Termination of an IT Maintenance Contract for Alleged Security Breaches: What Must the Client Prove?

JACQUES DE WERRA, MARIANNA SORTON

A client attempted to terminate (with immediate effect) a three-year IT maintenance contract it entered into with an IT provider, by claiming major security violations and other alleged breaches of contract. The termination was deemed to be invalid and the IT Provider was awarded full damages, which corresponded to the contractual fees due for the original (full) term of the contract.

Judgment of the Federal Supreme Court of 29 July 2024

Case Reference: 4A_505/2023

Facts

Between 2014 and 2016, B. LLC ("the **IT Provider**") carried out various IT services for a company active in commodities trading, A. SA ("the **Client**").

The Client and the IT Provider (collectively "the **Parties**") concluded a first contract in 2014 (for a term of one year). In 2015, the Parties concluded a second contract for a term of three years ranging from January 1, 2015 to December 31, 2017, with tacit renewal for a year unless terminated with a three-months' advance notice ("the **Contract**"). Under the Contract, the IT Provider undertook to carry out various IT services, including the **maintenance** of the Client's IT infrastructure, for a monthly fee of CHF 20,500.

The Contract provided for **early termination** per the following terms:

- If a party breaches any material term of the Contract and does not remedy the breach within 30 days of receiving notice, the other party may terminate the Contract in writing. If it is impossible to remedy the breach within the 30-day period, a further reasonable period, not exceeding 60 days from receipt of the notice, shall be granted.
- In addition, either party may terminate the Contract with immediate effect in the event of gross negligence or intentional wrongful conduct.

The IT Provider was run and managed by C, who had formerly been employed by the Client as its (in-house) IT system engineer. During the Contract, C/the IT Provider worked in close collaboration with the Client's IT department.

Every year, the Client conducted an internal and external IT audit. These audits did not raise any particular issue or security problem during the term of the Contract, except for a few recommendations that had always been promptly followed.

However, the relationship between the Client and the IT Provider deteriorated between 2015 and 2016:

- On March 26, 2015, C (on behalf of the IT Provider) sent a **complaint via email** to the Client stating that the Client's IT operations had been negatively impacted by the Client's delay to renew specific IT contracts (e.g. those related to servers and archives). C expressed his concern related to that delay, which had a considerable impact on "all of the [IT] department's functions". He indicated that he would continue to make every effort to provide quality service under these conditions, but he expressly refused to bear any responsibility caused by any delay, negligence or lack of management with regard to the administrative and operational functions of the IT infrastructure.
- In the fall of 2015, the Client admitted it was facing financial difficulties and asked its employees if they would

be willing to work part-time.

- In April 2016, the Client hired a new IT Department Head who commissioned a third party (G) to conduct an audit of its IT system. In its report, G identified various issues affecting the Client's IT system, which did not meet current standards and required upgrades. The report also alleged security flaws and pointed to a wide disparity in the equipment used. Overall, the equipment was deemed obsolete and in need of replacement.

The very same day that the Client received G's report, it sent the IT Provider a **notice of termination** of the Contract with immediate effect for gross negligence. In essence, the Client accused the IT Provider of numerous breaches of the Contract and of accepted IT best practices, which it claimed had led to **major security breaches**. These alleged breaches included non-compliance with security standards and norms, shortcomings and omissions relating to services and maintenance, and a blatant lack of information about the shortcomings that had been – or should have been – identified.

Following the termination of the Contract, the Client hired several companies to carry out additional IT audits, which all reported various problems affecting the Client's IT infrastructure.

In 2017, the Client initiated civil proceedings against the IT Provider to claim over CHF 250,000 in damages corresponding to costs incurred to restore the Client's IT system as well as the costs of audits and legal fees. The IT Provider counter-claimed for outstanding and future fees that it was entitled to under the Contract, which was initially set to expire on December 31, 2017.

