WIPO

WIPO/IP/KYI/00/3
ORIGINAL: English
DATE: May 17, 2000

WORLD INTELLECTUAL PROPERTY ORGANIZATION
Kyiv

Seminar organised by the WIPO, the International Association of the Academies of Sciences and the National Academy of Sciences of Ukraine Kyiv 17-19 May 2000

Confidentiality in Technology Transfer Agreements

Prof. Ph.D. Arnold Vahrenwald
Vahrenwald & Kretschmer
Lamontstr. 25
D-81679 Munich
Telephone: +49-89-99.75.01.54
Telefax: +49-89-99.75.01.55
Email: arnold.vahrenwald@jrc.it

Contents

Introduction

Confidentiality clauses in technology transfer agreements serve to protect the proprietary nature of the technology. The drafting of the appropriate clauses can be essential for the maintenance of the value of the technology.

1. Confidentiality as a Means for the Protection of Technology

The role of confidentiality to protect technology increased during the recent decade. This is, in part, due to the rising costs of patent protection, whether concerning the grant of the patent or patent litigation. Another factor which favours confidentiality is the short life of innovations with an industrial application. The increase in competition has led to shorter periods within which new technologies can be exploited successfully. Thus periods of several years which may be necessary to obtain patent protection may be counteractive to the continuous innovation process.

The public interest in the communication of the patented technology has to be weighed against the public interest in the use of products and processes which employ new but secret technologies. If a system for the exploitation of new technologies under the regime of secrecy is more advantageous to a society than the operation of a patent system, the avoidance of the misallocation of resources demands the protection of secrecy. Such a protection can be afforded by the legal recognition of the validity and the enforcement of confidentiality clauses in technology transfer contracts.

2. The Protection of Secret Technologies

The confidentiality of technology can be protected in a variety of environments. In order to avoid the disclosure of new technologies at an early stage it is essential to oblige the personnel, to retain information which they obtained in the exercise of their duties confidential.

During the initial phase it should be avoided to release information about the new technology through its description. Thus any information relating to new technologies should be kept secret at a degree equivalent to that which is required in the case of an invention for which a patent will be applied for.

The improvements of information technologies may facilitate industrial espionage. Accordingly, measures have to be implemented to safeguard the confidentiality by appropriate technological means. These means should be implemented together with rules which bind the staff of the organisation which owns the technology and of the recipient to observe similar standards.

2.1. Which Technologies Can Be Protected by Confidentiality?

There is no inherent limit to the subject-matter of technological information which can be protected by secrecy. Whereas technologies, in order to attract patent protection, must be of industrial application, the secrecy may protect any technology which has a value for the owner.

However, there may be differences in national jurisprudence concerning the scope of the protectable technology. Generally, it has to be differed between technologies which appertain to an employer and the general skill which an employee acquired during the performance of his contractual duties. After the termination of the contractual relation, a non-competition clause may restrict the former employee from working in sectors of the trade or industry which use competing technologies. However, such clauses must not be in restraint of trade which means that they should be limited in time and/or territory.

Another borderline may have to be drawn between Confidential technology and information which is not protectable for reasons of the public interest. Accordingly, technologies obtained by criminal activities would not merit protection by confidentiality.

2.1.1. Technology

Secret technological information is generally differed from secret business information. The definition of the technology protected by civil or criminal law depends on the relevant applicable law. These definitions may vary, so that no general assumptions about the protectability can be made. The application of the EU Technology Transfer Block Exemption according to which clauses which might restrain competition can be permissible, requires, for example, that the technology must consist of a substantial and identified secret know-how.

2.1.2. Not in the Public Domain

Generally, technological information is protectable only if it does not belong to the public domain. The text which is applied in many legal systems is not the text of patentability, that is to say absolute secrecy, but 'relative' secrecy. Accordingly, it may suffice, if the relevant technology cannot easily be obtained or if it is not publicly accessible.

2.2. Obligation of Protection in Civil Law

The obligation concerning the protection of technology transfers can be based on civil law, in particular on the law of contractual obligations, whether express or implied.

2.2.1. Contract

Confidentiality clauses outline the terms according to which secret technology will be exchanged in technology transfer agreements. The conclusion of a confidentiality agreement may precede the conclusion of the final technology transfer agreement, because the parties may not be able to assess their interest in the conclusion of the final contract before they can evaluate the technology. Accordingly, the parties may, before the conclusion of the final contract on technology transfer which incorporates a confidentiality clause, conclude a confidentiality agreement. This agreement should outline obligations similar to those which will be incorporated in a clause in the final contract.

The conclusion of confidentiality agreements is of particular importance in the case of not yet disclosed patentable inventions. The communication of such inventions without the obligation of confidentiality could destroy the secrecy of the invention and lead to its unpatentability.

2.2.2. Implied Duty of Confidence and Fiduciary Duties

Within certain relations there exists an implied duty of confidence. Thus a patent attorney is, by reason of his professional duties, obliged to maintain information about technologies which he obtained from his clients confidential. Also the staff of an institute or a business will generally be considered impliedly bound to keep confidential secret information about the employer's technologies. However, the scope of the implied duty of confidence and fiduciary duties may be difficult to ascertain and depend on the circumstances of the individual case. For this reason it is recommendable to rely particularly in employment contracts on express clauses which describe the scope of an employee's duty to keep his employers technological information confidential.

Whether and up to which degree a business partner to whom confidential technologies have been communicated will be obliged to preserve the secrecy of the information may be controversial. For this reason it is useful to establish the conditions for the use which the recipient of the information can make in a confidentiality agreement.

2.2.3. Protection Against Acts of Unfair Competition

The Italian Patent Act establishes in Article 6-bis the conditions for the protection of secrets against acts of unfair competition. Accordingly a technology (a) must be secret, that is to say not generally known or easily accessible by experts or persons working in the sector, whether in whole or in the combination of its elements; (b) it must have an economic value insofar as it is secret, and, (c) the holder of the secret must take appropriate measures to maintain the secrecy. The Italian provision corresponds with Article 39 of the TRIPs which obliges Contracting States to a particular protection of secret information.

