



O2 Czech Republic a.s. Prague, Czech Republic

SYSTEM AND ORGANIZATION CONTROLS (SOC) 3 REPORT

REPORT ON CONTROLS AT SERVICE ORGANIZATION
RELEVANT TO DESCRIPTION OF O2 CZECH REPUBLIC
A.S. SYSTEM AND ON THE SUITABILITY OF THE DESIGN
AND OPERATING EFFECTIVENESS OF CONTROLS TO
MEET THE CRITERIA FOR THE SECURITY, AVAILABILITY,
CONFIDENTIALITY, PROCESSING INTEGRITY AND
PRIVACY.

THROUGHOUT THE PERIOD
2023-12-01 THROUGH 2024-11-30

TABLE OF CONTENTS

TABLE OF CONTENTS	1
I. INDEPENDENT SERVICE AUDITOR'S REPORT	4
II. ASSERTION OF O2 CZECH REPUBLIC A.S. MANAGEMENT	8
III. ATTACHMENT A	10
DESCRIPTION OF THE BOUNDARIES OF THE O2 CZECH REPUBLIC A.S. SYSTEM	10
O2 CZECH REPUBLIC A.S. COMPANY PROFILE	11
ORGANISATIONAL STRUCTURE	11
KEY RESPONSIBILITIES	11
POLICIES AND PROCEDURES	12
SYSTEM COMPONENTS USED TO PROVIDE THE SERVICE	12
CONTROL ENVIRONMENT	19
CODE OF CONDUCT AND ETHICS.....	20
INFORMATION AND COMMUNICATION.....	21
MONITORING	22
RISK ASSESSMENT PROCESS.....	23
HR MANAGEMENT.....	23
PHYSICAL SECURITY.....	24
ACCESS CONTROL.....	25
ENDPOINT PROTECTION	25
CHANGE MANAGEMENT.....	25
DISASTER RECOVERY	26
VULNERABILITY MANAGEMENT.....	27
IV. ATTACHMENT B	29
DESCRIPTION OF A O2 CZECH REPUBLIC A.S. SERVICE ORGANIZATION'S PRINCIPAL SERVICE	
COMMITMENTS AND SYSTEM REQUIREMENTS	29
SERVICE COMMITMENTS	29
SYSTEM REQUIREMENTS	29
PRIVACY	30
AVAILABILITY	31
CONFIDENTIALITY	31
PROCESSING INTEGRITY	32

EXECUTIVE SUMMARY

Scope	Cloud
	O2 Cloud (VDC)
	O2 Privátní cloud
	O2 Zálohování
	O2 Zálohování VDC
	O2 NGFW Advance
	O2 NGFW Premium
	O2 Antispam
	O2 AntiDDoS
	SIEM
	Log Management
Period of Examination	December 1, 2023, to November 30, 2024,
Applicable Trust Principle(s)	Security, Availability, Confidentiality, Processing Integrity, and Privacy
Location (s)	Prague, Czech Republic
Subservice Providers	O2 IT services s.r.o.
	CETIN, a.s.
Opinion Result	Unqualified

I. Independent Service Auditor's Report

I. INDEPENDENT SERVICE AUDITOR'S REPORT

To: Board of Directors of O2 Czech Republic a.s.

Scope

We have examined O2 Czech Republic a.s. (“O2 Czech Republic” or the “service organization”) accompanying description of its system entitled “Description of O2 Czech Republic a.s.”, including application maintenance and support services provided by and controls operated by O2 IT services s.r.o. and CETIN a.s. Subservice Organization (O2 ITS and CETIN), throughout the period December 1, 2023 to November 30, 2024, (description) based on the criteria set forth in paragraph 1.26 of the AICPA Guide Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality and Privacy (SOC 2®) (description criteria) and the suitability of the design and operating effectiveness of controls, included in the description throughout the period December 1, 2023 to November 30, 2024 to meet the criteria for security, availability, processing integrity, confidentiality and privacy set forth in TSP section 100, *2017 (update 2022) Trust Services Criteria for Security, Availability, Processing Integrity and Confidentiality in AICPA Trust Services Criteria*.

O2 IT services s.r.o. is an independent subservice organization providing application maintenance and support services to O2 Czech Republic a.s. The description includes those elements of the application maintenance and support services provided to O2 Czech Republic a.s. and the controls designed by O2 Czech Republic a.s. and operated by O2 IT services s.r.o. that are necessary for O2 Czech Republic a.s. to achieve its service commitments and system requirements based on the applicable trust services criteria.

Service Organization’s Responsibilities

O2 Czech Republic has provided the accompanying assertion titled, “Management of O2 Czech Republic’s Assertion,” (assertion) about the fairness of the presentation of the description based on the description criteria and suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria. O2 Czech Republic is responsible for preparing the description and assertion; including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; identifying the risks that would prevent the applicable trust services criteria from being met; designing, implementing, and documenting controls that are suitably designed; and operating effectively to meet the applicable trust services criteria stated in the description.

Service Auditor’s Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period December 1, 2023 to November 30, 2024 to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

O2 Czech Republic uses O2 IT services s.r.o., a subservice organization, to provide infrastructure as a service. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at O2 Czech Republic, to achieve O2 Czech Republic's service commitments and system requirements based on the applicable trust services criteria. The description presents O2 Czech Republic's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of O2 Czech Republic's controls.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement. Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve O2 Czech Republic's service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve O2 Czech Republic's service commitments and system requirements based on the applicable trust services criteria.

Subservice Organization's Responsibilities

O2 IT services s.r.o. has provided the accompanying assertion titled "O2 IT services s.r.o." about the description and the controls stated therein. O2 IT services s.r.o. is responsible for preparing the portion of the description related to the application maintenance and support services provided to O2 Czech Republic a.s. and the O2 IT services s.r.o. assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; and implementing, operating, and documenting controls designed by O2 Czech Republic a.s. which enable O2 Czech Republic a.s. to achieve its service commitments and system requirements.

Inherent Limitations

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within O2 Czech Republic's transportation management system were effective throughout the period December 1, 2023 to November 30, 2024 to provide reasonable assurance that O2 Czech Republic's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

BDO Consulting s.r.o.