The cantonal courts (both first and second instance) ruled that the Client's termination of the Contract **lacked good cause** and was therefore unjustified and ineffective. As a result, the IT Provider was awarded full compensation, corresponding to the contractually agreed fees due for the remaining term of the Contract (i.e. from April 2016 to December 31, 2017). The Client appealed to the Federal Supreme Court.

Issue

Before the Federal Supreme Court, only two issues were in dispute:

(1) Despite the fact that the Contract was terminated without good cause (i.e. that the performance of the IT Provider did not justify the immediate termination of the Contract by the Client), was the IT Provider nonetheless **contractually liable** under Art. 97 para. 1 SCO for damages (allegedly) caused to the Client?

and

(2) With regards to the damages awarded to the IT Provider, should certain **earnings, savings or avoidable expenses** following the termination of the Contract have been deducted by the cantonal courts?

Decision

A brief look at the judgment of the Cantonal Court of second instance

Before delving into the decision of the Federal Supreme Court, it is worth noting two key points of the judgment of the cantonal court of second instance ("the Cantonal Court"):

- First, the Contract was qualified as a **maintenance contract**, i.e. a contract under which one party undertakes to monitor an asset and maintain it in working order (e.g. an IT system) for a fee. Under Swiss contract law, this contract must be qualified as a long-term, '*sui generis*' unregulated (or innominate) contract with similarities to the contract for works and services (363 et seq. SCO). The Cantonal Court held that where the parties provide for a detailed termination mechanism in their contract (which was the case here under the Contract), there was no need to determine whether legal provisions governing regulated contracts apply to termination.

- Second, the Cantonal Court ruled that the Client termination **lacked good cause** and was therefore unjustified and ineffective. It found that the real reason for the Client terminated the Contract appeared to be financial in nature, given that it had been experiencing financial difficulties prior to the termination. Witness testimony also showed that the Client wished to cut costs by relocating its IT department to Eastern Europe (which it eventually did after it notified the IT Provider of the termination of the Contract).

Moreover, even if **numerous patches and updates** had not been installed by the IT Provider, the Cantonal Court found that this did not amount to a material breach of the Contract nor did it constitute a violation of good IT practices by the IT Provider. The reason being that some patches could not be installed because the Client's IT infrastructure was obsolete (the Client's IT budget was insufficient to replace 'end-of-life' hardware), while other patches were deliberately avoided because they could paralyze the Client's business activities.

In addition, the Cantonal Court found that the facts of the case demonstrated that the Client was generally satisfied with the IT Provider's services as the Client never issued any warnings to the IT Provider, and never expressed dissatisfaction during the entire contractual relationship, even though the Client's IT department was subject to an external and an internal audit every year.

In this sense, by failing to notify the IT Provider that its conduct would amount to a breach of the Contract, the Client was deemed to have accepted the services provided by the IT Provider under the Contract, and was precluded from relying on these events as valid grounds for immediate termination of the Contract.

All in all, the breaches cited by the Client in its termination notice were deemed to be no more than a **pretext** to terminate the Contract that had in reality become too costly.[1]

Finally, the Cantonal Court held that the Client could have applied the contractually agreed mechanism and granted the IT Provider a notice to remedy any alleged breaches before terminating the Contract. It failed to do so and therefore had to bear the consequences of its actions.

These findings were not challenged before the Federal Supreme Court.

The decision of the Federal Supreme Court

The Federal Supreme Court ruled on two issues.

(1) First, it had to determine whether the IT Provider had a duty to pay damages to the Client based on Art. 97 para. 1 SCO. It began by recalling **the four conditions for contractual liability**: (1) damage; (2) a breach of contract (i.e. non-performance or improper performance of a contractual obligation); (3) a causal nexus [between the breach and the damage]; and (4) fault, which is presumed. The claimant bears the burden of proof (Art. 8 SCC) and must properly allege the first three conditions.

