Report of the President of UKE on Compliance in the Polish Market with Regulation 2015/2120 on Open Internet

Warsaw, 28 June 2024

Office of Electronic Communications | UKE

Table of contents

1. Conclusions

The President of UKE has conducted an analysis of compliance in the Polish telecommunications market with the provisions of the Regulation (EU) 2015/2120 of the European Parliament and of the Council on open internet access[1] in the period from 1 May 2023 to 30 April 2024.

This eighth report gives an insight into commercial practices and traffic management measures used by internet access providers and into specialised services as provided. It also analyses how information required under Article 4(1)(d) (first part) of the Regulation is presented in contractual documents.

Further, as every year, the report provides data on the quality of the internet access service. The market situation analysis shows that:

1. All of the audited service providers amended their contractual documents in line with the requirements laid down by the Regulation, in particular by introducing the required information on the quality of services they provide. However, these amendments, especially with regard to the information on the speed of the services offered, were not implemented in a uniform manner and failed to ensure a fully transparent source of information. In some cases, this resulted in the need to initiate administrative proceedings due to the failure of the ISPs audited to rectify the irregularities identified in the audit recommendations within the set deadline.

2. The audit of compliance with Article 3(2) and (3) of the Regulation by the largest mobile operators providing internet access services confirmed that all operators audited sold access to selected services and content in a 'zero rating' model.

3. No negative impact of the provision of specialised services on the availability and overall quality of the internet access service was identified.

4. No traffic management practices breaching the rules of open internet access, as referred to in Article 3(3) of the Regulation, were identified.

5. With regard to data transmission speeds for downloading, this area has seen a particular increase in the last few years. The average speed rose from 50.6 Mbps in 2020 to over 130 Mbps in 2024, meaning an increase of almost 160%. Over the same period, the average upload speed increased by more than 100%, from 21.4 Mbps in 2020 to 49.1 Mbps in 2024.

2. List of legal acts and abbreviations

- **Certified mechanism** – a measurement system for performing certified measurements and generating a report on certified measurements of the quality of internet access services provided in fixed public telecommunications networks. The system comprises, among other things, a website and a measurement application (for example, desktop computers and laptops). The system has been established on the basis of Article 4(4) of the Regulation;

---

[1] Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and retail charges for regulated intra-EU communications and amending Directive 2002/22/EC and Regulation (EU) No 531/2012.

- **Telecommunications Law (Pt)** – Act of 16 July 2004 – Telecommunications Law (consolidated text in Dz.U. [*Journal of Laws*] 2024, item 34);

- **Regulation** – Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and retail charges for regulated intra-EU communications and amending Directive 2002/22/EC and Regulation (EU) No 531/2012;

- **Gambling Act** of 19 November 2009 (consolidated text in Dz.U. [*Journal of Laws*] 2023, item 227);

- **BEREC Guidelines** – BEREC Guidelines on the Implementation of the Open Internet Regulation – BoR (22) 81;

- **APN** (*Access Point Name*) – name or address of a gateway between an operator's mobile network and another computer network, enabling, among other things, routing packets between these networks;

- **BEREC** – Body of European Regulators in Electronic Communications;

- **BGP** (*Border Gateway Protocol*) – a protocol for routing traffic between autonomous systems (i.e. a network or group of networks under a common administration and with a common routing policy), using TCP;

- **CSSR** (*Call Setup Success Rate*) – indicator of the effectiveness of calls measured as the fraction of call attempts that result in a connection to the dialled number;

- **DCR** (*Dropped Call Rate*) – indicator of disconnected calls measured as the fraction of the telephone calls which, due to technical reasons, were cut off before the speaking parties had finished their conversation and before one of them had hung up;

- **DSCP** (*Differentiated Services Code Point*) – a 6-bit field in the IP header used by network devices to implement QoS policies on the network by assigning appropriate values to different categories of traffic;

- **DVB-C** (*Digital Video Broadcasting – Cable*) – standard for the broadcast transmission of digital television intended for use in cable operator networks;

- **FIFO** (*First-In-First-Out)* – a basic packet transfer service mechanism that treats all packets equally; a packet that has arrived at an interface is placed at the end of the queue and waits its turn to be sent;

- **FTTB (Fiber To The Building)** – an access network architecture in which optical fiber is brought into a building or a room in a building (e.g. a basement) but the final section to the subscriber's premises is a physical medium other than optical fiber;