20.01.2025

II. Assertion of O2 Czech Republic a.s. Management

II. ASSERTION OF O2 CZECH REPUBLIC A.S. MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within O2 Czech Republic a.s. Service Organization's (O2 CZ's) transportation management system (system) throughout all of the period: December 1, 2023 to November 30, 2024, to provide reasonable assurance that O2 Czech Republic a.s.'s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, processing integrity and privacy (applicable trust services criteria) set forth in TSP section 100, 2017 (update 2022) Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteria. Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout all of the period: December 1, 2023, to November 30, 2024, to provide reasonable assurance that O2 Czech Republic a.s.'s service commitments and system requirements were achieved based on the applicable trust services criteria. O2 Czech Republic a.s.'s objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls stated in the description operated effectively throughout all of the period: December 1, 2023, to November 30, 2024, to provide reasonable assurance that O2 Czech Republic a.s.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

III. Attachment A
Description of the boundaries of the O2
Czech Republic a.s. system

III. ATTACHMENT A

DESCRIPTION OF THE BOUNDARIES OF THE O2 CZECH REPUBLIC A.S. SYSTEM

O2 Cloud brings new possibilities to build a modern global IT infrastructure. O2 Cloud enables improved customer service, increased process speed, reduced operational complexity (installation and operating costs, asset management and control) and enhanced security.

O2 Security services include Next Generation Firewall, AntiDDoS and Antispam to protect customers communicating over the internet, by e-mail and corporate IT.

O2 Security Expert Centre offers complete protection of the customer's ICT environment based on log management tools, SIEM and an expert security team.

This report has been prepared to provide information on internal controls of O2 that may be relevant to customers seeking security, availability, processing integrity, confidentiality, and privacy.

The scope covered in the report includes the following services:

Cloud services (O2 Cloud)

- Virtual data center (VDC)
- Private cloud
- Virtual data center - SQLaaS
- MBR Backup
- VDC Backup
- Veeam Cloud Connect

Security services (O2 Security)

- NGFW Advanced
- NGFW Premium
- O2 AntiDDoS Standard
- O2 Antispam

Security Expert Centre services (O2 SEC)

- Security expert Centre - SIEM (SIEM service)
- Security expert Centre - LM (Log management)
- Security expert Centre

The scope of locations covered in this report includes facilities located in the Czech Republic:

- Praha, Za Brumlovkou 266/2, 140 00 (Headquarters)
- Praha, V lomech 2339/1, 149 00 (Data Centre Chodov)
- Praha, K Zahrádkám 2065/2, 155 00 (Data Centre Stodůlky)

O2 CZECH REPUBLIC A.S. COMPANY PROFILE

O2, the leading telecommunications operator on the Czech market, continues its mission to deploy technologies that improve people's everyday lives. O2 provides voice, internet and data services to customers ranging from households and small and medium-sized businesses to large corporations and governmental organizations. Right now, O2 is building a fifth-generation mobile network (5G), launched as the first one into commercial operation. The O2 mobile network also includes virtual operators offering their services such as BLESKmobil, Tesco Mobile and MOBIL OD ČEZ. At the same time, O2 is the largest provider of internet for households and businesses, offered to 99% of addresses.

With its O2 TV service, O2 is the country's largest operator of TV over the internet. Having purchased a number of sports licenses, O2 is able to offer its customers the most appealing sports content on the Czech market. O2 is one of the key players in the field of hosting and cloud services, as well as managed services and ICT. As trends in the telecommunications industry change significantly, O2 also focuses on the development and offering of non-traditional telecommunications services. These include financial services such as hardware insurance or mobile travel insurance. Organizational structure The company is headed by the Board of Directors. The Chief Executive Officer (CEO) reports to the Board. The executive line of the organisational structure reporting directly to the Chief Executive Officer includes the following divisions and units: Commercial Division, Technology Division, Finance Division, Legal and Regulatory Affairs Division, Human Resources Division, Security unit, Public Administration Unit, Wholesale Services Division, Corporate Communications Unit and General Secretariat Department. The Company's top management consists of the Company's Board of Directors, the Chief Technology Officer (CTO) and the Chief Commercial Officer (CCO). The Company also has an Executive Committee as an advisory body to the Chief Executive Officer. The members of the Executive Committee are Directors of the Commercial Division, the Technology Division, the Finance Division, the Legal and Regulatory Affairs Division, the Human Resources Division and the Corporate Communication Department.

ORGANISATIONAL STRUCTURE

The company is headed by the Board of Directors. The Chief Executive Officer (CEO) reports to the Board. The executive line of the organizational structure reporting directly to the Chief Executive Officer includes the following divisions and units: Commercial Division, Technology Division, Finance Division, Legal and Regulatory Affairs Division, Human Resources Division, Security unit, Public Administration Unit, Wholesale Services Division, Corporate Communications Unit and General Secretariat Department. The Company's top management consists of the Company's Board of Directors, the Chief Technology Officer (CTO) and the Chief Commercial Officer (CCO). The Company also has an Executive Committee as an advisory body to the Chief Executive Officer. The members of the Executive Committee are Directors of the Commercial Division, the Technology Division, the Finance Division, the Legal and Regulatory Affairs Division, the Human Resources Division and the Corporate Communication Department.

KEY RESPONSIBILITIES

In O2, responsibilities are set out primarily in the Organizational Rules, which summarize the essential information about the company, determine the system of internal management and organization, define the responsibilities and accountabilities of all company bodies, units and individual employees, determine the reporting lines of the units and responsibilities towards the company bodies including the system of internal management documentation.

As to the services described in this SOC3 report, the following O2 units are of crucial importance:

Product management teams provide and coordinate the development of products and services including launch; manage the lifecycle of products and services.

The network teams take care of the operation of O2 security services, including the operation of the inevitable infrastructure, other teams are dedicated to providing O2 SEC services to O2 customers, including the operation of the inevitable infrastructure.

The Security unit defines and enforces the company's strategy and security policy, manages and defines security measures, promotes the implementation of the measures and controls how these are followed in all areas of physical, information and cyber security.

Suppliers used by O2, namely CETIN (a sister organization) and O2 IT Services (a daughter organization), have significant responsibilities, too.

CETIN owns the data centers used by O2 to operate its cloud services. CETIN thus provides O2 with services for the operation of non-IT infrastructure, is responsible for the availability as well as the physical protection of the data centers and access to the data centers. The data centers are certified for TIER/RATE III.

O2 IT Services operates hardware, and the virtualization platform used for the O2 Cloud services and ensures the performance of the Service Desk.

POLICIES AND PROCEDURES

The Company's activities are governed by general legal regulations, the Articles of Association and O2 internal management documents regulating all internal management systems and organisation.

The management documents set out in detail the principles, rules and procedures for internal managing activities, taking into account their specific importance, location, technology, goals and other relevant parameters. Based on the company's strategy, policy and objectives, the management documents incorporate in detail all mandatory elements of external legislation into the company's conditions.

The rules for the administration and management of the corporate management document system are defined in a separate document.

SYSTEM COMPONENTS USED TO PROVIDE THE SERVICE

Infrastructure

Cloud and backup services

The provision of cloud and backup services is the role of O2 ITS, an organization responsible for the operational part of services such as O2 VDC, O2 Private Cloud, O2 Backup VDC and O2 Backup. The services are operated at CETIN data centers in two

locations, Praha Chodov (DC CH) and Praha Stodůlky (DC JZM) with the 24x7x365 monitoring.

