Baker McKenzie.

Client Alert

January 2024

Switzerland: New obligation to report cyber incidents

In brief

The Federal Information Security Act (ISA), which only entered into force on 1 January 2024 is already being amended with an obligation to report cyberattacks for operators of critical infrastructures. The term "critical infrastructures" is defined in a broad manner and captures many private companies. On 18 January 2024, the deadline for challenging the amendment by way of a public referendum expired. This means that the amended version ("**revISA**") will become law, with the new obligation to report cyberattacks expected to come into force in 2025, although an exact date has not yet been set.

In this alert, we address the most pressing questions around this new reporting obligation and provide you with important takeaways.

Contents

Important takeaways

- The new far-reaching reporting obligation applies, to cyberattacks "in Switzerland" even if the IT resources concerned are located abroad — as long as the incident has an impact on Switzerland.
- The reporting obligation applies to operators of critical infrastructures, such as banks and insurance companies, certain telecommunications providers, and providers and operators of cloud computing with registered offices in Switzerland. That said, the list of affected companies is even broader and covers, for example, companies that supply essential everyday goods and whose failure or impairment may lead to considerable supply bottlenecks as well as manufacturers of hardware or software whose products are used by operators of critical infrastructure (a comprehensive list is set out in article 74b revISA).
- Reports must be submitted to the recently established Federal Office for Cybersecurity (BACS) (previously called the National Cyber Security Centre (NCSC)).
- Reports must be made within 24 hours following the discovery of the cyberattack and can be made anonymously.
- Reporting obligations under the revISA, the Data Protection Act (FADP) and the FINMA Act (see article 29(2) and FINMA Guidance 05/2020) differ and apply independently.
- Breach of the reporting obligation under the revISA can lead to a fine of up to CHF 100,000.

Q&A

Which incidents must be reported?

Only cyberattacks are subject to the reporting obligation. A cyberattack is a cyber incident that was caused with intent. A cyber incident is defined as an "event in the use of IT resources that results in the confidentiality, availability or integrity of information or the traceability of its processing being compromised".

In particular, an incident needs to be reported if it meets the following cumulative requirements:

1. Intentional causation of the cyber incident or impairment.
2. Impairment of any of the following protective goals (alternatively):
    a. Confidentiality of information.
    b. Availability of information.
    c. Integrity of information.
    d. Traceability of the processing of the information.
3. Impairment caused during the use of IT resources.
4. Cyberattacks that fulfill any of the following conditions:
    a. Jeopardizes the functionality of the critical infrastructure concerned.
    b. Has led to a manipulation or outflow of information.
    c. Remained undetected for an extended period of time, especially if there are indications that it was carried out in preparation for further cyberattacks.
    d. Is associated with blackmail, threats or coercion.
5. The cyberattack has an impact on Switzerland regardless of whether the IT resources concerned are located in Switzerland or abroad.

Who has to report?

The reporting obligation applies to:

1. Universities, in accordance with Article 2 paragraph 2 of the Higher Education Funding and Coordination Act of 30 September 2011.
2. Federal, cantonal and communal authorities as well as intercantonal, cantonal and intercommunal organizations, with the exception of the Defense Group ("*Gruppe Verteidigung*"), if the armed forces perform assistance service in accordance with Article 67 or active service in accordance with Article 76 of the Military Act of 3 February 1995.
3. Organizations with public law tasks in the areas of security and rescue, drinking water supply, waste water treatment and waste disposal.
4. Companies that are active in the areas of energy supply in accordance with Article 6 paragraph 1 of the Energy Act of 30 September 2016, energy trading, or energy measurement or energy control, with the exception of license holders in accordance with the Nuclear Energy Act of 21 March 2003, if a cyberattack is carried out on a nuclear installation.
5. Companies that are subject to the Banking Act of 8 November 1934, the Insurance Supervision Act of 17 December 2004, or the Financial Market Infrastructure Act of 19 June 2015..
6. Healthcare facilities that are included on the cantonal hospital list in accordance with Article 39 paragraph 1 letter e of the Federal Health Insurance Act of 18 March 1994.
7. Medical laboratories licensed in accordance with Article 16 paragraph 1 of the Epidemics Act of 28 September 2012.
8. Companies that have a license to manufacture, place on the market and import medicinal products in accordance with the Therapeutic Products Act of 15 December 2000..
9. Organizations that provide benefits to protect against the consequences of illness, accident, incapacity to work and earn, old age, disability and helplessness.
10. The Swiss Radio and Television Corporation.
11. News agencies of national importance.

12. Providers of postal services that are registered with the Postal Commission in accordance with Article 4 paragraph 1 of the Postal Act of 17 December 2010.
13. Railroad undertakings pursuant to Article 5 or 8c of the Railways Act of 20 December 1957 as well as cableway, trolleybus, bus and shipping companies with a license pursuant to Article 6 of the Passenger Transport Act of 20 March 2009.
14. Civil aviation companies that have a license from the Federal Office of Civil Aviation and the national airports in accordance with the sectoral aviation infrastructure plan.
15. Companies that transport goods on the Rhine in accordance with the Maritime Navigation Act of 23 September 1953, as well as companies that register, load or unload goods in the port of Basel.
16. Companies that supply the population with essential everyday goods and whose failure or impairment would lead to considerable supply bottlenecks.
17. Providers of telecommunications services that are registered with the Federal Office of Communications in accordance with Article 4 paragraph 1 TCA.
18. Registry operators and registrars of internet domains in accordance with Article 28b TCA.
19. Providers and operators of services and infrastructures which serve the exercise of political rights.
20. Providers and operators of cloud computing, search engines, digital security and trust services and data centers, provided they have a registered office in Switzerland.
21. Manufacturers of hardware or software whose products are used by critical infrastructures, provided that the hardware or software has remote maintenance access or is used for one of the following purposes:
    a. Control and monitoring of operational systems and processes.
    b. Ensuring public safety.