- **FTTH (Fiber To The Home)** – an access network architecture in which optical fiber is brought to the customer's premises;

- **IAS** – internet access service;

- **IPTV** (*Internet Protocol Television*) – delivery of television signal over Internet Protocol (IP) broadband networks;

- **ISP** – internet service provider;

- **MMS (Multimedia Messaging Service)** – a mobile messaging format that, apart from text, contains multimedia content such as graphics, animations, video clips or sounds, and uses packet data transmission;

- **M2M (Machine to Machine)** – a service for direct communication between devices in wired and wireless networks;

- **MPLS (Multi-Protocol Label Switching)** – a layer 2.5 technique of the ISO-OSI model, applied by routers, with packet routing replaced by the so-called label switching, used to mark different types of traffic in the network and enabling the implementation of QoS mechanisms in IP networks;

- **multicast** – a method of signal distribution in telecommunications networks, with a signal sent from a single source to selected recipients who request it;

- **NAT** (*Network Address Translation*) – technique for transmitting network traffic through a router that involves remapping of source or destination IP addresses;

- **NB-IoT** *(Narrowband Internet of Things)* – radio technology standard developed to enable the implementation in a low-power and low data rate wide-area network of, e.g., M2M services (Machine to Machine);

- **LTE** or **4G** (*Long-Term Evolution*) – standard developed by the 3GPP consortium for wireless data transmission, successor of 3G systems;

- **President of UKE** – President of the Office of Electronic Communications;

- **QoS** – Quality of Service;

- **Report** – Report of the President of UKE on compliance in the Polish telecommunications market with Regulation (EU) 2015/2120 of the European Parliament and of the Council laying down measures concerning open internet access;

- **SNMP** (*Simple Network Management Protocol*) – a network protocol used to manage devices such as routers, switches, computers, or telephone exchanges over an IP network;

- **TCP** – Transmission Control Protocol;

- **VOD** (*Video on Demand*) – service allowing users to access video or sound recordings at any time, without the constraints of a typical broadcasting schedule;

- **VoIP** *Voice over Internet Protocol*) – technology enabling voice processing over Internet Protocol (IP) networks;

- **VoLTE** (*Voice over Long Term Evolution)* – voice transmission over LTE technology;

- **VoWiFi** (*Voice over WiFi*) – technology enabling audio calls to be made over wireless local area networks;

- **VPBX** (*Virtual Private Branch Exchange*) – a virtual PBX, providing voice calls over IP networks, as a cloud-based solution;

- **VLAN** (*Virtual Local Area Network*) – a network technology of the data link layer (layer 2 of the ISO-OSI model), described in the IEEE 802.1Q standard, which allows within one physical local network to create multiple logical networks (virtual networks) by separating traffic between groups of ports on switches;

- **VPN** (*Virtual Private Network*) – an encrypted private connection service that allows remote access to the internet via VPN servers.

3. Monitoring of the Regulation

Article 5(1)(2) of the Regulation obliges the President of UKE, as the national regulatory authority for the telecommunications services market, to publish annual reports on the monitoring of the market situation with regard to open internet access and actions taken in this respect, as well as to submit these reports to the European Commission and BEREC. The present report covers the period from 1 May 2023 to 30 April 2024, and includes, in particular, information on actions taken by the President of UKE in the area of:

- monitoring and evaluation of traffic management mechanisms applied by ISPs;

- monitoring and evaluation of provision of specialised services by ISPs and impact of these services on the availability and overall quality of IAS;

- reports by end-users with regard to the rights and obligations as set out in Article 3 and Article 4(1) of the Regulation;

- monitoring and evaluation of contractual provisions in terms of the required information on the internet access services provided;

- data concerning the quality of IAS;

- IAS quality monitoring.