The server infrastructure is built on a farm of servers from the world's leading vendors combined with the state-of-the-art virtualization technologies at the High Availability level. All the servers, including the infrastructure are connected redundantly to minimize the downtime due to technology failures. Guaranteed service availability is 99.9%.

O2 Next Generation Firewall

NGFW is designed with the concept of concentrating top-class HW security elements and centralized security in one place. It's because this solution is better in terms of costs, performance and durability than the concept of spread security. Using centralized security, one can achieve the same or higher level of security at lower acquisition and operating costs.

Centralized services over the communication infrastructure dramatically reduce the likelihood of intrusion from the external environment into customer's internal IT environment and create conditions for the customer and the provider to better coordinate their steps in the effort to fight against potential hackers.

NGFW is a geographically redundant security infrastructure developed by backing up production elements in two identical branches located in two different locations, thus achieving great service reliability and availability. NGFW is located at hosting centers meeting strict security requirements with strict parameters, designed and operated at the Tier III level (under the Uptime Institute classification).

The environment meets the following requirements of computing and communications security:

- redundant data connectivity is connected to two independent directions terminated on separate technology in different buildings/facilities,
- communication infrastructure used for the provision of services is technically and geographically redundant,
- Communication infrastructure is located in a safe environment of a hosting center or equivalent environment,
- access to the management system of elements and services (local and remote) is controlled in an environment separated from customer environment and,
- infrastructure is controlled by skilled professionals with adequate certifications.

Safety requirements are guaranteed and adhered to throughout the entire term of contract. The O2 CZ ISP network consists of two independent locations providing peering connectivity.

O2 AntiDDoS

The O2 CZ ISP network consists of two independent locations providing peering connectivity with local peering (NIX) and transit internet connectivity provided by several different upstream providers (Tier1 ISPs).

As to AntiDDoS, O2 uses platform implemented in the network with regard to various parameters such as size, geolocation, etc.

The implementation consists of 3 sections:

- CP, which includes the analytical part of the system,
- TMS containing mitigation part,

- PI - portal interface for customers.

All configuration changes of TMS are performed in a CP device. The CP device creates BGP peering with the affected routers (ISP border routers) such as BGP host (RRC route reflector client) and receives all BGP notifications received or forwarded by ISP routers. The CP device is connected to border routers to receive NetFlow data, used as the main source for analyzing behavior and traffic. Once the CP device flags some traffic as suspicious, request will be sent to TMS for BGP rerouting the suspicious traffic for further investigation. If the traffic is classified as a DoS/DDoS attack, TMS will discard the unwanted traffic, or send it back via the original route to be later delivered to the destination.

O2 Antispam

O2 Antispam is a service using the system to detect spam. Principally, the service is a public e-mail gateway in the O2 infrastructure, in which a unique account is created for the user to administer the security policy of a protected domain or multiple domains. Next, in the domain provider location, using the MX record, change of delivery to the email gateway, serving as protection, will be made. The email gateway will then offer the user a total security solution as a service bearing in mind the plethora of various internet threats.

Malware (i.e. viruses, Trojan horses, spyware, etc.), spam, vulnerabilities, networks of infected computers (botnets), fraudulent emails, files and websites (phishing and pharming) and many more represent potential security threats to enterprises and their business. In addition to its own antispam functionality, O2 Antispam offers quarantine for the captured messages (to eliminate what is called “false positive”). The service can be implemented separately and does not require other services such as NGFW.

O2 Security Expert Centre

The aim of deploying O2 SEC is to boost the security of the IT environment and get a picture of what is happening on the network and endpoints in order to better identify and eliminate ongoing threats in a timely manner.

The service provides the following functionalities:

- collection, storage and analysis of logs of the defined systems,
- security monitoring (no need for customer to do monitoring internally).
- A central model of security monitoring/control for all organizations within a group.

The Service uses tools provided as part of the Service operated by O2. HW/SW probes are placed in the customer location to monitor traffic in the network (network probe). The tools include, in particular:

- Log management
- SIEM

The service includes a combination of complementary services aimed at protecting customers against all sorts of cyber threats that can bypass standard perimeter protection, antivirus systems to pose long-term or permanent threats to customer security and business, while creating an environment compliant with all legislative requirements. O2 SEC includes the 24x7x365 monitoring with proactive security control and periodical reviewing of cyber security events. The proposed solution provides a multitenant environment allowing the customer to select the setting of the form of visibility for individual supervised entities i.e. selective approach in terms of policies and reporting.

Logs are collected from devices defined by the customer and sent to what is called collectors. Collector is a collection point in the customer network installed as a virtual appliance in an HA setup in customer's DMZ network.

The collectors are connected to the firewall in the O2 Security Expert Centre via a secure connection (VPN, TLS, etc.). Stream processors process logs using log management functionalities, real-time or non-real-time SIEM. The solution is built as an HA active - active cluster.

O2 SEC includes systems for detecting anomalies in network traffic. The systems monitor the O2 SEC environment as a whole and provide audit trails. Another part of O2 SEC is the ticketing system, used as one of the communication channels between O2 SEC and the customer. Customers can use a web interface.

The offered solution is designed as highly available (HA) with implicit load balancing.

Software

Cloud and backup services

Cloud and backup services are structured into several PODs representing clusters of interconnected servers with hypervisor. Located in data centers, the clusters provide computing power to run customer environments. The role of hypervisor is played by market leading virtualization platform, run on a multi-tenant layer, a portal allowing customers to manage their environments. All servers in the clusters are equipped with SSDs and use vSAN to deliver great data speed and availability.

In both data centers there are separate PODs for SQLaaS. The PODs are optimized to run SQL and contain a high-frequency CPU. The servers in the PODs are fully licensed to run SQL databases. Along with the infrastructure, SPLA licenses are offered for the services: OS Windows server Standard license, RDS license, Application license for MS SQL Standard and Enterprise, RHEL license.

The VDC Backup service uses specialized software from Veeam, which provides advanced features for data backup and recovery in a virtualized environment.

O2 Next Generation Firewall

The company uses a firewall that connects all security and network components to ensure seamless integration. This enables the convergence of network and security features to deliver consistent user experience and resilient security position across all types of environments, including on-premises, cloud, hybrid, and convergent IT/OT/IoT infrastructure.

O2 AntiDDoS

The company uses a solution used to detect DDoS attacks. The system allows you to monitor network traffic and use data for smart traffic analysis, usage optimization, intelligent network expansion planning, threat elimination and reporting for customers and users.

The system is able to remove malicious parts from a communication session without disrupting other key network services.

