionatory measures and procedures for those that do not respect the professional secrecy

When a platform such as TrustCom is involved, it is important to be able to monitor and to provide evidence of those elements that are considered by law or statute as relevant in documenting the unlawful act. Some of these elements are: the fact that the access or use was not authorised or excessive, the identity of the responsible party, the impact that the act had on the confidential document in cause (it was destroyed, it reached the public domain, or it was used for the benefit of the infringer or for that of a third party). These elements would be fundamental in both

---

[53] See article 4.508 of the Principles of European Contract Law as well as article 7.4.13 of the UNIDROIT Principles for International Commercial Contracts.

[54] However, despite any agreement to the contrary the specified sum may be reduced to a reasonable amount where it is grossly excessive in relation to the loss resulting from the non-performance and the other circumstances.

[55] see Section 4.2 of this Study

establishing the responsibility for the act and the extent of damages to be awarded as well as the legal base of the sanction towards the third party. Opposite from the contractual remedies in case of infringement where the parties could reach an agreement on the extent of the damages, the criminal sanctions will have to be imposed by a court of law.

As pointed out in Section 4, in addition to the contractual liability, confidential information may be protected through imposing criminal sanctions on the guilty party, in accordance with the national laws implementing Title 1 (Offences against the confidentiality, integrity and availability of computer data and systems) of the Budapest Convention on Cybercrime.[56]

[56] available at: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

6 Disclosure obligations

The previous chapters discussed non-disclosure as a right of one business to preserve the secrecy over certain sensitive information with strategic and commercial value. The disclosure of such information is optional, and those few business partners who do have access to it have to comply with restrictive conditions regarding their use and with an absolute prohibition of their disclosure to third parties. For example, the information exchanged by the parties during negotiations is to be kept confidential.

This chapter focuses instead on those few situations in which non-disclosure of certain information by the parties during negotiations may "destroy" the contract making it voidable and opening the possibility for the innocent party to claim damages. There is some information about itself (internally designated confidential information) that the organisations cannot hide from potential business partners under the umbrella of confidentiality, either in the negotiation- identification phase of the Virtual Organisation lifecycle or during the execution of the contracts/ operational phase. In this case, it is not the disclosure that is sanctioned by the law, but the non- disclosure. In such circumstances, the information cannot be hidden under the umbrella of confidentiality.

According to article 3.8 of the UNIDROIT Principles of International Commercial Contracts, "*A party may avoid the contract when it has been led to conclude the contract by the other party's fraudulent representation, including language or practices, or* ***fraudulent non-disclosure of circumstances which, according to reasonable commercial standards of fair dealing, the latter party should have disclosed."*** The nature of these factual circumstances can be different. In each case a court will have to assess their relevance in inducing the opposing party to enter the contract. It has to be proven that they were determining factors in the parties decision to enter the contract and that the other party willingly and knowingly has kept them secret.

However, if one party (A) asks the other (B) about such circumstances and that party (B) expresses its inability to disclose it due to confidentiality reasons, and still, the parties (A and B) agree to conclude the contract, it is understood that A will no longer be able to avoid the contract as he thus takes upon himself the associated contractual risks.

Another situation where non-disclosure can lead to the vitiation of the contract is where one of the parties has made a "relevant **mistake**[57]" at the time he decided to enter the contract. According to article 3.5 of the UNIDROIT Principles, "*a party may only avoid the contract for mistake if, when the contract was concluded, the mistake was of such importance that a reasonable person in the same situation as* ***the party in error would only have concluded the contract on materially different terms or would not have concluded it at all if the true state of affairs***

[57] Mistake is an erroneous assumption relating to facts or to law existing when the contract was concluded (article 3.4 UNIDROIT Principles)

had been known, and *[…] "the other party made the same mistake, or caused the mistake, or* ***knew or ought to have known of the mistake*** *and it was contrary to reasonable commercial standards of fair dealing to leave the mistaken party in error".*

In the first case, the non-disclosure of relevant facts actively "tricks" the party into entering the contract.

In the second case, one party is in error about certain facts and the other party either intentionally or by negligence does nothing to eliminate that error although he knew or ought to have known about it.

Both of these situations are seen as vitiating the consent given by one party in the conclusion of the contract. The party in error as well as the party that was "tricked" into entering the contract will be able to avoid the contract, meaning that it can request in court that the contract be seen as it has never existed, and even claim damages.

Using the TrustCoM CE Scenario, an example could be provided.

The reputation scores given by a company to its business partners and the internal policies involved in dealing with the business partner as a consequence of these scores are definitely information protected by confidentiality. They may even compel one company to refrain from doing business with certain business entities, although this is not necessarily one issue to put forward publicly.

If the CE VO is in error (either because its management does not know, or this fact was deliberately hidden from them) regarding the identity of one of the partners used by the TC-ConsEng in performing the analysis design (for example the identity of the TC- HPC), CE-VO may avoid the contract (that is exit from it) and look for another partner that does not rely on the services provided by a partner he does not like. He has this faculty since the identity of the contractual partner is a factor can influence the quality of the contractual obligations assumed by the analysis team and therefore is a determinant factor in the conclusion of the consultancy contract between CE-VO and the Analysis VO. CE-VO will have to prove that the TC-ConsEng either deliberately hidden the true identity of the TC-HPC or knew that CE-VO is mistaken about this fact and did nothing to eliminate the error.