Who do I have to report to?

The draft still provides for reporting to the National Cyber Security Centre (NCSC). However, the NCSC has ceased to exist after its functions and staff were transferred to the newly established Federal Office for Cybersecurity (BACS) on 1 January 2024. It can therefore be assumed that reports will have to be submitted to the BACS. A corresponding portal for reporting a cyber incident is on the BACS website.

Within which timeframe do I have to report and what is the content of the notification?

A report must be made within 24 hours following the discovery of a cyberattack. Information must be provided on the company subject to the reporting obligation, the type and execution of the cyberattack, its effects and the measures taken. If further action is already known, this must also be reported. The fact that information must be provided about the company subject to the reporting obligation must not be misunderstood as an obligation to name the company. The law expressly provides for the possibility of anonymous reporting.

The law explicitly stipulates that no information must be provided that would incriminate the person who has to fulfill the reporting obligation for a company.

Obviously, 24 hours is a very tight deadline, which is why the law stipulates that information that is not yet available can be submitted later.

What happens if I do not report?

If a company subject to the reporting obligation fails to comply with its reporting obligation and BACS becomes aware of this, BACS will first inform the company and set a deadline. If the company allows this deadline to pass without reporting, the BACS will issue an order, set a new deadline and refer to the potential fine. If the company fails to comply with this order, a fine of up to CHF 100,000.00 may be imposed.

What happens after I have reported?

The report is analyzed by the BACS. The reports are used by the BACS to identify attack patterns, recognize them at an early stage, and recommend suitable preventive and defensive measures.

A request can be made to the BACS for a recommendation on how to proceed. In addition, companies that are obliged to report a cyberattack may be entitled to support from the BACS in dealing with the incident.

The BACS is authorized to publish information on cyber incidents if this serves to protect against cyber threats. This information may only provide information about the natural or legal person concerned if they consent to it and it concerns misused identification features and addressing resource.

The BACS is also entitled to forward reported information to authorities and organizations that are active in the area of cyber security. This information may only include personal data if the data subject consents.

How does this new obligation interplay with existing reporting obligations under Data Protection and financial market law?

The Swiss Data Protection Act (FADP) provides for a reporting obligation in case of a data breach. This reporting obligation differs from the reporting obligation under the revISA in a number of ways, including as follows:

1. **RevISA is not limited to personal data:** While under the FADP a data security breach must only be reported if personal data is affected, under the revISA a reporting obligation also exists if no personal data is involved.
2. **RevISA requires intent:** According to the FADP, no intentional breach of data security is required to trigger the notification obligation.
3. **Addressees of the reporting obligation under the revISA — exhaustive list:** The operators of critical infrastructures subject to the reporting obligation under the revISA are listed exhaustively in the law (article 74b revISA). A reporting obligation under the FADP generally applies to all companies in their function as data controllers.
4. **RevISA only for the use of IT resources:** A reporting obligation under the revISA only exists if the cyber incident was caused by the use of IT resources. The reporting obligation under the FADP does not require this and also exists, for example, if a person steals physical files.
5. **Criminal liability under the revISA:** A breach of the reporting obligation leads to criminal liability if a corresponding order of the BACS is violated. A breach of the reporting obligation under the FADP is not directly punishable, but the implementation of inadequate technical and organizational measures potentially is.

In view of these differences, it must be examined in relation to each cyber incident whether a report must be submitted in accordance with the revISA, the FADP or both laws. With the revISA entering into force, the FADP will be revised and a new article 24 paragraph 5bis will be added, according to which the Federal Data Protection and Information Commissioner (FDPIC) may forward data breach reports to the BACS if the data controller agrees.

For completeness, in addition to the reporting obligation under the FADP and the new reporting obligation under the revISA, Swiss financial institutions licensed under Swiss financial market regulations are subject to yet another reporting obligation related to cyber incidents. Namely, under article 29 paragraph 2 of the Federal Act on the Swiss Financial Market Supervisory Authority (FINMASA), licensed financial institutions have to report any cyber incidents that are of "substantial importance to the supervision." To provide guidance to licensed financial institutions, FINMA has issued Guidance 05/2020.

Contact Us

Alessandro Celli
Partner
Zurich
alessandro.celli
@bakermckenzie.com

Christoph Kurth
Partner
Zurich
christoph.kurth
@bakermckenzie.com

Julia Schieber
Partner
Zurich
julia.schieber
@bakermckenzie.com

Eva-Maria Strobel
Partner
Zurich
eva-maria.strobel
@bakermckenzie.com

Johanna Mösch
Associate
Zurich
johanna.moesch
@bakermckenzie.com

Meera Rolaz
Associate
Zurich
meera.rolaz
@bakermckenzie.com

Nicole Schön
Associate
Zurich
nicole.schoen
@bakermckenzie.com