2.3. Obligation of Protection in Criminal Law

Protection of trade secrets by criminal law often differs between industrial secrets and business secrets. This differentiation may be justified by the object of the protection, either the industrial plant or the offices of an undertaking. The protection of trade secrets by criminal law is of a considerable importance, because it constitutes a viable threat against industrial espionage. A comprehensive protection may be established by protection against three basic violations: first, against the breach of confidence by employees during the subsistence of their contractual duties. Second, against the espionage of a secret with technological means and third the unauthorised exploitation of a secret or the communication of a secret which was obtained in an unauthorised manner. In the sector of trade secrets processed electronically computer-related offences have to be considered.

2.4. Duration of Protection

Technologies are protectable by confidentiality only during the subsistence of secrecy. If a technology is no longer secret, it cannot be protected by confidentiality agreements. The delimitation between secret and not secret technologies may be made by reference to its public accessibility. Once information has fallen into the public domain, it is no longer secret. The standard to be applied for the delimitation may rely on the accessibility of the information. If a technology can not without difficulty be acquired by a member of the public, it appears that it is protectable by confidentiality. The reason for this assumption is, that the information represents a valuable financial interest. Accordingly, the 'holder' of the technology who has obtained it, either by his own work, as a result of his undertaking's efficacy or as a result of an acquisition, merits protection by the law.

Once the information is accessible without difficulties, the justification for its protection by confidentiality fails and the legal order no longer sustains obligations which would refrain a person from the use of such technologies. The legal systems, whether based on common law or codified law, achieve very similar results. A popular test developed in the common law system is referred to as the 'springboard' metapher: "A person who has obtained information in confidence is not allowed to use it as a springboard for activities detrimental to the person who made the confidential communication, and springboard it remains even when all the features have been published or can be ascertained by any member of the public. (...) The possessor of the confidential information still has a long start over any member of the public" (Roxburgh J., Terrapin v. Builders Supply (1976) UK, R.P.C. 375 at 392).

3. The Pre-contractual Relation

Before communicating the technology to third parties, the holder should consider whether the state of the evolution of the technology justifies the risks deriving from the divulgation. A confidentiality agreement with another party should only be concluded if the development of the technology has progressed to such a degree that the involvement of persons external to the own organisation is necessary.

3.1. The Establishment of a Confidentiality Agreement

The pre-contractual relations which are directed toward the conclusion of a confidentiality agreement should identify the framework for the negotiation of the final contract. The draft confidentiality agreement should contain the necessary information about the parties and the persons involved in the negotiations, a brief description of the Confidential technology and of the means used for communications between the parties. This draft should be circulated between the parties and complemented with regard to any details which may be helpful, in particular concerning the circle of persons involved on each side and the means for communications.

3.2. Identification of Persons Involved in Negotiations

At the beginning of the negotiations, the circle of persons involved should be identified. It may be useful if each party established a list of persons, describing their exact responsibilities, including addresses, telephone, fax and email contacts. Additionally, it may be appropriate to identify the means for the communication between the parties.

3.3. Description of Confidential Technology

During the pre-contractual phase it is important not to reveal the essential elements of the technology through its description until the contractual partner has been found with whom the final contractual arrangement will be concluded. The description of the secret technology should disclose only as much information which the recipient needs for the purpose envisaged. If negotiations are conducted with several potential recipients, it is essential to limit the description of the technology in order to avoid that those organisations with which no contract is concluded will not be able to exploit the technology.

3.4. Preliminary Termination of Negotiations

If the negotiations did not lead to the conclusion of a confidentiality agreement or a long term contract, the parties may terminate their relation at will. Occasionally, a confidentiality agreement contains a clause in which the parties envisage a certain time schedule for the conclusion of a final contract.

4. Contractual Terms Concerning Confidentiality

The contractual terms which bind a party to maintain a technology confidential is based on the principle of the freedom of contract. However, this freedom is, in general, limited in the public interest. Accordingly, obligations which contravene the public order of a state are void, without effect and cannot be enforced before the courts of that state.

4.1. Confidentiality Clauses

Confidentiality clauses may be a part of a contract. Such contracts may concern the acquisition of a plant or company, they may relate to a licence for the use of a know-how or a patented invention and other facts.

4.2. Applicable Law in International Contracts

If the parties to the agreement are established in different states it may be recommendable if they chose the law applicable to the agreement. Since it can be difficult for a party to accept the application of the law of the state where the other party is established, they may consider the application of transnational rules of law or the settlement according to equitable principles.

If a contract and the subsequent exchange of information is made electronically, the parties should avoid doubts about the effects of the data exchange. It could be helpful if the parties agreed upon the application of the UNCITRAL Model Law on Electronic

Commerce which defines, amongst others, the time of receipt of a data message and which establishes rules on evidence concerning the use of electronic data messages.

4.3. Penalty Clauses

Penalty clauses may be used to facilitate the obeisance with contractual obligations. Such clauses are particularly useful in the case where it is difficult to calculate the amount of damages. However, taking into account of the fact that at an early stage the value of the Confidential technology will not easily be ascertainable, it may be difficult to arrive at an amount of damages for a breach of the contract or confidentiality which is acceptable for both parties.

4.4. Enforceability of Confidentiality Clauses and Competition Law

A confidentiality agreement constitutes a contract. Contracts are enforceable, unless they violate the public order. In the case of agreements on Confidential technology the enforcement may be refused according to a national jurisdiction if the agreement constitutes a prohibited cartel fin restraint of competition. In particular the attempt to 'monopolise' the use of a secret technology may be reprehended, and also an attempt to extend the recipient's obligation of confidentiality beyond the fall of the information into the public domain. However, it is difficult to indicate in a general manner the effect of confidentiality clauses, taking into account that the contractual types in which such clauses are contained, may differ considerably. Thus a confidentiality clause may be an element of a comprehensive licence contract which covers patented and non-patented technologies, it may be contained in a pooling of patented technologies, in cross-licence agreements and many other contractual types. Additionally, the enforceability of confidentiality clauses depends on the relevant national law. Thus no generally applicable rules can be indicated but only certain types of clauses which may give rise to concern when their enforcement is sought for.