In the period covered by the Report, the President of UKE carried out activities to evaluate how the Regulation is implemented and complied with in Poland:

1. A questionnaire with detailed questions on the subject was prepared and addressed to the following twenty-five ISPs, chosen based on, among other things, the largest market share when it comes to the number of end-users: Orange Polska S.A., P4 sp. z o.o., Polkomtel sp. z o.o., T-Mobile Polska S.A., Vectra S.A., Netia S.A., Cyfrowy Polsat S.A., Multimedia sp. z o.o., Premium Mobile sp. z o.o., Inea sp. z o.o.,Toya sp. z o.o., Leon Telekom sp. z o.o. spółka komandytowa, Jerzego Krempa conducting business under the name Przedsiębiorstwo Produkcyjno-Montażowe Urządzeń Elektronicznych TELPOL Jerzy Krempa, Koba sp. z o.o., Oxylion S.A., Zicom Next sp. z o.o., Starlink Internet Services Ireland Limited, Tel-Kab sp. z o.o., Skyware sp. z o.o., Beskid Media sp. z o.o., Asta-Net S.A., Przedsiębiorstwo Promax Spółka Jawna Zofia Fórmanek-Okrój, Wiesław Okrój, Otvarta sp. z o.o., Klucz Telekomunikacja sp. z o.o., and Lycamobile sp. z o.o.

The questionnaire included questions on:

A. traffic management measures applied by the ISP – obligation of non-discriminatory treatment of data transmission (Article 3(3) of the Regulation);

B. use of specialised services, i.e. compliance with the obligation to ensure sufficient network capacity to provide high-quality internet access services on a non-discriminatory basis, the availability and overall quality of which must not be degraded by the provision of services other than internet access services at a specified quality level (Article 3(5) of the Regulation);

C. obligation to put in place transparent, simple and efficient procedures to address complaints of end-users relating to the rights and obligations laid down in Article 3 and Article 4(1) of the Regulation;

D. establishment of new procedures or amendment/adaptation of existing procedures for handling end-users' complaints relating to the rights and obligations laid down in Article 3 and Article 4(1) of the Regulation, that is whether there are new helplines, model complaints, additional communication channels for complaints, etc.

2. Follow-up activities were performed for the audit recommendations concerning contractual documents and issued for nine ISPs with regard to the information as required under Article 4(1)(d); and as a result, four administrative proceedings were initiated due to the failure of the ISPs audited to rectify the irregularities identified in the audit recommendations within the set deadline.

3. In 2023, the President of UKE audited the implementation of audit recommendations that had been issued in 2021 for ten ISPs. The audit results showed that the undertakings had mostly implemented the audit recommendations. Administrative proceedings were initiated in the case of one ISP as it had provided an incorrect definition of the normally available speed in the fixed network.

4. Following the audit of one of the largest (in terms of users) ISPs in Poland conducted to verify the compliance with Article 3(3) and Article 5(2) of the Regulation in the period from 2017 to 2019, i.e. to verify the application of traffic management mechanisms in the internet access network, under the Decision of 3 April 2024, the President of UKE waived the imposition of a penalty and instructed to act in accordance with the law, namely to comply with the obligation laid down in Article 3(3) of the Regulation by treating data transmission equally.

5. Comparative monitoring of the quality of internet access services provided was evaluated.

3.1. Information prepared on the basis of end-users' reports to UKE and questionnaires received from ISPs

3.1.1. Traffic management measures

In order to fulfil the obligation set forth in Article 5(1) of the Regulation, the traffic management measures used by ISPs were studied.

The analysis of the replies to the UKE questionnaire showed that there were no identified traffic management practices that were breaching the rules of open internet access, as referred to in Article 3(3) of the Regulation.

The traffic management measures applied by ISPs are allowed by way of derogations set out in Article 3(3)(a)–(c) of the Regulation. These include:

▪ blocking traffic due to obligations under Article 15f(5) of the Gambling Act of 19 November 2009[2] (point a);

---

[2] Article 15f(5) of the Gambling Act – a telecommunications undertaking providing internet access services is obliged to: 1) prevent, free of charge, access to websites using internet domain names entered in the Registry by removing them from

- blocking traffic at the request of authorised entities on the grounds of a threat to defence, national security, as well as public safety and order, Article 180(1) of the Telecommunications Law[3] (point a);

- performing obligations provided for in Article 2f(1) of the Council Regulation (EU) No 833/2014 of 31 July 2014[4] concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine (point a);

- managing traffic in accordance with applicable legislative acts (Article 175(1) of the Telecommunications Law[5] and Article 175c of the Telecommunications Act[6]) in order to preserve the integrity and security of networks and services provided over these networks, as well as of end-users' terminal equipment (points a and b);

- managing traffic in order to prevent network congestion (points c and b);

- blocking access to websites using internet domain names published on the warning list maintained by the Research and Academic Computer Network, National Research Institute (Naukowa Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy, NASK – PIB), which are used to defraud end-users of their data and funds. Blocking consists in removing them from ICT systems used to convert internet domain names into IP addresses and is implemented on the basis of Article 20[7] of the Act on Combating Abuse of Electronic Communications of 28 July 2023 (point a).