The Cantonal Court did not rule out the possibility that a breach of contract – which would *not* in and of itself amount to good cause for terminating the Contract – could nevertheless cause damage and give rise to contractual liability on the part of the breaching party under Art. 97 para. 1 SCO. However, in this case, the Cantonal Court found that the Client had **failed to establish a breach of contract** by the IT Provider. In addition, the causal nexus between such potential contractual breach and the poor state of the Client's IT infrastructure was not established.

Given that two of the above-mentioned conditions were not met, the Federal Supreme Court upheld the Cantonal Court's refusal to award damages to the Client under Art. 97 para. 1 SCO.

(2) Second, the Federal Supreme Court had to review the decision of the Cantonal Court to award the IT Provider **full compensation** of the contractually agreed monthly fee for the remaining term of the Contract (i.e. from April 2016 to December 31, 2017).

The Client argued that certain **earnings and savings made following the termination of the Contract** should have been deducted from the damages sought by the IT Provider. The Client alleged that the IT Provider had lost its only customer and was no longer operational, while its manager C. was receiving unemployment benefits. Therefore, the IT Provider was allegedly saving on operational costs.

However, the Client claimed that it was unable to provide the exact amount which should be deducted from the damages due to the IT Provider. For this reason, it claimed that based on Art. 42 para. 2 SCO, the courts should have estimated the value of the alleged savings/earnings at its discretion.

The Federal Supreme Court found, however, that the Client had failed to establish the amount the IT Provider would have saved or earned following the termination of the Contract. It further added that even if Art. 42 para. 2 SCO were applicable, the party alleging damage must still establish all of the circumstances that would enable the court to determine an estimate. Yet the Client had failed to show which of its allegations covered the relevant facts. It also failed to

demonstrate that it had unsuccessfully requested evidence from the IT Provider – evidence that would have enabled it to prove these facts to the court's satisfaction.

On this basis, the Federal Supreme Court held that the Cantonal Court had not misapplied the rules of Swiss contract law when deciding not to deduct any alleged savings or earnings from the damages awarded to the IT Provider.

Key takeaway

In order to validly terminate a long-term IT maintenance contract for breach of contract (namely for alleged IT security breaches), clients must **diligently track, document and notify breaches** committed by their IT provider. Depending on the nature of the breach in question and the agreed termination mechanism, the client may have to grant its IT provider a reasonable time-period to remedy the breach(es).

If a client has wrongfully terminated its IT maintenance contract with immediate effect (i.e. without good cause), it is, as a rule, liable for its undue or unjustified notice of termination. As such, the client must pay damages corresponding to the contractual fees owed to the IT provider until the originally agreed term expired. The client may attempt to reduce the damages to be awarded by any earnings or savings made by the IT Provider as a result of the early termination, based on the IT provider's **duty to mitigate its damage** (Art. 44 para. 1 SCO applicable to contractual damage claims via Art. 99 para. 3 SCO). This requires the client to meet its burden of proof and to properly allege all relevant facts regarding the alleged earnings or savings made by the IT provider.

Comments

1) First, as noted above, the courts found that the Client failed to prove a **breach of contract** by the IT Provider within the meaning of Art. 97 I SCO.

In denying the existence of breach on the part of the IT Provider, the courts gave significant weight to three factual elements:

- **The Client was late in validating the renewal of certain IT contracts** (in particular maintenance contracts for HP servers as well as contracts for electronic storage). This was evidenced by **an email** sent by the IT provider to the Client, in which the IT Provider complained that the Client's delay was negatively impacting "all the [IT] department's functions". In that same email, the IT Provider had expressly warned the Client that it refused to bear any responsibility, namely with respect to the functioning of the IT system, caused by the Client's delay, negligence or lack of management.
- **The general state of the Client's IT infrastructure and its budgetary constraints.** The Client's IT infrastructure was obsolete and its IT budget was insufficient to replace 'end-of-life' hardware. As such, the Client's budgetary constraints obligated the IT provider to operate with outdated IT infrastructure.
- The fact that the Client had **never issued any warning to the IT Provider,** nor expressed any (substantial) dissatisfaction with its services during the entire contractual relationship. In this sense, the Client was deemed to have accepted the services provided by the IT Provider under the Contract. In these circumstances, it was **not sufficient** for the Client to spontaneously commission an external audit and to rely on the findings of the audit report in order to justify the immediate termination of the contract.

