

December 16 2022

# Measures to improve security of telecoms networks effective as of 1 January 2023

Walder Wyss Ltd | Tech, Data, Telecoms & Media - Switzerland

- › [Introduction](#)
- › [Improved reporting duty for telecoms operators](#)
- › [Increased network security](#)
- › [Enhanced security of 5G networks](#)

## Introduction

In a press release dated 16 November 2022 (available in [French](#), [German](#), [Italian](#) and [English](#)), the Federal Council announced the implementation of a series of measures to strengthen the security of telecoms networks. These enhancements will be set out in the revised Ordinance on Telecommunications Services (rOTS), which is due to enter into force on 1 January 2023.

Telecoms operators will be required to inform the National Emergency Operations Centre (NEOC) if a network outage could affect at least 10,000 customers. Furthermore, internet service providers (ISPs) will have to step up the anti-tamper mechanisms for their telecoms systems. Last, but not least, the security requirements of 5G networks will be strengthened.

## Improved reporting duty for telecoms operators

In order to improve the reporting of incidents, telecoms operators will have to announce disruptions to telecoms systems as soon as they affect 10,000 customers, instead of 30,000, as it currently stands. Additionally, instead of submitting notifications to the Federal Office of Communications (OFCOM), as has been the case up until now, notifications will have to be made to the NEOC, which operates around the clock. This will allow disturbances to be dealt with in real time, which is particularly important for crisis management. The NEOC will then pass on the information to the OFCOM. In addition, network outages will have to be published on an open-access website.

## Increased network security

ISPs will be required to reinforce their anti-piracy mechanisms to increase network security. For instance, an ISP detecting malicious activity on a website, such as a phishing attempt, must be able to block or restrict the internet connection. These enhanced anti-tamper mechanisms will also serve the purpose of isolating infected or vulnerable devices. Furthermore, ISPs will have to operate a special unit that receives reports of tampered telecoms devices. ISPs will also be required to strengthen the existing measures against cyberattacks, particularly regarding those cyberattacks aiming to make servers, services or infrastructures unavailable. For example, ISPs will have to find a way to filter and extract data that originates from their network but uses a false source IP address.

## Enhanced security of 5G networks

The new regulation adopted by the Federal Council also takes recent technological developments in the field of telecoms into account. To this extent, the rOTS address the security of next-generation (ie, 5G) mobile networks and the services operated on them. For instance, telecom operators will be required to implement an information security management system that meets the OFCOM's requirements.

In addition, network operation and security management centres will be allowed to be located in Switzerland or in another country whose legislation guarantees an adequate level of data protection.

Moreover, in the context of the renewal of the allocation of mobile frequencies scheduled for 2027-2028, the Federal Council has instructed the Federal Ministry of the Environment, Transport, Energy and Communications to examine whether mobile network operators should be required to operate their centres exclusively in Switzerland.

*For further information on this topic please contact [Jürg Schneider](#), [Hugh Reeves](#) or [Marc Grezella](#) at Walder Wyss by telephone (+41 58 658 58 58) or email ([juerg.schneider@walderwyss.com](mailto:juerg.schneider@walderwyss.com), [hugh.reeves@walderwyss.com](mailto:hugh.reeves@walderwyss.com) or [marc.grezella@walderwyss.com](mailto:marc.grezella@walderwyss.com)). The Walder Wyss website can be accessed at [www.walderwyss.com](http://www.walderwyss.com).*



JÜRIG  
SCHNEIDER



HUGH REEVES



MARC  
GREZELLA