---

telecommunications undertakings' information and communication systems for converting internet domain names into IP addresses, no later than 48 hours after the entry in the Registry; 2) to redirect, free of charge, calls referring to internet domain names entered in the Registry to the website maintained by the minister responsible for public finance, containing a message, directed to recipients of internet access services, including, in particular, information about the location of the Registry, entry of the sought internet domain name in this Registry, a list of entities legally offering gambling on the territory of the Republic of Poland, as well as notification of the threatened criminal and fiscal liability of the participant of games arranged in violation of the provisions of the Act; 3) provide free access to websites using domain names deleted from the Registry, no later than within 48 hours of deletion of the internet domain name from the Registry.

[3] The telecommunications undertaking is obliged to immediately block telecommunications connections or information transmissions, at the request of authorised entities, if such connections may threaten defence, national security, as well as public safety and order, or to enable such blocking by these entities.

[4] It shall be prohibited for operators to broadcast or to enable, facilitate or otherwise contribute to broadcast, any content by the legal persons, entities or bodies listed in Annex XV, including through transmission or distribution by any means such as cable, satellite, IP-TV, internet service providers, internet video-sharing platforms or applications, whether new or pre-installed.

[5] The provider of publicly available electronic telecommunications services and, if necessary, also the operator of a public telecommunications network shall take technical and organisational measures to ensure security and integrity of the network, services and transmission of messages in relation to the services they provide. The measures taken should ensure a level of security corresponding to a given level of risk, taking into consideration state-of-the-art technical advancements and costs of implementing such measures.

[6] A telecommunications undertaking, taking into account Article 160(2), shall take proportional and reasonable measures with the purpose of ensuring security and integrity of the network, services and transmission of messages pertaining to the provided services, including:
1) eliminating the message transmission that is a threat to the security of the network or services;
2) stopping or limiting the provision of the telecommunications service at the end of the network wherefrom messages that are a threat to the security of the network or services are transmitted.

[7] Article 20 [Reporting an internet domain to be included in the warning list]
1. In order to protect internet users from websites that defraud them of their data, including personal data, and lead them to the disadvantageous disposal of their property, an agreement may be concluded between the President of UKE, the

In their responses to the UKE questionnaire, ISPs stated that the security mechanisms as implemented could potentially affect the availability of content, applications or services. Monitoring user reports is used to adjust security mechanisms in a way that minimises their undesirable effects. The analysis of complaints received by UKE shows that in individual cases, security mechanisms as implemented caused some restrictions in the use of the internet access service. In response to complaints, these restrictions were removed by the ISP, where possible. Moreover, applying the NAT mechanism also could affect the use of certain services, as well as the availability of ports open within an active session.

In cases where the quality of services deteriorated due to increased traffic levels, ISPs took steps to expand the network and increase its capacity. Such actions were mentioned by two ISPs.

In 2024, seven ISPs reported the practice of blocking TCP/UDP ports. For incoming traffic directed to the customer equipment, the following ports are blocked: TCP 21, TCP 22, TCP 23, TCP/UDP 53, TCP 80, TCP 110, UDP 123, TCP/UDP 137-139, TCP 443, TCP 445, TCP 465, TCP 587, TCP 8080. One ISP stated that it blocked all ports for incoming traffic. Ports are blocked for incoming traffic due to: vulnerability of services running on these ports, ensuring the security of end-users and their data, and limiting external access to devices.

Port 25 (TCP) is blocked for outgoing traffic to the internet. The blocking of port 25 was reported by six ISPs. One ISP stated that it was possible to unblock this port at the end-user's request. The blocking of port 25 is implemented if this port is used for sending unsolicited commercial information or information containing spywares, or for launching other attacks on computer systems. The reason for blocking, provided by ISPs, is the obligation to ensure integrity and security of networks and services provided over those networks, as well as of end-user's terminal equipment.