In order to prevent the risks arisen form this uncertainty of the contractual relation, it is advisable that the confidentiality agreement signed by the parties during the negotiations includes a list of incompatibilities or preferences that the partners might have as well as other factors seen to be determinant in deciding to enter into the contract or not. Since this list would appear as a term in confidentiality agreement, secret in itself, the confidentiality concerns of the parties could be properly mitigated. If this option appears unsuitable in the concrete case, the parties should at least internally decide and then discuss during negotiations the parameters that they consider determinant in entering the contract, while keeping in

mind that they will have to bear the contractual risks for what has been discussed and agreed.[58]

[58] see Paragraph 4 of this Section.

7 Summary of Appendix A

The appendix to this report contains a legal risk analysis of the TrustCoM CE scenario. The appendix exemplifies, based on the CE scenario, how confidentiality issues may be proactively analysed and addressed. The objective of the case study is to analyse the risks related to confidential information in the CE scenario from a legal point of view and to identify means that can contribute to effective risk reduction.

The appendix is structured as follows: Section 2 synthesizes the storyboard of the TrustCoM CE scenario, which was the basis for this case study. Section 3 presents the methodology utilized in this case study. The analysis of the scenario is presented in the subsequent sections. Section 4 presents the risks; Section 5 discusses the different options to treat these risks. Section 6 and 7 respectively discuss how these risk treatments can be transformed into contract requirements and integrated into contract drafts. Finally, Section 8 summarizes the findings of this risk analysis as well as the findings of the main report in a check list of risks related to confidentiality issues.

The following Table 1 contains an overview of the identified risks and the relevant treatment options, concentrating on the non-disclosure clause in the respective contracts. The inclusion of the risk as well as its risk value and treatment measure in one table should allow some degree of traceability. Thus, the collaborators will be able to identify why a particular contract clause is suggested and they should be able to analyze whether the suggested treatment measure effectively reduces the value of the risk. Available treatments to the identified risks need to be assessed in a cost-benefit analysis, as discussed in Appendix A, Section 6.

	Con-sequence	Likelihood	Risk value	Treatment
Risk 1 **Distribution -> loss legal protection**	Major	Possible	Major	Avoid distribution to public through confidentiality clause
Risk 2 **Utilized by TC ConsEng for competing purposes**	Major	Possible	Major	Limit use to project related purposes
Risk 3 **Utilized by competitor**	Major	Possible	Major	Avoid distribution to competitor: confidentiality clause

Table 1 Risk and treatment table

The risks as well as the available treatment options are analysed in detail in the Appendix. The analysis indicates again that risks related to collaboration in a VO need to be addressed in an integrated manner, where legal treatments (specific contract clauses) need to be combined with more technical approaches like those developed in other work packages in the TrustCoM project. In order to ensure the usability of the results of this research, the main confidentiality risks are summarized in a checklist, which mentions examples from the analysed scenario.

8 Conclusions

This study identified what may legitimately described as confidential information, how that designation is to be made, what kind of rights it ensures and what remedies are available once this information is unlawfully disclosed to unauthorized parties. The analysis was conducted having the provision of legal input in the design and deployment of policies governing the access to confidential information in the TrustCom framework as a main goal. Therefore, the main part of this Deliverable provided a legal analysis of confidentiality while Appendix A tailored the identified legal requirements to the specificity of the TrustCom CE Scenario, as described in TrustCom Deliverables D 10 and D 41.

The law requires that a person lawfully in control of information it designates as confidential must have the possibility of preventing it from being disclosed to, acquired by, or used by others without his or her consent in a manner contrary to honest commercial practices.

As it can be concluded from Section 3 of the Study, technical and commercial knowledge alike can be designated as confidential, as long as it is:

- not common knowledge in the given field of activity or business (relatively novel);
- a business asset to the rightful holder (exploitable) provided it is kept secret;
- it was subjected to reasonable efforts to maintain it secret by the rightholder.

Confidentiality obligations can arise consensually (that is following an agreement between business partners or between employer and its employees) or be imposed by law. The agreement through which the parties decide on the scope and the extent of their obligations of confidentiality towards each other is called confidentiality or non-disclosure agreement. Section 4 analysed the role played by confidentiality agreements in the complex of legal measures supposed to safeguard the interests of the party disclosing confidential information.

Section 5 discussed in detail the provisions of confidentiality agreements. This part includes the most consistent part of the legal input regarding the possible content of the policies governing the access to confidential information in the TrustCom framework. Policy suggestions were provided in terms of:

- the definition and designation of confidential information (Section 5.1.2);
- the obligations that should be assumed by the parties for efficient access management and concrete issues that should be bore in mind in negotiating them(Section 5.1.3);
- the possible duration of the confidentiality obligations (Section 5.2.1);
- the limits on the enforceability of the contractual provisions among signatory parties and between them and external parties.

The usability of these policy suggestions in the TrustCom Context is exemplified by Section 7 of the Appendix A providing example clauses and Section 8 of the

Appendix A illustrating how contractual provisions can be used as contractual treatments in order to mitigate risks to confidential information.

Furthermore, Section 6 illustrated situations in which the parties have to disclose information about themselves since non-disclosure jeopardizes the validity of the collaboration agreement among them.

In addition to input to the design of policies governing access to confidential information, Appendix A of the study provides an updated methodology for identifying, estimating and evaluating risks to confidential information in the TrustCom framework and for using the contractual requirements as risk treatments.

The findings of the legal analysis carried out in the main report have been summarized in a risk checklist (Section 8 of the Appendix) that uses the legal risk analysis of the CE scenario as described in Appendix A in order exemplify risks to confidentiality in the proposed scenario.