4.4.1. Applicability of Rules of Competition Law

The applicability of the rules of competition law requires that certain conditions are fulfilled. For example, EU law prohibits in Article 81 of the EC Treaty only agreements, decisions and concerted practices which have as their object or effect the restriction of competition and which may affect the trade between member States. The EU Technology Transfer Block Exemption of 1996 is applicable to patent or know-how licences and mixed licences. If a clause meets with the conditions which are restrictions of the type contained in the 'white list', the clause is exempt from the prohibition of cartels. But there is also a list of 'black clauses' where the exemption will not be available.

4.4.2. Requirements Concerning the Confidential Technology

The EU Technology Transfer Block Exemption is applicable to 'know-how' which is secret, substantial and identified. This means that the know-how must not generally be accessible, that it must include information which is useful and it must be described or recorded in such a manner as to make it possible to verify that it satisfies the criteria of secrecy and substantiality.

4.4.3. Generally Permissible Clauses

Generally permissible clauses are standard confidentiality clauses and clauses which extend the obligation of confidentiality beyond the duration of the contract, provided that the technology is still secret; grant back clauses, by means of which the licensee is obliged to communicate improvements to the licensor are admissible, if the obligation is non-exclusive and reciprocal; quality standards or tie-in provisions for the supply of goods or services from the licensor if these are technically justified by reference to the technology; field of use restrictions by means of which the licensor limits the use to certain industrial sectors.

4.4.4. Clauses which May Be without Effect

Without effect may be clauses by means of which the duration of the obligation to maintain the technology confident is extended beyond the time when the information has become part of the public domain; non-competition clauses by means of which the licensee has to refrain from the development of competing technologies.

4.5. Arbitration in International Contracts

Should a dispute arise between the parties with regard to the confidentiality agreement or the final contract, it may be recommendable to settle the dispute by arbitration. Arbitration may be suggested if the parties wanted to avoid the subjection of the dispute to the jurisdiction of national courts. In international agreements, especially the institutional arbitration may offer an adequate service. Thus the parties may include in their agreement an arbitration clause such as those offered by WIPO or other institutions responsible for arbitration services.

In the case of confidentiality agreements it may be reasonable to resort to expedited arbitration which is less expensive and more expeditious than the full-fledged arbitration procedure. The recommended WIPO expedited arbitration clause states: "Any dispute, controversy or claim arising under, out of or relating to this contract and any subsequent amendments of this contract, including, without limitation, its formation, validity, binding effect, interpretation, performance, breach or termination, as well as non-contractual claims, shall be referred to and finally determined by arbitration in accordance with the WIPO Expedited Arbitration Rules. The place of arbitration shall be ... The language to be used in the arbitral proceedings shall be ... The dispute, controversy or claim shall be decided in accordance with the law of ..."

4.6. Rules on Evidence

In a contract on technology transfer the parties may determine the burden of proof with regard to the establishment of evidence. Whereas, as a general principle, the party which asserts a proposition in its favour has to establish the proof of this assertion, the parties may agree on an inversion of this rule in the case of the use of confidential technologies. Accordingly, for the case that the Confidential technology is used in a manner not covered by the contract, the parties may envisage that the burden of proof concerning a contractual use of the Confidential technology vests upon the recipient. By means of such a clause the burden of proof is imposed on the party which is 'closer'

to the liability for having communicated the technologies. Accordingly, the inversion of the basic rule of evidence appears justifiable. Since the recipient of the confidential technology will have to indicate to the owner of the information the circle of the persons to whom the information has been confided, it is not unreasonable to expect that he will be able to discharge the burden of proof through appropriate statements from these persons.

Differently, if the burden of proof vested with the owner of the information, he would have to prove the facts establishing the unauthorised leaking of the technology. This is a task which he will hardly be able to fulfil, taking into account that there may be a collusion of interests between the recipient and the unauthorised user in the free use of the technology.

4.7. Standards for the Classification of Confidential Technology

The standards for the classification of confidential technology may vary between different organisations, in particular if they are established in different states. It is useful to provide for the marking of confidential technology, no matter on which carrier the information is stored. Internal rules could establish definitions for unified classification markings (see for example the OECD Guidelines for the Security of Information Systems and its Review of 1998). The degrees of confidentiality may vary.

Marking should be foreseen for information whose unauthorised disclosure would cause significant harm to the interests of the organisation. Such a harm would consist in a financial loss in the loss of profitability or opportunity. A higher standard for marking should be provided for information whose unauthorised disclosure would cause serious damage to the interests of the organisation. Such harm would be caused by serious damage to the interests of the organisation, or serious financial loss, or a severe loss of profitability or opportunity.

Minimum standards should be established for the handling of the relevant technology covered by markings. In particular, rules should regulate the access to the relevant information, the storing, handling and transmission. It could be provided where the markings should be attached on the material carrier of the secret information, whether such technology may be communicated abroad, and whether personnel security checks should be carried out. Particular rules should cover information technology systems and the handling and storage of confidential technology on such systems. The conditions for release of the confidential technology may be established and for copying. Conditions for sending by post, courier service, fax and electronic communications technologies, for example by reference to encryption standards, should be identified. Also the circumstances under which such information may be destroyed could be defined and whether carriers containing the information may be taken on journeys and home by employees.

4.8. Evaluation of Security of Information Systems

The definition of the security of information systems used for the communication of confidential technology or other sensitive information is increasingly important. The definition of the standards to be used depends essentially on technological developments and may have to be adapted accordingly. The EU Commission's Joint Research Centre offers an 'Advanced Software Toolset for System Dependability Analysis'.