The DPI technique is used by two ISPs. The purpose of using it is to classify traffic for the purposes of billing and providing services covered by the ISP's offer. The data contained in the IP packet header is also subject to analysis, but there is no analysis of the content sent by end-users.

3.1.2. Specialised services

Monitoring by the President of UKE of compliance of the practices applied and services provided with the provisions of Articles 3 and 4 of the Regulation covers the evaluation of the conditions for the provision of services other than internet access services which are optimised for specific content, applications or services, or a combination thereof, where the optimisation is necessary in order to meet requirements of the content, applications or services for a specific level of quality, namely services referred to in BEREC Guidelines as 'specialised services.'

UKE's study, covering the last reporting period, was based on an analysis of ISPs' responses to the questions in UKE's questionnaire and an analysis of subscriber complaints received by UKE in relation to, among other things, the provision of specialised services.

---

minister responsible for informatisation, the Research and Academic Computer Network, National Research Institute and the telecommunications undertaking(s) to maintain a warning list and prevent access to such websites.

2. If the agreement referred to in paragraph 1 is concluded, the entity responsible for maintaining the warning list shall be CSIRT (Computer Security Incident Response Team) at NASK (Research and Academic Computer Network).

3. Internet domains whose primary objective is to mislead internet users and defraud them of their data or cause the disadvantageous disposal of their property shall be included in the warning list.

The study on the provision of specialised services aimed at determining whether:

(1) the specialised services indicated by ISPs meet the requirements regarding the freedom to offer such services in accordance with the first subparagraph of Article 3(5) of the Regulation, in particular whether:

- they are services other than IAS;

- they are optimised for specific content, applications or services, or a combination thereof;

- optimisation is objectively necessary in order to meet requirements for a specific level of quality;

(2) the conditions for establishing and providing specialised services by an ISP are compatible with the second subparagraph of Article 3(5) of the Regulation, that is:

- the network capacity is sufficient to provide a specialised service in addition to any internet access services provided;

- specialised services are not usable or offered as a replacement for internet access services;

- specialised services are not to the detriment of the availability or general quality of internet access services for end-users;

(3) specialised services are not used by the ISPs to circumvent the traffic management measure rules applicable to the internet access service.

The ISP's responses to the UKE questionnaire show that:

(1) 12 ISPs provide specialised services in their network, including: IPTV (9 ISPs), VoIP (8 ISPs), data transmission (7 ISPs), VPN (3 ISPs), VoLTE (2 ISPs), VPBX (2 ISPs), telemetry (2 ISPs), private APN (2 ISPs), VOD (2 ISPs), APN Xcap, MMS, NB-IoT, and VoWiFi;

(2) 6 ISPs stated that, in addition to providing specialised services in their network, they also acted as brokers to offer a specialised IPTV service for and on behalf of another entity;

(3) 13 ISPs stated that they neither provided nor brokered specialised services for and on behalf of others.

The most frequently indicated specialised services by the ISPs last reporting year were linear IPTV, VoIP telephony, VPN, and data transmission services. It was indicated that the APN Xcap service consisted in redirecting connections and hiding numbers. The private APN service was highlighted by two ISPs that provide services on the mobile network as a solution to accompany the delivery of services such as: M2M, telemetry, video monitoring, server backup, or corporate network access.

IPTV and VoLTE are considered to be specialised services in BEREC Guidelines (par. 113) provided that they meet the requirements of the Regulation, in particular of the first subparagraph of Article 3(5). In the case of the IPTV service, the ISPs stressed in their responses that the way the internet was used could degrade this service, and that the internet was not sufficient to fulfil the technical requirements for this service (e.g. multicast transmission).

The ISPs which identified VoIP as a specialised service argued that it could not be provided under IAS for reasons including the need to ensure: appropriate QoS parameters (low latency, latency

fluctuations, packet loss), arrival of packets in the order in which they were sent, security of the connection and a separate logical addressing to connect VoIP devices (telephones, gateways) to the exchange.