O2 Antispam

The company uses an operating system that ranks among the largest cybersecurity platforms on the market, organically built on a common governance and security framework. It connects all necessary security and networking components to ensure seamless integration. This enables the convergence of network and security functions to ensure a consistent user experience and resilient security posture across all types of

environments, including on-premises, cloud, hybrid and converged IT/OT/IoT infrastructures.

The system is an organically evolving system augmented with new features to increase the potential to provide unprecedented visibility and enforcement in hybrid environments. Additionally, the system accelerates security operations through AI-driven prevention, automation and real-time response. Furthermore, the system offers secure network management, increased prevention, early detection and real-time response, and reduced risk of various cyber threats.

O2 Security Expert Centre

O2 SEC takes cyber security as no.1 priority using professional tools from renowned manufacturers. The workplace has a sophisticated software ecosystem designed to monitor and immediately identify all potential cyber threats. The software used for log management and SIEM services enables compliance with relevant cybersecurity legislation, GDPR and ISO 27001.

People

The actual operation and development of Cloud services requires the involvement of several different roles ranging from technical to commercial ones. The operation of these services is the responsibility of O2 IT Services, taking care of the technical operation of the service, including the Service Desk. The operation of security services is provided by O2 Czech Republic. Key technical roles for cloud services include Solution Architect, Service Manager and Operations Specialist. Commercial, security and network infrastructure fall among the roles of O2 Czech Republic. The roles include Product Manager, Segment Manager, Sales and Presales Manager, Security Specialist and Network Infrastructure Specialist. All roles of security services are delivered by O2 Czech Republic. To confirm the level of competency of our core service providers, VMware, Veeam Software and Fortinet, we maintain a certain level of partnership, evidence of which is the required number of specialized certifications. You can check our partnership level on our vendors' websites - VMware, Veeam Software and Fortinet. Our goal is to continuously increase the level of partnership and competence, confirmed by the certifications obtained by our specialists.

The services of the O2 Security Expert Centre are provided by competent security staff. The key security roles include L1 Security Operator (a team of L1 operators working 24/7 in charge of security supervision, evaluation of alerts and events from monitoring systems), L2 Security Analyst (L2 Analysts operating in 8/5 mode with standby outside standard business hours whose tasks include more profound analysis based on L1 level findings, reporting and communication with customers) and L3 Security Architect (a team of L3 architects working in 8/5 mode with the possibility of standby outside standard business hours, and responsibilities including communication with suppliers, onboarding, and technical support to other teams).

Competent system administrator is responsible for setting up and deleting access accounts to the Services. Administrator activities are carried out in accordance with internal regulations. Periodical checking of access takes place once a year to make sure that all accesses are properly controlled and comply with the defined security requirements. This ensures that data and systems are protected from unauthorized access and misuse. System administrators play a key role in managing access accounts and maintaining security standards.

Procedures

O2 Czech Republic is committed to maintaining top-level safety for its systems and infrastructure. This includes to ensure relevant confidentiality, integrity, and availability of data and systems through its internal policies and procedures.

O2 Czech Republic has implemented - as part of the integrated management system - a unified management system for policies and regulations. The policies and procedures relate to service processes, including the management and designing of product and service lifecycles, customer process management (customer onboarding and offboarding), change management processes, operational monitoring, incident management, and more. The goal of the policies and procedures is to ensure the security and protection of data and systems. O2 Czech Republic regularly reviews and updates the policies and procedures to ensure their compliance with the latest security standards and technologies.

Creating and maintaining strong safety awareness among employees is another important part of O2's focus. O2 Czech Republic provides training and educates its employees to be able to recognize and respond to potential security threats.

With its approach, O2 Czech Republic demonstrates its commitment to maintain a safe environment for its customers and protect sensitive information. Safety and security represent no.1 priority for O2 Czech Republic, forming an integral part of our business.

O2 Czech Republic is aware of the continuing evolution of security threats and vulnerabilities. Having this in mind, we regularly monitor and review our systems and infrastructure to identify any potential security risks and to adopt efficient measures to minimize the occurrence.

In addition, O2 Czech Republic cooperates with information security experts and monitors the latest trends and technologies to be able to respond to the new threats and implement best practices and measures to ensure adequate security.

The protection of customer privacy is another important aspect of security. O2 Czech Republic complies with all relevant laws and regulations pertaining to the protection of personal data and is committed to the correct and secure processing of such data. O2 customers can be sure that their data is protected and processed with the utmost care and security.

O2 Czech Republic pays enormous attention to security as such as well as the protection of personal data and systems. The commitment to safety can be demonstrated in several key areas such as:

- Security infrastructure: O2 Czech Republic invests in modern security technologies and infrastructure is able to detect and respond to potential threats. For example, the company uses advanced firewall systems and systems for detecting and preventing attacks.
- Monitoring and detection: O2 Czech Republic regularly monitors its systems and networks to identify suspicious activities or anomalies. If a potential security incident is detected, the company responds immediately and takes steps to minimize the damage.
- Employee training: O2 Czech Republic recognizes that security measures can only be effective if employees are adequately informed and trained. Having this in mind, O2 delivers regular training to employees to inform them of the latest security threats and best practices for protecting data and hardware.
- Protection against DDoS attacks: O2 Czech Republic also provides protection against DDoS (Distributed Denial of Service) attacks and AntiSpam measures. DDoS attacks are attacking that target network or web server congestion to deny user access. O2 Czech Republic uses advanced technologies and infrastructure to detect and avert DDoS attacks to keep its services available to users.

- Security policies and procedures: O2 Czech Republic has strict security policies and procedures in place to serve as a framework for protecting data and systems. The policies include rules for accessing sensitive information, password security, data encryption, and other security precautions.
- Regular updates and backups: O2 Czech Republic regularly updates its hardware and software to ensure the latest security patches and protection against known vulnerabilities. In addition, O2 performs regular data backups to minimize the risk of losing data in the event of a disaster or attack.

O2 Czech Republic is actively engaged in collaboration with security organizations and offices to share information about new threats and cooperate in solving them. This is our contribution to the overall improvement of digital security.

O2 Czech Republic makes considerable efforts to ensure that our customers are secured and their personal data thoroughly protected. Our investing in modern technologies, periodical monitoring and employee training demonstrate our commitment to security and data protection.

All internal policies and regulations (a list of which is summarized at the end of this section) are periodically reviewed and audited.