5. Post-contractual Protection

The confidentiality agreement may provide for post-contractual obligations, for example concerning the maintenance of the confidentiality. Generally, such a clause, by means of which the recipient is obliged to keep the technology confidential after the termination of the contractual relation will be considered valid. But, if, subsequent to the communication to the recipient, the technology has become part of the public domain, such a clause will hardly be enforceable.

Post-contractual obligations may bind employees not to divulge technologies which they have acquired during the performance of their employment contract. It may be difficult to differentiate between the employer's technologies and the professional skill which the employee obtained in the execution of his contract. The latter will belong to him, and the confidentiality clause cannot refrain the employee from making use of it.

Non-competition and non-solicitation clauses are additional means to limit the use of a protected technology beyond the duration of a contract. The validity of such clauses depends on the relevant national law. Such clauses should be limited in time and in territory. In the case of labour law the validity of such clauses may depend on the stipulation of a financial compensation for the benefit of the former employee.

ANNEX 1. Model Clauses

Confidentiality Provision in Employment Contract

1. Definition

Confidential Information is any technical or business information of the employer, not in the public domain, which:

- is marked 'confidential', or
- is confidential by nature, or
- is communicated to the employee as confidential information.

2. Use of Confidential Information

2.1. During the employment the staff member will make use of the employer's confidential information only for purposes of his contractual duties.

2.2. The staff member will keep the confidential information secure.

2.3. Confidential information may be disclosed only to persons who need to know it in order to perform their duties or obligations for the employer, provided that they undertake themselves to keep the information confidential. To other persons confidential information may only be disclosed if the law so requires.

3. Security of Information Systems

3.1. The staff member is obliged to use a password coordinated with his senior for the protection of his computer terminal against access by unauthorised persons.

3.2. Before leaving his workplace the staff member is obliged to switch off his computer terminal.

3.3. The staff member is obliged to use a password permitting access to his email account.

3.4. The staff member is cooperate with the security officer and to follow his directives concerning the security of information systems.

4. Termination of the Employment Contract

4.1. On the termination of the contract the employee is obliged to render to the employee and documentation which he may have containing any confidential information which he has obtained during the subsistence of the contract.

4.2. After the termination of the contract the employee has to refrain from using any confidential information which he has obtained during the subsistence of the contract.

5. Post-contractual Obligations

5.1. Non-competition: after the termination of the employment the staff member may not, directly or indirectly be engaged in any business which is, in whole or in part, competing with the business of the employer.

5.2. The obligation of non-competition has a duration of ... months/years.

5.3. The obligation of non-competition concerns the territory of: ... provinces/districts.
5.4. During the obligation of non-competition the employee may not provide consultancy to any business which is, in whole or in part, in competition with the business of the employer.
5.5. Non-solicitation: after the termination of the employment the staff member may not, directly or indirectly, solicit or accept the business of any client for whom the employer provided goods or services within the last ... months/years before the termination of the contract or with any person with whom the employer had negotiated the supply of goods or services during this period.
5.6. The obligation of non-solicitation has a duration of ... months/years.

6. Severability

6.1. The parties agree that each of the covenants are separate and severable.
6.2. If any such covenant should be void or without effect for whatever reason, the parties agree that such covenant shall be applicable with such deletions as may be necessary to render it valid and effective.

General Confidentiality Clause

Confidentiality clause to be used for a variety of agreements between the parties to a contract, here named an "Institute" and a "Recipient"

1. Definition of Confidential Technology
Confidential Technology means any technology which is communicated in written or graphic form on a material support whatsoever or which is communicated orally, including, but not limited to, scientific knowledge, patentable and unpatentable inventions, know-how, plans, biological materials, products, processes, mathematical and/or other formulae, codes and/or computer software.

2. Use of Confidential Technology
The Recipient may not use the Confidential Technology for any other purposes than those described in this agreement.

3. Disclosure of Confidential Technology and Marking
3.1. Any Confidential Technology disclosed within the framework of this agreement shall be in writing. Any such writing shall be marked with the word "CONFIDENTIAL" and the date of the communication.
3.2. If exceptionally oral communication of Confidential Technology is made, it shall be confirmed in writing, marked with the word "CONFIDENTIAL" and the date of the communication.

4. Communication of Confidential Technology
4.1. The Recipient will not communicate the Confidential Technology or any part thereof to any person or organisation outside of the scope of this Agreement.
The Recipient will limit the communication of the Confidential Technology within his organisation to a circle of persons which is communicated to the Institute and which is aware of this Agreement.
4.2. The Recipient shall bind the persons within his organisation to whom the Confidential Technology is communicated by the terms of this Agreement.
4.3. The Recipient may communicate Confidential Technology to third parties to the extent contemplated by this Agreement, on the condition that the Recipient enters into an agreement with the third party which binds the third party on equivalent confidentiality terms to those contained in this Agreement.

5. Use of Confidential Technology
5.1. The Recipient will make use of the Confidential Technology exclusively for the purposes of this Agreement.
5.2. Any use of the Confidential Technology by the Recipient beyond the purpose of this Agreement requires the prior written authorisation by the Institute.

5.3. Nothing in this clause shall be construed to grant the Recipient a licence for the use of the Confidential Technology.

6. Information in the Public Domain
The obligation of confidentiality does not relate to technologies which became part of the public domain without the fault of the Recipient.

Alternatively:
6.1. The obligation of confidentiality does not relate to technologies which became part of the public domain prior to the date the Confidential Technology was marked "CONFIDENTIAL"; or
6.2. The obligation of confidentiality does not relate to technologies which became part of the public domain not due to some unauthorised act by or omission of the Recipient after this Agreement is executed; or
6.3. The Recipient can demonstrate by written records that it developed such Confidential Technology independently of the Institute; or
6.4. The Confidential Technology was disclosed to the Recipient by a third person who had the right to make such a disclosure.