In order to ensure that optimisation is appropriate for specialised services, the ISPs use solutions such as:

- traffic separation at the network data link layer (e.g. by allocating separate VLANs);
- traffic separation at the physical layer of the network (e.g. via dedicated ports on the customer's terminal equipment);
- use of equipment dedicated to a specific specialised service (e.g. STB decoders);
- allocation of separate IP or Ethernet network;
- bandwidth reservations for specialised services;
- allocation of a specific frequency resource from the available band to a particular specialised service;
- application of the MPLS technology in the network;
- configuration of DSCP to differentiate and prioritise network traffic;
- configuration of private APNs for separated data transmission;
- implementation of encryption mechanisms for network connections.

The analysis of the responses to the UKE questionnaire shows that eight ISPs do not use a specialised service to provide IAS, or there is a possibility to provide IAS as a separate service from the specialised service. 3 ISPs indicated that in some cases or optionally, a specialised service might include IAS, which is provided under general conditions. 1 ISP noted that the IPTV service provided on decoders uses the internet to support embedded applications. This access is limited by decoder functions.

Most ISPs assess the impact of specialised services on IAS. 2 ISPs highlighted that as a rule they do not make such an assessment due to the marginal level of traffic generated by specialised services. Measures taken by ISPs to assess the impact on IAS exerted by providing specialised services in their network include:

- monitoring packet/frame loss on network interfaces;
- monitoring service quality indicators within a mobile network, i.e. CSSR call success rate and DCR call failure rate;
- controlling the capacity of connections and analysing access quality;
- analysing network load in the backbone, access and transmission segments;
- carrying out a technical survey to determine technical possibilities for the provision of a specialised service;
- applying a network monitoring software, using the SNMP protocol, with port-level accuracy from selected network infrastructure devices;
- continuous monitoring of IAS quality.

The analysis of the ISPs' responses shows that in most cases specialised services occupy from 0.5% to 20% of the bandwidth available in the network, while this occupancy depends on the network segment and the number of customers using these services at a given time. In the case of the NB-IoT service, the ISP reported that a frequency resource with a bandwidth of 200 kHz is used, which was separated from the 800 MHz LTE channel in use, so this specialised service has a negligible impact on the frequency resource dedicated to IAS.

The majority of IAS providers take measures to ensure the quality of this service in situations where specialised services are simultaneously provided in their networks. The most common measures include:

- expansion of network capacity conducted on the basis of network traffic forecasts and current link utilisation;
- construction of a backbone network with excess capacity that will enable the demand for bandwidth to be met;
- modernisation of infrastructure aimed at increasing network capacity while exceeding certain bandwidth occupation levels by specialised services;
- base station network densification in the case of mobile networks;
- BGP protocol configuration change;
- purchase of additional bandwidth for traffic exchange nodes.

ISPs undertaking development activities stated that the decision to expand infrastructure was usually made when the load on the network reached 60-80% of its capacity. One ISP stated that it did not take measures in this regard as in the model of specialised service provision it had adopted, specialised services did not affect the quality of IAS.

In addition, the President of UKE examined four complaints submitted to UKE by subscribers, which concerned specialised services, among other things. The allegations raised in these complaints were related primarily to the poor quality of specialised services, with no reference to their impact on the availability and overall quality of IAS offered in ISPs' networks.

3.1.3. End-users' reports to UKE[8]

The President of UKE, as part of his tasks, provides assistance to end-users by taking action on the issues reported by them with regard to telecommunications services. The quality of internet accesses services was the most common subject of the reports related to the open-internet right, submitted to the President of UKE in the period from 1 May 2023 to 30 April 2024. Compared to the previous period, the total number of reports increased by about 5%.

End-users most frequently reported that their lines did not reach the minimum, normally available, maximum or advertised download and upload speeds as specified in their contracts with the ISP. They also pointed to dropped calls, coverage problems, and low data transfer under the data service.

The largest number of reports, that is 50%, concerned the quality of services provided in mobile networks, and just over 26% were related to the quality of services in fixed networks. Compared to the previous period, the number of problems reported in this area:

- decreased by 13% for mobile networks;
- increased by 3% for fixed networks.

The remaining 24% of reports concerned other net neutrality issues, that is:

- ISPs' contractual provisions or commercial practices, restricting access via the internet to services, applications, content, or the use of terminal equipment (e.g. imposing restrictions

---

[8] Interventions, requests for out-of-court settlement of consumer disputes (ADR proceedings), inquiries.

on the use of terminal equipment connecting to the network; practices restricting tethering, banning access to sites) – approx. 3%;

▪ traffic management measures and unequal treatment of data transmission: discrimination, restriction of or interference with data transmission (e.g. blocking access to specific websites, slowing down data transfer speeds, limiting the quality of internet content) – approx. 4%;

▪ specialised services – services other than internet access services (e.g. VoLTE and linear IPTV services) – approx. 3%;

▪ and other issues related to the provision of an internet access service in accordance with the principles of an open internet – approx. 14%.