Data

Data protection represents a key element for O2 Czech Republic to the provision of its services. O2 is committed to compliance with all relevant legal regulations, including GDPR (General Data Protection Regulation) and ZoEK (Electronic Communications Act). This chapter deals with the types of data used to provide services and the measures adopted by O2 Czech Republic to ensure the confidentiality, integrity and availability of the data. The types of data used for our services are as follows:

- Content of communication: O2 Czech Republic conveys communication between customers and other entities. The content of the communication is conveyed without O2 having access to the content. This means that all transmitted data is protected from unauthorized access.
- Customer contact information: O2 Czech Republic stores customer contact information such as name, address, phone number, and email. This information is necessary for the communication with customers as well as for the provision of services.
- Contracts and communication with customers: O2 Czech Republic stores all contracts and communications with customers containing crucial information about the services including the terms and conditions. These documents are protected and stored in compliance with relevant legal requirements.
- Usage (traffic) data needed for the billing of services provided to customers and proving the legitimacy of billing: O2 Czech Republic collects traffic data necessary for the correct billing of customer services and for proving their legitimacy. This data is protected and processed in compliance with the internal policies and regulations.
- Other traffic data needed for analyzing errors and security of communication in the networks: O2 Czech Republic collects traffic data necessary for the correct billing of customer services and for proving their legitimacy. This data is protected and processed to minimize risks and provide network security.
- Data stored by the customer in the provided (cloud) services: O2 Czech Republic provides cloud services in which customers can store their data. This data is

protected and secured against unauthorized access and loss. As O2 Czech Republic does not have access to the content of the data the confidentiality and privacy of customers is preserved.

Data and personal data protection measures: O2 Czech Republic has established internal policies and regulations to ensure the confidentiality, integrity and availability of data and personal data. The policies and regulations are in line with legislative requirements such as GDPR and the Electronic Communications Act, as well as the standards making up the integrated management system, including ISO 27001.

The defined policies and regulations set out responsibilities, powers, and procedures for the area of data and information protection including data access control, use of appropriate data protection tools such as firewall, intrusion prevention system (IPS), intrusion detection system (IDS), and security information and event management (SIEM). These measures are used to identify and detect threats and vulnerabilities to ensure safety of data and communication.

Data protection and personal data protection requirements are also incorporated in agreements between O2 Czech Republic and its customers. The agreements set out for both parties their obligations in compliance with applicable legislation.

O2 Czech Republic is responsible for the protection of customer data incl. personal data and takes this obligation very seriously. As indicated above, O2 strives to continuously improve its procedures and technologies to deliver maximum protection for all data including personal data.

CONTROL ENVIRONMENT

The Company has set up an internal control system described in management documents, approved by the Company's Board of Directors. An important role in this system is played by a unit called O2 Internal Audit, functionally reporting to the Supervisory Board. Internal Audit provides the Company's bodies with an independent and professional assessment of the internal control and management system, the condition and development of the examined area against current best practice. In addition, Internal Audit fulfils internal audit functions for O2 daughter organisations. Depending on the findings of the audits, adequate corrective measures are taken by relevant managers. The O2 Internal Audit monitors how the findings are dealt with and reports the results to the Company's bodies. The principles of internal auditing, including principles of independence and objectivity, are described in the IA O2 Statute.

The basic principles applied in the Company's accounting procedures include control based on the "four eyes control" and the separation of the process of creating and administering business partner data from the process of payment and settlement of booked liabilities. At the same time, the list of people authorised to create, edit or approve accounting records in the SAP system is limited and periodically monitored. For individual accounting documents, one can always identify a concrete user who created or cancelled the document. The correctness of accounting and financial statements is continuously reviewed within the Finance Division. Selected areas of accounting and compliance of internal processes with the applicable legislation and internal guidelines and procedures are verified by internal audit. In the event of inconsistency, corrective measures are immediately proposed and promptly implemented. The efficiency of the internal control system, the process of developing individual and consolidated financial statements, and the process of external audit are monitored by the Supervisory Board.

The Finance division includes a department called “Revenue Assurance” whose goal is to reveal potential revenue losses due to data leakage. This end-to-end process covers all billing activities from the initiation of CDR to the issuing of customer invoice (bill).

The control environment also includes the application, compliance and checks of compliance with the requirements of ISO standards for management systems, implemented within the integrated management system. With regard to the scope of this report, the following standards are particularly relevant:

- ISO 20000-1 Information technology - Service management,
- ISO 27001 Information technology - Security techniques - Information security management systems supplemented by requirements of ISO 27017 Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services and ISO 27018 Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors,
- ISO 22301 Security and resilience - Business continuity management systems.

The compliance with the above standards is reviewed through internal audits and periodical certification and inspection audits conducted by a renowned certification body.

CODE OF CONDUCT AND ETHICS

The Company adheres to the recommendations of the Czech Corporate Governance Code 2018, the general rules of which are based on the applicable legislation of the Czech Republic. The recommendations are also inspired by comparable national codes of corporate governance (in particular, the German and Austrian codes) and international standards of corporate governance (in particular, the G20 / OECD Principles of Corporate Governance of 2015). Support for the performance of corporate governance and management, including the fulfilment of the requirements of the Czech Corporate Governance Code 2018, is the responsibility of Company Secretary, organizationally a member of the Legal and Regulatory Affairs Division.

The Compliance Code is part of the internal culture of O2 Czech Republic a.s. representing its approach to the compliance with legal regulations raising the ethical and responsible business standards. Measures derived from the aforementioned rules called the „compliance program” and the focus on abiding by the rules fall among the priorities of the O2 management. The prime goal of the measures is to set up an internal mechanism for O2 to prevent any illegal activities and, if any such activity occurs, to be identified and responded to accordingly.

O2 has a comprehensive and interconnected system of internal regulations and procedures in place, to ensure company compliance with laws and regulations. The starting point and central point are “Our Business Principles” (hereinafter referred to as the “Business Principles”) representing the source of values and principles to define our internal regulations. Numerous internal regulations explicitly refer to our business principles, boosts the awareness and the importance of the principles. All areas described in Our Business Principles form a traditional part of the country’s legal order. Furthermore, O2 describes in its internal regulations how its employees and members of bodies are supposed to act in specific situations in line with O2 internal processes.

This system is seen as measures within the meaning of §8 Art. 2 of Act no. 418/2011 Coll.

Our Business Principles are both an internal regulation approved by the Board of Directors and a document published on the O2 website (section "Responsible Approach"). The original version of the Business Principles is in Czech. The English version of the O2 website and Our Business Principles are available, too.

The Compliance Officer is responsible for the content and updating of the training. The objective of the training is to explain to all employees the content and meaning of Our Business Principles and the basic principles and rules arising from the key internal regulations to be followed by all employees to eliminate the risk of unlawful conduct. The elementary version of the training is mandatory for all O2 employees.

The Employment Rules govern the basic obligations of all O2 employees arising from their employment relationship. The Employment Rules are derived from Our Business Principles. The Policy of Accepting and Providing Gifts and Hospitality and the Conflict-of-Interest Policy constitute an integral part hereof.

The Signature Rules are another key internal regulation dealing with internal procedures of O2 employees when acting on behalf of O2 externally.