7. Treatment of Confidential Technology
7.1. The Recipient will treat the Confidential Technology according to the standards of a reasonable man, taking into account of the circumstances of the case and the state of the art.
7.2. The Recipient will treat the Confidential Technology at least with the same degree of care as he treats his own Confidential Technology.

8. Evidence
In the case of the use of a Institute's Confidential Technology by the Recipient or a third person which is not based on this agreement the burden of proof that the use is authorised lies on the Recipient.

9. Duration of Obligation of Confidence
Without regard to the duration of the Agreement, the Recipient shall be obliged to treat the Confidential Technology as confidential during a period of five years subsequent to the signature of the Agreement.

for the Institute:

.....
place, date

for the Recipient:

.....
place, date

Witnessed by:

.....
place, date

Non-disclosure Agreement Concerning the Communication of Confidential Technology

Non-disclosure Agreement between

...
the "Institute"

and

...
the "Recipient"

Whereas the Institute has developed a technology concerning a:

- (a) a technological product:.....

- (b) a technological process.....

which is considered secret and which is referred to as Confidential Technology;

Whereas the Institute is desirous of disclosing the Confidential Technology as herein defined to the Recipient under the condition of confidentiality with the aim to enable the Recipient to:

- (a) produce a prototype of the product for use in industrial application;

- (b) develop the process up to the stage of industrial application; and/or

- (c) assess the appropriateness of the establishment of a collaborative Agreement;

Whereas the Recipient has an interest to use the Confidential Technology for the purposes of:.....

The parties agree as follows:

1. Definition of Confidential Technology
Confidential Technology means any technology which is communicated in written or graphic form on a material support whatsoever or which is communicated orally, including, but not limited to, scientific knowledge, patentable and unpatentable inventions, know-how, plans, biological materials, products, processes, mathematical and/or other formulae, codes and/or computer software.

2. Use of Confidential Technology

The Recipient may not use the Confidential Technology for any other purposes than those described in this agreement.

3. Disclosure of Confidential Technology and Marking
3.1. Any Confidential Technology disclosed within the framework of this agreement shall be in writing. Any such writing shall be marked with the word "CONFIDENTIAL" and the date of the communication.
3.2. If exceptionally oral communication of Confidential Technology is made, it shall be confirmed in writing, marked with the word "CONFIDENTIAL" and the date of the communication.

4. Communication of Confidential Technology
4.1. The Recipient will not communicate the Confidential Technology or any part thereof to any person or organisation outside of the scope of this Agreement.
4.2. The Recipient will limit the communication of the Confidential Technology within his organisation to a circle of persons which is communicated to the Institute and which is aware of this Agreement.
4.3. The Recipient shall bind the persons within his organisation to whom the Confidential Technology is communicated by the terms of this Agreement.

5. Use of Confidential Technology
5.1. The Recipient will make use of the Confidential Technology exclusively for the purposes of this Agreement with the aim to establishing a close cooperation between the parties.
5.2. Any use of the Confidential Technology by the Recipient beyond the purpose of this Agreement requires the prior written authorisation by the Institute.

6. Information in the Public Domain
The obligation of confidentiality does not relate to technologies which became part of the public domain without the fault of the Recipient.

Alternatively:
6.1. The obligation of confidentiality does not relate to technologies which became part of the public domain prior to the date the Confidential Technology was marked "CONFIDENTIAL"; or
6.2. The obligation of confidentiality does not relate to technologies which became part of the public domain not due to some unauthorised act by or omission of the Recipient after this Agreement is executed; or
6.3. The Recipient can demonstrate by written records that it developed such Confidential Technology independently of the Institute; or
6.4. The Confidential Technology was disclosed to the Recipient by a third person who had the right to make such a disclosure.

7. Treatment of Confidential Technology

7.1. The Recipient will treat the Confidential Technology according to the standards of a reasonable man, taking into account of the circumstances of the case and the state of the art.
7.2. The Recipient will treat the Confidential Technology at least with the same degree of care as he treats his own Confidential Technology.

8. Evidence
In the case of the use of a Institute's Confidential Technology by the Recipient or a third person which is not based on this agreement the burden of proof that the use is authorised lies on the Recipient.

9. Assignment of Agreement
The parties to this Agreement agree that the rights and duties under this Agreement are not assignable unless with the prior written approval by the other party.

10. Termination of Agreement
10.1. On the termination of the Agreement the Recipient is obliged to render to the Institute any documents received during the term of the Agreement, including any copies which may have been made for the execution of this Agreement and models, samples or specimen embodying the Confidential Technology.
10.2. The Recipient is not authorised to make use of the Confidential Technology beyond the term of this Agreement.

11. Duration of Agreement
11.1. This Agreement begins on.....
11.2. It terminates on.....
or at any time before that date if the Recipient has evaluated the technology and notified the Institute in writing that it is no longer interested in continuing with the evaluation or if it is determined by either party that an agreement concerning the use of the Confidential Technology cannot be successfully negotiated.

12. Breach of Agreement
In the case of a breach of this Agreement by the Recipient the Institute shall be entitled to terminate this Agreement.
In the case of a breach of confidence the Recipient shall pay the Institute a penalty of:
.....

13. Form and Limitations
13.1. This Agreement is in writing.
13.2. This Agreement embodies all the understanding between the parties concerning the Confidential Technology.
13.3. Any amendments or modifications to this Agreement must be made in writing and signed by the parties.
13.4. This Agreement does not grant a licence or conveyance of any rights in the use of the Confidential Technology for the commercial exploitation.

14. Applicable Law

The parties to this Agreement choose the law of the state of ..... as the law applicable to the Agreement, any data messages by the parties shall be subject to the UNCITRAL Model Law on Electronic Commerce.

Alternatively:
The parties authorise the arbitrator to settle the dispute on equitable principles.