These elements made it difficult for the Client to establish a breach by the IT Provider of its contractual obligations.

As evidenced by the first two factors (see (1) and (2) above), the performance of an IT maintenance contract by an IT provider may depend on its client duly performing its own contractual obligations or duties ("*incombances*"/"*Obliegenheit*").[2] This shows the potential interdependence between the contracting parties in a long-term IT maintenance contract and the **shared responsibilities** that may result from this, particularly where the IT provider works in close collaboration with the client or under the supervision of the client's in-house IT staff. In this sense, a client may struggle to claim that its IT provider breached its contractual obligations if the client *itself* has not taken the necessary measures to ensure that the IT Provider can perform its obligations (e.g. by validating the renewal of IT contracts in a timely fashion and by allocating sufficient resources to address its IT needs). Moreover, depending on the industry in which the client operates, companies can be bound by stringent legal obligations that oblige them to **maintain a certain standard of cybersecurity**. This can particularly result from rules on the protection of personal data (e.g. Art. 8

Data Protection Act/Art. 3 Data Protection Ordinance; Art. 32 GDPR), as well as certain industry-specific rules (e.g. FINMA Circulars applicable to the financial industry)[3] or cross-sectorial rules (e.g. EU NIS2 (2022/2555) Directive).[4] From this perspective, companies may have *legal* obligations to ensure a sufficient level of cybersecurity and for which they must therefore allocate adequate resources.[5]

With regards to **proof of a breach of contract** (see (3) above), the lesson is that clients should establish a track record of their IT Provider's performance. Thus, in addition to possible reports, audits or other quality control documents collected during the term of the contract, any issues in maintenance services should ideally be substantiated in writing between the parties or using a well-documented complaint mechanism (e.g. IT support tickets or lists of submitted requests).

Finally, a contracting party under a long-term contract may be expected to notify breaches to the other party and to give a **reasonable time period** for curing such breach before proceeding to terminate the contract. This is what was agreed upon in the Contract in the case at hand. This also results from certain provisions in Swiss contract law (e.g. Art. 107 SCO, Art. 366 SCO).[6] Certain circumstances may justify the termination of the contract with immediate effect (i.e. with no notice period), namely if the relationship of trust is broken (which equates to good cause for termination). For instance, a major IT security breach or cyberattack *may* warrant immediate termination for good cause, but this was not the scenario at play here.

2) In its **second argument**, the Client argued that the IT Provider had violated the **duty to mitigate its damages**, i.e. its duty to do everything that can reasonably be expected of it to reduce the damage that it has suffered. This duty is derived from the principle of good faith (Art. 2 SCC) and its breach may result in a reduction of the amount of damages awarded to the aggrieved party (Art. 44 SCO applicable via Art. 99 III SCO).[7] The party claiming a breach of this duty (by the other party) bears the burden to prove it (Art. 8 SCC).

The SCO expressly provides for such a duty to mitigate damages, for instance, in the event of a premature and unjustified termination of an employment contract (see Art. 337c II SCO).[8] For other contracts, a general argument is made in legal literature that, based on the duty to mitigate damages, the party at the receiving end of an unjustified notice of termination may see **certain earnings or savings deducted from the damages owed to it by the terminating party**.[9]

In the case at hand, the Client claimed that the damages that it was found to owe to the IT Provider should be reduced by the amount corresponding to any savings made by the IT Provider following the early termination of the Contract. It argued that given that the Client had been its only customer for many years, the early termination of their agreement meant that the IT Provider was saving on operational costs. The Client failed, however, to adequately allege and substantiate facts in relation to these alleged savings.