In order to achieve the objectives set out in the Compliance Code and to ensure prevention, O2 has implemented an internal whistleblowing system as an essential element to report a complaint about potentially unlawful conduct directly affecting O2. A whistleblower who meets the conditions for filing a report under the Whistleblower Protection Act is guaranteed adequate protection.

INFORMATION AND COMMUNICATION

Effective communication increases people's engagement and improves understanding of the needs and expectations of external and internal customers, contributing to the effective functioning of the company.

There are five rules of communication with customers at O2 (1. I say everything that is important, 2. I tell the truth, 3. I follow up on the customer's request, 4. I represent O2, 5. I am polite), and these communication rules should be used company-wide, including in internal communication.

In O2, the basic information channel for all employees is the intranet, as well as email communication or SMS. In addition to the electronic channels, information is also provided in person during meetings, meetings with the top management or off-site meetings.

The internal communications include, but are not limited to, communication of O2 policies and procedures, corporate events, new initiatives, and awareness on information and cyber security. Also, an annual process exists to set objectives among all executives and is rolled down to employees. These objectives are filtered down to team members through the annual and midyear review process.

External communication is carried out by relevant functions and roles within the company, e.g.:

- customer communication: sales consultants, call centre operators, account managers, service managers, service desk etc.,
- public and media communication: Corporate Communication unit,
- communication with suppliers: Purchasing, Logistics, Vendor Management, CTO Strategy Office,
- crisis management communication: Crisis Team.

A range of channels are used for external communication, from face-to-face meetings, phone calls to electronic tools such as email, chat, social networks and the company website, www.o2.cz.

MONITORING

Operational and safety monitoring

O2 maintains reasonable and appropriate technical and organisational measures, internal controls and information security procedures to protect its information assets as well as all customer data from accidental loss, destruction or alteration, unauthorised disclosure or access, or unlawful destruction.

O2 uses a number of automated monitoring systems for operational and security monitoring to ensure top-class performance and service availability. Monitoring is used at the level of user applications, user stations, servers and technological stations, security devices and network elements. Selected points of connection of the O2 network with public data networks and interfaces between selected security zones are monitored by IDS. Traffic between public or third-party networks and the O2 network is controlled by firewalls. The configuration of the firewalls is based on the principle of “everything which is not allowed is forbidden”.

Operational and security monitoring is followed by relevant incident management processes, including security incident management.

The requirements for operational monitoring of information system elements respect all legislative requirements (especially GDPR) and separate management documentation.

As a provider of cloud services, O2 provides customers with logging options depending on the type of service and offers the possibility of monitoring the operation (traffic) of these cloud services.

Internal audit

In the Our Business Principles document (see below), O2 defined the commitment to apply appropriate control mechanisms to assess and manage risks for O2, its employees and its image. Therefore, the Company has established an internal audit function to assure the Company's bodies and management of the efficiency of all internal governance and risk management processes, as well as to comply with the recommendations of good corporate governance practices. Internal audit is an independent and objective activity based on the philosophy of adding value by improving internal company operations. Internal audit helps O2 achieve its objectives by using a systematic methodological approach to evaluate and improve the efficiency of the risk management system, management and control processes, and corporate governance. Internal audit activities follow the rules of the International Professional Practices Framework (IPPF): a) Key principles b) Code of Ethics c) Standards d) Definition of internal audit. Furthermore, audit activities are carried out in accordance with the relevant legal regulations and internal management documents governing the performance of internal audit. Internal Audit provides independent and objective assurance as to whether the company ensures: compliance with the requirements of legal regulations and other mandatory requirements, reliability of information, efficiency of risk management processes and prudent management and protection of company assets.

O2 internal audit plays the role of the third line of defence in the IPPF's three-line model. In this model, the first line of defence includes operational management, the second line various functions of risk and compliance control incorporated by O2 management, while the third line includes independent assurance.

RISK ASSESSMENT PROCESS

Risk management is one of the basic managerial tools of the Company's effective management system, whose aim is to support the fulfilment of the Company's vision and strategy. The risk management system is developed as an integral tool of the Company's internal control. Risks are identified based on regular assessments by competent managers, suggestions from Risk Management and other Company units. Risks are evaluated from the perspective of potential financial impact and likelihood of occurrence. Members of the Board of Directors are kept up to date about all major risks to the Company and the way they are managed.

Operational risk management in information security and business continuity follows the RAMSES methodology, based on the previous CRAMM methodology. CRAMM is also the basis of the eponymous web application developed to enhance the efficiency of using RAMSES in extensive analyses and to present the results of risk assessments and security status. RAMSES is run on-premises on O2 servers. Pursuant to the cybersecurity legislative requirements, the assessment of operational risks takes into account relevant threats and vulnerabilities.

People responsible for the implementation of business plans and sustainable development of the company must consider the following three areas:

- potential damage to the business, caused by security failures;
- real likelihood of relevant vulnerabilities due to prevailing threats vs. security measures in place;
- importance of asset vulnerabilities to possible threats.

O2 carries out risk assessments for all company systems and situations arising from the context of the organisation.

HR MANAGEMENT

O2's business success and prosperity depends, but not only, on long-term relationships with customers, seeing O2 as a stable, strong and reliable partner keeping all customer data confidential. In order not to undermine the trust of our customers, to meet their expectations, not to compromise our image and risk of being excluded from public projects, we carefully select our employees for specific positions both in terms of qualification and integrity.

The selection of employees is based on clear criteria in terms of security suitability, trustworthiness, reliability and clean criminal record. The criteria are reviewed for each employee both before and during his or her employment, in accordance with the procedure laid down in our Security Regulations. The criteria for selecting employees are set by the Human Resources Division and all security aspects consulted with the Security unit.

Depending on the type of sensitive information, all employees supposed to get in touch with sensitive information during the performance of their jobs must sign all relevant non-disclosure statements.

O2 employees must attend an obligatory training course covering various topics incl. Our Business Principles, Information protection and GDPR. The training must be periodically repeated. Security training is obligatory for all O2 employees and all external (third-party) individuals and organisations working on the O2 premises.

Each employee is subject to a periodical Performance & Talent Review. The review includes meeting of individual targets, conduct and approach, which also includes adherence to corporate culture, communication and team cooperation as well as an active, logical and effective approach to solving problems. The outcome of the review also includes the identification of needs for further education and individual development.

PHYSICAL SECURITY

O2 Data Centres are designed to guarantee maximum security and privacy for customer devices and data. The data centres are owned by CETIN a.s., a sister organisation of O2, operating non-IT data centre technology and security services, including access control and security.

To protect the assets, the O2 Security unit installs technical and mechanical protection tools following relevant regulations, sets regime measures to create a uniform standard for access control and the scope of security of O2 facilities, and carries out all necessary periodical inspections.