15. Settlement of Disputes

In the case of a dispute between the parties relating to this agreement the issue shall be solved by expedited arbitration. The proceedings shall be kept confidential. The body responsible for arbitration shall be:

- WIPO

Alternatively

- .....

for the Institute:

.....
place, date

for the Recipient:

.....
place, date

Witnessed by:

.....
place, date

Non-disclosure Agreement Concerning the Exchange of Confidential Technology

Non-disclosure Agreement concerning the exchange of Confidential Technology between:

...
the "Institute"

and

...
the "Recipient"

Whereas the Organisation has developed a technology concerning a:

- (a) a technological product:.....

- (b) a technological process.....

which is considered secret and which is referred to as Confidential Technology;

Whereas the Institute is desirous of disclosing the Confidential Technology as herein defined to the Recipient under the condition of confidentiality with the aim to enable the parties to:

- (a) produce a prototype of the product for use in industrial application;

- (b) develop the process up to the stage of industrial application; and/or

- (c) assess the appropriateness of the establishment of a collaborative Agreement;

Whereas the Recipient owns a Confidential Technology concerning a:

- (a) a technological product:.....

- (b) a technological process.....

which is considered secret and which is referred to as Confidential Technology;

Whereas the Recipient is desirous of disclosing the Confidential Technology as herein defined to the Institute under the condition of confidentiality with the aim to enable the parties to:

- (a) produce a prototype of the product for use in industrial application;

- (b) develop the process up to the stage of industrial application; or

- (c) assess the appropriateness of the establishment of a collaborative Agreement;

The parties agree as follows:

1. Definition of Confidential Technology
Confidential Technology means any technology which is communicated in written or graphic form on a material support whatsoever or which is communicated orally, including, but not limited to, scientific knowledge, patentable and non-patentable inventions, know-how, plans, biological materials, products, processes, mathematical and/or other formulae, codes and/or computer software.

2. Use of Confidential Technology
A party may not use the other party's Confidential Technology for any other purposes than those described in this agreement.

3. Disclosure of Confidential Technology and Marking
3.1. Any Confidential Technology disclosed within the framework of this agreement shall be in writing. Any such writing shall be marked with the word "CONFIDENTIAL" and the date of the communication.
3.2. If exceptionally oral communication of Confidential Technology is made, it shall be confirmed in writing, marked with the word "CONFIDENTIAL" and the date of the communication.

4. Communication of Confidential Technology
4.1. A party will not communicate the other party's Confidential Technology or any part thereof to any person or organisation outside of the scope of this Agreement.
4.2. A party will limit the communication of the other party's Confidential Technology within his organisation to a circle of persons which is communicated to the other party and which is aware of this Agreement.
4.3. A party shall bind the persons within his organisation to whom the other party's Confidential Technology is communicated by the terms of this Agreement.

5. Use of Confidential Technology
5.1. The Recipient will make use of the Confidential Technology exclusively for the purposes of this Agreement with the aim to establishing a close cooperation between the parties.
5.2. Any use of a party's Confidential Technology by the other party beyond the purpose of this Agreement requires the prior written authorisation by the other party.

6. Information in the Public Domain

The obligation of confidentiality does not relate to technologies which became part of the public domain without the fault of the party to whom the Confidential Technology was communicated.

Alternatively:
6.1. The obligation of confidentiality does not relate to technologies which became part of the public domain prior to the date the Confidential Technology was marked "CONFIDENTIAL"; or
6.2. The obligation of confidentiality does not relate to technologies which became part of the public domain not due to some unauthorised act by or omission of the other party after this Agreement is executed; or
6.3. The other party can demonstrate by written records that it developed such Confidential Technology independently of the party which communicated the Confidential Technology; or
6.4. The Confidential Technology was disclosed to the other party by a third person who had the right to make such a disclosure.

7. Treatment of Confidential Technology
7.1. Each party will treat the other party's Confidential Technology according to the standards of a reasonable man, taking into account of the circumstances of the case and the state of the art.
7.2. Each party will treat the other party's Confidential Technology at least with the same degree of care as he treats his own Confidential Technology.

8. Evidence
In the case of the use of a party's Confidential Technology by the other party or a third person which is not based on this agreement the burden of proof that the use is authorised lies on the other party.

9. Assignment of Agreement
The parties to this Agreement agree that the rights and duties under this Agreement are not assignable unless with the prior written approval by the other party.

10. Termination of Agreement
10.1. On the termination of the Agreement each party is obliged to render to the other party any documents received during the term of the Agreement, including any copies which may have been made for the execution of this Agreement and models, samples or specimen embodying the other party's Confidential Technology.
10.2. A party is not authorised to make use of the other party's Confidential Technology beyond the term of this Agreement.

11. Duration of Agreement
11.1. This Agreement begins on.....
11.2. It terminates on.....

or at any time before that date if a party has evaluated the technology and notified the other party in writing that it is no longer interested in continuing with the evaluation or if it is determined by either party that an agreement concerning the use of the Confidential Technology cannot be successfully negotiated.

12. Breach of Agreement
In the case of a breach of this Agreement by a party the other party shall be entitled to terminate this Agreement.
In the case of a breach of confidence the Recipient shall pay the Institute a penalty of:
.....
In the case of a breach of confidence the Institute shall pay the Recipient a penalty of:
.....

13. Form and Limitations
13.1. This Agreement is in writing.
13.2. This Agreement embodies all the understanding between the parties concerning the Confidential Technology.
13.3. Any amendments or modifications to this Agreement must be made in writing and signed by the parties.
13.4. This Agreement does not grant a licence or conveyance of any rights in the use of the Confidential Technology for the commercial exploitation.

14. Applicable Law
The parties to this Agreement choose the law of the state of ..... as the law applicable to the Agreement any data messages by the parties shall be subject to the UNCITRAL Model Law on Electronic Commerce.

Alternatively:
The parties authorise the arbitrator to settle the dispute on equitable principles.

