Escrow Agreements

A Software Escrow Agreement establishes the obligation to deposit the source code of a computer program and other relevant material at (in most cases) a neutral third party. In case of one of the contractually established trigger events, the material has to be handed over to the user. Escrow Agreements have a great importance for DP systems as a large number of risks can be effectively minimized. The agreement helps to balance the conflicting interests of the software developer and the user.

Phases

1. Escrow Planning: Preparatory measures, identifying/analyzing the critical business processes depending on the software
2. Escrow Execution: Initial deposit process, verification, storage, deposit of new software versions (if necessary)
3. Escrow Redeployment: Release in case of trigger event

Risks to be covered (possible trigger events)

- Insolvency of the software developer
- Liquidation of the software developer
- No further development of the software (end-of-life-letter of advice)
- Refusal or failure to fulfill the contractually established obligations

One contract model for Escrow Agreements is a chain of contracts. The software developer and the user sign a contract that transfers the ownership of the source code and other relevant material to the user but also obliges him to use an Escrow Agent for the execution of the contract. Subsequently, the software user signs a Software Escrow Agreement with the Escrow Agent. In earlier years Escrow Agent were mostly lawyers and notaries, today specialized companies with the knowledge necessary to fulfill the relevant contractual obligations and to assure the quality of the deposited material often undertake the tasks of the Escrow Agent. They establish the detailed proceedings of the preparation and execution of the Escrow Agreement. The software developer is obliged to hand over to the Escrow Agent a copy of the material specified in the contract – usually the source code and adjacent materials – within a period of time determined in the agreement.

Deposited objects

- Source code of the software (complete and clearly arranged)
- Program description
- Object code
- Translator (compiler) or other support software
- Current status of the documents and information
- Details to allow the access to the deposit material like password or encryption
- Name and home address of responsible programmers

Since the material must meet certain requirements concerning its quality, a verification process has to be carried out. The two most important possibilities are:

1. Standard verification (virus free, readable, completeness in comparison with the table of contents, ability to decompress compressed data, random samples of the documentation and their fitness for use)
2. Full verification (identification of the material, examination of the formal accordance, compilation, verification of the software and its executable form, operability with corresponding reports)

Software Specific Risks

- Reading errors on the medium
- Incomplete source code
- Configuration/instructions not available
- Insufficient documentation
- Absent licenses
- Objects are out of date

The Escrow Agreement should contain terms of liability because the Escrow Agent can be held liable for damages suffered by the software developer or user. Liability can be limited to a maximum amount. However, it is possible to establish liability only for damages which are typical for escrow work. In any case, insurance should be taken out. The material has to be treated confidentially, during the Escrow execution as well as after the release of the material. Unauthorized access must be prevented.

Obligations of the Escrow Agent

- Acceptance of the material
- Notification obligations (e.g. after receipt, in case of damage or destruction)
- Verification of the material
- Storage (safe and secure environment) and replacement of the material
- Handing over the deposited material in case of trigger event
- Confidentiality

To ensure that the latest version of the source code and the relevant material is in storage at the Escrow Agent, he needs the right to demand regularly the newest version of the source code from the software developer. Additionally, it is recommendable to entitle the Escrow Agent to migrate deposited materials from out-of-date mediums to more current storage devices to safeguard its accessibility.

The Escrow Agreement has to determine precisely under which circumstances the source code should be handed over. If the Escrow agreement is supposed to cover the risk of insolvency of the software developer, trigger events for the release of the Escrow materials may be the decision of the competent insolvency court to open the bankruptcy proceedings or the dismissal of the opening of bankruptcy proceedings due to lack of assets.

The software user has the obligation to inform the Escrow Agent about the occurrence of any of the established trigger events and provide sufficient evidence. Then the Escrow Agent is obliged to inform the software developer about this announcement and give him the chance

to dissent the handover of the materials. If the developer refuses the occurrence of a trigger event, the Escrow Agent will not release the materials until a final arbitrament of an arbitration court is made. The consequences of the release regarding the rights to the source code should be stated in the Escrow Agreement. Usually the original rightholder remains owner of all commercial rights of exploitation to the code. However, in order to protect the user's investment, he needs more than just the simple right to use the software. Often it is essential to entitle him to fix bugs, adapt the program to altered demands, perform maintenance tasks and make copies of the program necessary for his own use. The scope of rights transferred can depend on the actual trigger event and the specific needs resulting from it.