Access control

Based on the security zoning of the Data Centre, the level of access control security is defined. The entry to the Data Centre is allowed to authorised/register personal using multiple authentications of contactless cards and PIN on the access control readers. Highly protected DC areas require the combination of the above with biometric systems. Every person moving in the DC premises is visibly marked. All visitors to the data centre must be accompanied by a DC employee.

O2 Security is responsible for checking compliance with the access rules as well as for the conducting of audits to verify compliance with the incident response procedures by the DC access control staff.

24x7x365 security monitoring

The perimeter, interior, areas containing supporting technology and the technological rooms are monitored by security and camera systems, supervised by authorised security staff.

All elements, functional and IT, of the data centre are monitored by IT monitoring centre staff.

Fire protection

All areas of the DC are secured with elements of the electric fire alarm system, the technology rooms include VESDA laser early detection systems and a system of automatic stable fire extinguishing system with inert gases.

Power supply and redundancy

Power supply to the data centre is protected by powerful uninterruptible power supply (UPS) units feeding dually customer's power distribution units (PDU). All data centres are protected against long-term power failure by diesel generators backing up the UPS system.

A backup of minimum N+1 ensures business continuity even in the event of a failure of one of the UPS.

Diesel generators contain fuel for at least 24 hours of operation without the need for refilling. If necessary, the supplier can deliver some more fuel. Cooling is provided by powerful, fully replaceable air conditioning units.

All our data centres are built and operated under the TIER III standard.

ACCESS CONTROL

Access control policy

Access control is implemented mainly for controlling user access to protected (classified) information, preventing UNAUTHORIZED access, ALTERING, disclosure or theft of information and media, all at the level of physical and logical access control.

During access control, our competent staff cooperate mainly with the Security unit, the Personal Data Protection unit and the administrators who OVERSEE the administration of information resources.

Access to networks and network services

Users are allowed to access networks and network services for which THEY are explicitly AUTHORIZED.

User administration and access control

Physical access control is governed by the Company Entrance Control directive. The logical access control of users follows the Corporate Access and Rights Management directive and the Administrator Security Manual.

Users are required to proceed in accordance with the approved access rules. Managers may only approve requests that are necessary for the performance of an employee's job. Access control for external workers is ruled by third-party access control to internal information systems and the "External workers register".

Users are prohibited from seeking authentication data needed for accessing information resources, using an account other than the one assigned, and connecting unapproved IT elements to the network. All users are obliged to report any suspicious behavior or security incident in accordance with the Definition and reporting of security incidents and events directive.

As a cloud service provider, O2 provides procedures and tools for the registration and de-registration of cloud service users. Moreover, O2 provides the customers with tools to manage user access rights and privileges.

As a cloud service provider, O2 provides the administrators with efficient tools to securely log in for the administration of the service, including monitoring and configuration of security elements.

ENDPOINT PROTECTION

The protection of company endpoints includes monitoring and protecting endpoints from cyber threats. The protected endpoints include desktops, laptops, smartphones, tablets, and other devices. There are various cybersecurity solutions you can install and monitor to protect the devices from cyber threats, irrespective of whether these are in or out of the corporate network.

O2 has installed Endpoint Security (ENS) using proactive reporting of threats, and able to deliver adequate protection throughout the entire lifecycle of an attack.

Endpoint Security Suite contains Endpoint Security and Endpoint Detection and Response.

CHANGE MANAGEMENT

The main goal of ICT Change Management is to make sure that standardized methods and procedures are used to deal with all changes effectively and quickly. It is also important that all service changes and configurations are recorded in the Configuration Management System. Another goal is to optimize overall business risk.

The goal of the ICT Change Management procedures is to respond to changing customer business requirements while minimizing incidents, failures, and duplications. It is equally important to respond to changing business and IT requirements so that services are aligned with the current business needs. In addition, it is necessary to ensure that all changes are recorded, evaluated, enabled, prioritized, planned, tested, implemented, documented and reviewed in a controlled fashion.

The procedure is binding in its entirety for all employees of O2 Czech Republic a.s., people working for O2 on a contractual basis (non-FTE, third-party) as well as for all other parties bound to comply with the Directive.

DISASTER RECOVERY

O2 defines the Business Continuity Management System (hereinafter referred to as the "BCMS" and the "Company"), creates the basic methodology and organizational prerequisites for the implementation of the Company's BCMS system. In connection with the Company's Business Continuity Management Policy (BCM Policy) and the company's governing documents (Organizational Rules, Security Rules), it defines the basic competencies of O2 management in the field of BCMS, sets out the principles of creation, the structure of BCMS and defines all elements and functions of the BCM system. The system enables O2 executives and the units under their management to focus on meeting the BCMS tasks and obligations arising from the relevant legal regulations and contracts. Implemented in the company's environment, BCMS uses the best-known practice and experience acquired in the field of BCMS.

The concept of O2 BCMS is multilayer, in terms of territory and sector:

Layer 1 - In order to deal with the impact of internal (plus some external) emergencies on the company's business solved by the relevant units within standard processes without requiring major modification, the BCM system is designed as a system for managing emergency situations (operational accidents, failures, closures, incidents, problems, service outages, events, etc.) without activating corporate crisis teams. The planning, creation, method of activation (escalation of activities), activity, support and development fall within the competence of the relevant management.

Layer 2 - In order to deal with the impact of external emergencies (crisis situations) as well as internal emergencies (large-scale emergency situations) on the company's environment, exceeding the scope, capacity and competencies of individual company units requiring the application of non-standard (modified) processes and forms of management, the BCM system is designed as a crisis management system with the activation of the company's crisis team. The planning, creation, way of activation and development of BCM are the responsibility of the CNOC unit while the activation falls within the competence of the particular crisis team leader. The transition from the system of ad-hoc dealing with emergencies by a particular unit to the system of crisis management (at the regional or national level) is usually decided by the leader of the crisis team in cooperation with the unit's line management of the unit/s depending on the assessment and evolution of a particular emergency.

Processes and procedures (BCP, DRP) to address emergencies are periodically reviewed, tested and, if required, updated. All exercises and tests are recorded in RAMSES.

VULNERABILITY MANAGEMENT

In the area of vulnerability management, the company has established basic rules, procedures, powers and responsibilities to efficiently manage the vulnerability of information systems and technologies to minimize the risk of security incidents, potential losses and to reduce business risks.

Efficient vulnerability management program includes:

Responsibility for the continuous maintenance of the information system

Continuous monitoring of the condition of updates and implemented information system patches.

Compliance with software vendor recommendations

Continuous and ad-hoc countermeasures to minimize security risks and incidents.

The aim of vulnerability management is to ensure compliance with the recommendations of the manufacturer and the Security unit while timely eliminating all vulnerabilities.