The issue was thus summarily dismissed by the Federal Supreme Court, with no discussion of the relevance of the duty to mitigate damages, nor its scope and extent. And yet the question is one of significant practical importance. Indeed, damages for unjustified termination of a long-term contract aim to restore the other party in the position that it would have been in had the contract been performed until the originally agreed term expired, typically providing full compensation under the contract. Depending on the term (duration) of the contract, this can imply **considerable financial compensation** (in this case, over 18 months' worth of fees at CHF 20,500/month(!)). The ability to deduct earnings made by the other party from substitute mandates, as well as savings related to costs that the other party has avoided or *could have* avoided in good faith after termination (e.g. software licences, subscriptions and other business costs) could have a substantial impact on the amount of damages owed by the terminating party.

Other source commenting the case

Federal Supreme Court Upholds IT Support Contract Termination: Key Lessons on Evidence and Timely Complaints, ICT & Digital @MLL Legal, LinkedIn Post (https://www.linkedin.com/posts/ict-digital-mll-legal_schweizerisches-bundesgericht-willkommen-activity-7237353475691429889-Mygt?utm_source=share&utm_medium=member_desktop)

[1] This approach resonates with another recent decision of the Federal Supreme Court which also dealt with the unjustified termination of a long-term IT contract and in which the *real* cause for termination was deemed to be financial in nature as well (i.e. lost profits due to outdated equipment). See the judgment of the Federal Supreme Court, 4A_573/2020/4A_575/2020, commented on this platform: Maxime Francis/Marianna Sorton, *Unilateral termination of a long-term IT contract: when is good cause not good enough?*, published on: Swiss Contract Law, August 16,

2022, https://swisscontract.law/18/.

[2] A duty can be defined as an act (or set of acts) that a party must abide by in order to avoid losing the benefit of certain rights; unlike an obligation, a party cannot be compelled to perform a duty (see Pierre Tercier/Pascal Pichonnaz, Le droit des obligations, 7 ed. 2024, N 326).

[3] See e.g. FINMA Circular 2023/1 on Operational risks and resilience – banks (entered into force in January 2024).

[4] The EU Directive 2022/2555 on measures for a high common level of cybersecurity across the Union as well as the EU Commission Implementing Regulation for IT-Service providers 2024/2690 (EU-CER (2022/2557) ; see in particular Art. 2 et seq. and related Annex).

[5] A commitment to conformity with standards can also be voluntary, see e.g. ISO/IEC 27001 Standard for information security management systems (ISMS).

[6] For another example, see judgment of the Federal Supreme Court, 4C_393/2006, of April 27, 2007, para. 3.3.3, where a provider was expected to put its client on notice before terminating a software-development contract.

[7] According to some legal commentators, the duty may be attributed to Art. 42 SCO instead (see Franz Werro/Vincent Perritaz, art. 44 N 26 and references, *in* Commentaire Romand, Code des obligations I [Luc Thévenoz/Franz Werro, edit.], 3 ed., Basel 2021).

[8] Under this provision, damages will be reduced by any amount that the employee has saved as a result of the early termination of the employment relationship or that it has earned by doing other work (or *would have* earned had it not intentionally foregone such work). See also: Art. 264 para. 3 SCO (early termination (restitution) in a lease agreement) or Art. 377 SCO (termination of a contract for works and services against full compensation of the contractor).

[9] See Marie-Noëlle Venturi-Zen-Ruffinen, La résiliation pour justes motifs des contrats de durée, 2007 Fribourg, N 1510; on IT contracts in particular, see Michel Jaccard/Vincent Robert, Les contrats informatiques, in: Pascal Pichonnaz/Franz Werro (ed.), La pratique contractuelle, Genève 2009, 95 et seq., at 123.

Reproduction authorized with the following reference : Jacques de Werra, Marianna Sorton , "Termination of an IT Maintenance Contract for Alleged Security Breaches: What Must the Client Prove?", published on: Swiss Contract Law, 2024-12-17 14:46:26, https://swisscontract.law/35/