15. Settlement of Disputes
In the case of a dispute between the parties relating to this agreement the issue shall be solved by expedited arbitration. The proceedings shall be kept confidential. The body responsible for arbitration shall be:
- WIPO

Alternatively
- .....

for the Institute:

.....
place, date

for the Recipient:

.....
place, date

Witnessed by:

.....
place, date

Research Agreement on Non-disclosure Concerning the Communication of Confidential Technology

Non-disclosure Agreement concerning the communication of Confidential Technology for purposes of research between:

...
the "Organisation"

and

...
the "Institute"

Whereas the Organisation has developed a technology concerning a:

- (a) a technological product:.....

- (b) a technological process.....

which is considered secret and which is referred to as Confidential Technology;

Whereas the Organisation is desirous of disclosing the Confidential Technology as herein defined to the Institute under the condition of confidentiality with the aim to enable the Institute to:

- (a) produce a prototype of the product for use in industrial application;

- (b) develop the process up to the stage of industrial application; and/or

- (c) assess the appropriateness of the establishment of a collaborative Agreement;

Whereas the Institute has an interest to use the Confidential Technology for the purposes of:.....

The parties agree as follows:

1. Definition of Confidential Technology
Confidential Technology means any technology which is communicated in written or graphic form on a material support whatsoever or which is communicated orally, including, but not limited to, scientific knowledge, patentable and non-patentable inventions, know-how, plans, biological materials, products, processes, mathematical and/or other formulae, codes and/or computer software.

2. Use of Confidential Technology
The Institute may not use the Confidential Technology for any other purposes than those described in this agreement.

3. Disclosure of Confidential Technology and Marking
3.1. Any Confidential Technology disclosed within the framework of this agreement shall be in writing. Any such writing shall be marked with the word "CONFIDENTIAL" and the date of the communication.
3.2. If exceptionally oral communication of Confidential Technology is made, it shall be confirmed in writing, marked with the word "CONFIDENTIAL" and the date of the communication.

4. Communication of Confidential Technology
4.1. The Institute will not communicate the Confidential Technology or any part thereof to any person or organisation outside of the scope of this Agreement.
4.2. The Institute will limit the communication of the Confidential Technology within its establishment to a circle of persons which is communicated to the Organisation and which is aware of this Agreement.
4.3. The Institute shall bind the persons within its establishment to whom the Confidential Technology is communicated by the terms of this Agreement.

5. Use of Confidential Technology
5.1. The Institute will make use of the Confidential Technology exclusively for the purposes of this Agreement with the aim to establishing a close cooperation between the parties.
5.2. Any use of the Confidential Technology by the Institute beyond the purpose of this Agreement requires the prior written authorisation by the Organisation.

6. Information in the Public Domain
The obligation of confidentiality does not relate to technologies which became part of the public domain without the fault of the Institute.

Alternatively:
6.1. The obligation of confidentiality does not relate to technologies which became part of the public domain prior to the date the Confidential Technology was marked "CONFIDENTIAL"; or
6.2. The obligation of confidentiality does not relate to technologies which became part of the public domain not due to some unauthorised act by or omission of the Institute after this Agreement is executed; or
6.3. The Institute can demonstrate by written records that it developed such Confidential Technology independently of the Organisation; or
6.4. The Confidential Technology was disclosed to the Institute by a third person who had the right to make such a disclosure.

7. Treatment of Confidential Technology

7.1. The Institute will treat the Confidential Technology according to the standards of a reasonable man, taking into account of the circumstances of the case and the state of the art.
7.2. The Institute will treat the Confidential Technology at least with the same degree of care as it treats its own Confidential Technology.

8. Evidence
In the case of the use of the Confidential Technology by the Institute or a third person which is not based on this agreement the burden of proof that the use is authorised lies on the Institute.

9. Assignment of Agreement
The parties to this Agreement agree that the rights and duties under this Agreement are not assignable unless with the prior written approval by the other party.

10. Termination of Agreement
10.1. On the termination of the Agreement the Institute is obliged to render to the Organisation any documents received during the term of the Agreement, including any copies which may have been made for the execution of this Agreement and models, samples or specimen embodying the Confidential Technology.
10.2. The Institute is not authorised to make use of the Confidential Technology beyond the term of this Agreement.

11. Duration of Agreement
11.1. This Agreement begins on.....
11.2. It terminates on.....
or at any time before that date if the Institute has evaluated the technology and notified the Organisation in writing that it is no longer interested in continuing with the evaluation or if it is determined by either party that an agreement concerning the use of the Confidential Technology cannot be successfully negotiated.

12. Breach of Agreement
In the case of a breach of this Agreement by the Institute the Organisation shall be entitled to terminate this Agreement.
In the case of a breach of confidence the Institute shall pay the Organisation a penalty of:.....

13. Form and Limitations
13.1. This Agreement is in writing.
13.2. This Agreement embodies all the understanding between the parties concerning the Confidential Technology.
13.3. Any amendments or modifications to this Agreement must be made in writing and signed by the parties.
13.4. This Agreement does not grant a licence or conveyance of any rights in the use of the Confidential Technology for the commercial exploitation.

14. Applicable Law

The parties to this Agreement choose the law of the state of ..... as the law applicable to the Agreement any data messages by the parties shall be subject to the UNCITRAL Model Law on Electronic Commerce.

Alternatively:
The parties authorise the arbitrator to settle the dispute on equitable principles.

15. Settlement of Disputes

In the case of a dispute between the parties relating to this agreement the issue shall be solved by expedited arbitration. The proceedings shall be kept confidential. The body responsible for arbitration shall be:

- WIPO

Alternatively

- .....

for the Organisation:

.....
place, date

for the Institute:

.....
place, date

Witnessed by:

.....
place, date

Confidentiality Clause in an Electronic Data Interchange Agreement

1. Confidentiality of Data
All messages shall be handled confidentially by taking into account the scope of this Agreement and the Individual Agreement concerned. In particular, each party must ensure that the number of persons dealing with the processing of Messages is restricted as far as possible and that all persons involved are obliged to observe the security and confidentiality measures provided in the Agreement and in each of the Individual Agreement concerned when processing Messages.