As various vulnerabilities differ in how critical they are, each responsible person (administrator) must judge which software patch should be applied in order to minimize the business impact and to plan enough time for testing and implementation in line with the change management process.

It is the responsibility of the administrators to obtain all software patches from renowned, trusted support channels, such as the actual vendors or third-party vendors. Each software patch must be downloaded and applied to licensed software where there is a support agreement in place.

In the event that objective reasons prevent the above activity the person responsible (admin) must apply for an exemption from the rule/s under the applicable Security Exception Management directive.

In places where there is open-source software without a trustworthy support channel, the person responsible must address the situation by applying the aforementioned exemption.

IV. Attachment B
Description of a O2 Czech Republic a.s.
service organization's principal service
commitments and system requirements

IV. ATTACHMENT B

DESCRIPTION OF A O2 CZECH REPUBLIC A.S. SERVICE ORGANIZATION'S PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

SERVICE COMMITMENTS

Commitments are declarations made by management to customers regarding the performance of O2 CZ System. Commitments to customers are communicated via Service Level Agreements, and/or Data Processing Agreements. Data Processing Agreements define the security and privacy obligations which the processors must meet to satisfy the organization's obligations regarding the processing and security of customer data.

Examples of service commitments:

As an example of a service commitment, we can mention the high level of service availability. This means that customers can rely on being able to access their telecommunications services at any time with minimum failures.

SYSTEM REQUIREMENTS

System requirements play a key role in the O2 business. The system requirements have been defined to provide efficient services, to comply with all legal requirements and to meet the company's targets. The system requirements follow the Cyber Security Act (ZoKB) implemented through system policies, procedures, contracts and regulations.

Examples of system requirements:

O2 Czech Republic must ensure adequate system availability and ability to withstand overloading so that customers can enjoy the full potential of all services. This includes implementing redundant infrastructure and non-stop monitoring.

Communication of commitments and requirements:

Transparency is a key responsibility of the management of O2 Czech Republic. By publishing the key service commitments and system requirements O2 allows its users to get a full picture of the O2 goals to evaluate the efficiency of the implemented controls.

O2 CZ is subject to relevant regulations, as well as state privacy security laws and regulations in the jurisdictions in which O2 CZ operates.

Security, Availability, Confidentiality, Privacy and Processing Integrity commitments to customers are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided on the O2 CZ website. Security, Availability, Confidentiality, Privacy and Processing Integrity commitments are standardized and included, but are not limited to, the following:

- Security and confidentiality principles inherent to the fundamental design of the O2 CZ System are designed to appropriately restrict unauthorized internal and external access to data and customer data is appropriately segregated from other customers.

- Security and confidentiality principles inherent to the fundamental design of the O2 CZ System are designed to safeguard data from within and outside of the boundaries of environments which store a customer's content to meet the service commitments.
- Availability principles inherent to the fundamental design of the O2 CZ System are designed to replicate critical system components across multiple Availability Zones and authoritative backups are maintained and monitored to ensure successful replication to meet the service commitments.
- Privacy principles inherent to the fundamental design of the O2 CZ System are designed to protect the security and confidentiality of O2 CZ customer content to meet the service commitments.
- Processing integrity principles inherent to the fundamental design of the O2 CZ System are designed to protect the security and confidentiality of O2 CZ customer data in transit to meet the service commitments.

O2 Czech Republic establishes operational requirements that support the achievement of security, availability, confidentiality, privacy and processing integrity commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in O2 CZ system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of various O2 CZ services and offerings. O2 CZ' service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality, privacy and processing integrity.

PRIVACY

As O2 Cloud services are primarily designed as Infrastructure as a Service, O2 does not process data belonging to customers. O2 security services are mostly analytical, monitoring and reporting services.

If the customer informs O2 that the scope of O2 Cloud services also involves the processing of personal data, the terms and conditions will also obtain a clause specifying the relationship between the controller and the processor of personal data pursuant to GDPR.

O2 has set up processes to ensure compliance with all legislative requirements regarding protection of personal and other data. An internal regulation sets out the rules for the protection of personal data (GDPR), the protection of identification, traffic and location data and the confidentiality of communications (see the Electronic Communications Act) and the protection of trade secret.

Each contract resp. the terms and conditions include a clause on the protection of personal data. In addition, customers are informed about the protection of personal data on the O2 website (<https://www.o2.cz/soukromi>). The O2 website shows how O2 uses cookies and handles personal data of the customers both in the role of data controller (Personal Data Processing Policy) and data processor (List of Personal Data Processors). It also includes

information on how complaints are dealt with including contact details of the Data Protection Officer and the right of each customer to escalate a complaint to the Office for Personal Data Protection.

AVAILABILITY

There is a documented procedure for capacity management. Capacity plans are prepared with warning and action thresholds set for monitored resources (compute, storage, memory). Appropriate monitoring tools are used for actual usage and capacity measurement. The current usage of resources and forecast of capacity demand is regularly reported to management.

Environmental threats are part of the list of threats in the risk assessment process in RAMSES. External environmental threats were considered, and datacentre are located out of flood, earthquake areas.

CETIN as a subservice provider is responsible for implementation and operation of environmental protection. Detection measures are implemented, such as fire, smoke detectors, air quality detectors, and liquid leak detectors. Environment and operations monitoring, and alerts are part of each DC surveillance system with 24/7 onsite personnel presence. Maintenance and test plans are prepared for both data centres.

Data centres are designed and operated in compliance with TIER III requirements. Data back-up processes are implemented according to the specifications of individual services in the scope of this report (configuration backups, replication at the storage level, synchronous data replication, etc.).

O2 has implemented a business continuity management system according to iso 22301 which covers both data centres. Business continuity plans with disaster recovery procedures are prepared for the services in the scope of this report. BCP/DRP include testing requirements (scope, frequency).

CONFIDENTIALITY

O2 sets out the rules and principles of information protection, including the powers and responsibilities for the identification, classification, processing and protection of confidential information.

In addition, a single system for document management, including rules for archiving and shredding, has been implemented in accordance with Act no. 499/2004 Coll., on Archiving and Records Management.

The rules for the protection of classified information pursuant to Act no. 412/2005 Coll., on the Protection of Classified Information and Safety Eligibility, are set out in separate internal regulations.

Procedures for the disposal of information depending on qualification level and medium i.e. printed documents, electronic file on various media are in place.

PROCESSING INTEGRITY

As O2 Cloud services are primarily designed as Infrastructure as a Service, O2 does not process data belonging to customers. O2 security services are mostly analytical, monitoring and reporting services. In these cases, it is stipulated in a contract what data the customer must provide and for what purpose of processing. The contract also determines the format of the input and output data (including reporting), the method of data transmission, the rules for the protection and storage of data. Process integrity control also includes operational and safety monitoring of the services.