2. Security Obligations and Checking of Malfunctions and Errors
Each party is obliged to protect against unauthorised access to its communications equipment by third parties, unauthorised transmission of messages or similar misuse of its communications equipment, as well as against loss of input and output of data after the Data transmission or Data retrieval of messages. The standard of care required from the parties shall be the prevailing state of the art, in accordance with the catalogue of requirements annexed hereto as Appendix.

3. Disruptions, Malfunctions and Errors Avoidance
3.1. If one party detects a disruption in the Communications System or if there is justified reason to presume such a disruption, the said party is obliged to inform the other party immediately. This obligation shall remain in force regardless of the area of responsibility in which the source of the detected or presumed disruption is located. If necessary, a means of communication other than the communication system (for example telephone, telex, telefax) must be chosen for notification.
3.2. Irrespective of the obligation to notify in accordance with the prevailing paragraph, each party must in such cases take all measures available to such party to identify and avoid errors in order to reduce damage, provided that the extent of the measures is not unreasonably out of proportion to the resultant reduction of damage.

4. Liability
4.1. Each party is liable for any damage arising from errors or disruptions within the party's sphere of responsibility. If. In connection with the occurrence of the damaging event, any of the obligations concerning security obligations and checking of malfunctions and errors and disruptions, malfunctions and errors avoidance is not discharged by any of the parties there shall be a rebuttable presumption that the damage has resulted from an error or a disruption having occurred within the sphere of responsibility of such party.
4.2. The sphere of responsibility of the sender of messages shall cover its communications equipment, its communications security and the period of time until receipt of the Message. The sphere of responsibility of the recipient of Messages shall cover its communications equipment, its communications security and the period of time following receipt of the message.

4.3. Each party shall bear the costs of identifying errors which are located or arise within its sphere of responsibility. If an error occurs which cannot definitely be assigned to either party's sphere of responsibility, the party most likely to have been in a position to avoid the error shall bear the entire costs of the search for errors. If this can also not be clarified, each party shall bear one half the costs of identifying the error.
4.4. The liability pursuant to the first paragraph shall cover all personal injury, damage to property and pecuniary loss including the costs of identifying errors, regardless of which party has borne the costs in the first place in accordance with the last paragraph. Compensation for damage to property and pecuniary loss shall be limited to a maximum amount of ... of the damage incurred by the other party as a result of reliance on the authenticity, accuracy or completeness of the message. Liability for damages shall arise only insofar as the other party was unaware that the message was not authentic, accurate or complete and also could not, with reasonable care, have recognised this fact. The maximum amount for intangible damage is ...

5. Message Encryption
5.1. Message encryption is a procedure in accordance with the Appendix to this Agreement which makes confidential messages unreadable, and thus protected from access by third parties.
5.2. In this connection it may be agreed that messages, in total or in part, are to be encrypted. Message encryption will be provided for on the basis of commonly defined standards.

ANNEX 2: Article 39 TRIPs

Article 39

(1) In the course of ensuring effective protection against unfair competition as provided in Article 10bis of the Paris Convention (1967), Members shall protect undisclosed information in accordance with paragraph 2 and data submitted to governments or governmental agencies in accordance with paragraph 3.

(2) 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 (see footnote 10) 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.

(3) Members, when requiring, as a condition of approving the marketing of pharmaceutical or of agricultural chemical products which utilise new chemical entities, the submission of undisclosed test or other data, the origination of which involves a considerable effort, shall protect such data against unfair commercial use. In addition, Members shall protect such data against disclosure, except where necessary to protect the public, or unless steps are taken to ensure that the data are protected against unfair commercial use.

Footnote 10:

For the purpose of this provision, "a manner contrary to honest commercial practices" shall mean 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.

Selected List of Literature

Basic Electronic Data Interchange (EDI) Agreement, EDI Law Review 3 (1996) 53-62

BAUMBACH/HEFERMEHL: "Wettbewerbsrecht", 21st ed., C.H. Beck, Munich 1999

Georges BONNET, ed.: "Code de la Propriété Intellectuelle", Dalloz, Paris 2000

William R. CORNISH: "Intellectual Property", 3rd ed., Sweet & Maxwell, London 1996

John HULL: "Commercial Secrecy", Sweet & Maxwell, London 1998

MARCHETTI and UBERTAZZI: "Commentario Breve al Diritto della Concorrenza" Cedam, Padova 1997

Websites

European Commission Joint Research Centre, Advanced Software Toolset for System Dependability Analysis
http://das-isis.jc.it/Astra

EU Commission Regulation No. 240/96 of 31/01/96 on the application of Article 85(3) EC Treaty to certain categories of technology transfer agreements
http://europa.eu.int/eur-lex/en/lif/dat/1996_en396R0240.html

OECD Workshop on "Intellectual Property Rights and Government-funded Research in Russia", Obninsk, October 1996, part of the programme of the CCET for policy dialogue and cooperation with the Russian Federation, in particular Paul RABETTE: "Disclosure, Publication Restrictions and Secrecy Agreements",
http://www.oecd.org/sge/ccet

OECD: "Patents and Innovation in the International Context", Working Group on Innovation and Technology Policy of the OECD Committee for Scientific and Technological Policy (CSTP) 1997
http://www.oecd.org and
http://www.oecd.org/dsti/sti/s_t/inte/prod/e_97-210.htm

OECD Guidelines for the Security of Information Systems of 26/11/92 and the Review of the 1992 Guidelines for the Security of Information Systems of 19/03/98
http://www.oecd.org/dsti/sti/it/secur/prod/e_secur.htm

Standard Agreement for University-Industry Collaboration, University of Sherbrooke
http://www.usherb.ca/bleu/anglais/researcher/agreement/nondisclosure/index.html

WIPO Arbitration and Mediation Center and arbitration clauses
http://arbiter.wipo.int/arbitration/index.html and
http://arbiter.wipo.int/arbitratiopn/contraqct-clauses/clauses.html