3.1.4. End-users' reports to ISPs

As part of his activities, the President of UKE also analysed the subjects of reports submitted to ISPs by end-users. Information provided by ISPs shows that complaints related to the right to open internet from end-users to providers between 1 May 2023 and 30 April 2024 were mainly related to:

▪ the quality of services provided (e.g. excessively slow or degraded transfer, provision of service below contractual parameters);
▪ the lack of internet access service (e.g. inability to open pages, dropped connections);
▪ network failures and congestion (e.g. overloaded stations, coverage problems).

Complaints of end-users concerned both fixed internet access and mobile internet access services.

In response to the questionnaire of the President of UKE, some ISPs stated that due to the number of complaints or the adopted method of their qualification, they could not indicate the precise number of complaints relating to the obligations set out in Articles 3 and 4 of the Regulation.

The majority of ISPs reported that they neither established new, nor amended/adapted existing end-user complaint handling procedures with regard to the rights and obligations set out in Article 3 and Article 4(1) of the Regulation between 1 May 2023 and 30 April 2024.

One ISP stated that it had improved the functioning of the internal application as he had made changes to the contact form by adding additional diagnostic tools for end-users, and expended the FAQs to include an additional pool of end-users' questions.

3.2. Audit concerning Article 3(2) and (3) of the Regulation

At the end of 2021 and the beginning of 2022, the President of UKE conducted an audit of one of the largest ISPs in Poland in terms of users with regard to compliance with the provisions of Article 3(3) and Article 5(2) of the Regulation, and this audit covered the period from 2017 to 2019. The audit procedure carried out and showed that in the period from 1 January 2017 to 15 May 2019 there was a violation of the terms of the Regulation resulting from the application of mechanisms for prioritisation of business traffic over residential customer traffic. These mechanisms, during the period of their application, were active continuously regardless of the level of traffic on the network and applied to internet access traffic, which had no special requirements in terms of latency and its fluctuations necessary for the correct operation of the service.

An on-line audit of the current status of the ISP's network equipment configuration in February 2022 did not reveal the use of traffic prioritisation mechanisms on that date. This situation is in line with the earlier statement of the ISP declaring the withdrawal of these mechanisms.

The analyses carried out and showed that the scale and scope of the breaches had little impact on the overall traffic and had a negligible impact on the quality of internet access services for residential users, i.e. B2C traffic. On average, it is estimated that the use of prioritisation mechanisms had an impact of around 0.5% of total B2C traffic volume, with this impact rising to around 2.5% at IRH (Internet Rush Hour).

Prioritisation worsened the quality for B2C traffic causing, depending on the time of day determining the B2B/B2C traffic ratio (from 1:4 to 1:27), for heavy loads of over 90%:

- an increase in delay for UDP packets of approximately 10–35% respectively;

- an increase in transaction times for non-real-time applications (e.g. WWW, FTP) using TCP by approximately 5–10% respectively.

This was due to the occasional occurrence of congestion states, where prioritisation mechanisms resulted in differentiated quality of service for business and residential customers.

At nominal network load states below 70%, the operation of the prioritisation mechanisms marginally differentiated the perceived quality of service for the two customer categories.

For B2C users, the increase in delay did not exceed 3 to 20% respectively, depending on the ratio of B2B/B2C traffic. In addition, the traffic peaks of business and residential customers were timing out over the course of the day, further limiting the impact of prioritisation mechanisms. Also, given the proportion of business to residential customer traffic volume, a significant advantage for the latter, the impact of using prioritisation mechanisms for business traffic had little impact on quality for residential users.

The use of prioritisation mechanisms significantly improved the quality of B2B service performance compared to when such mechanisms were not used (FIFO). The observed load on these services was less than 25% of the network and 3–5% of the total capacity in the peak hour. Therefore, the delays of the B2B packets were several times lower than would have been the case if a FIFO mechanism had been used.

Due to the highly specialised traffic prioritisation mechanism, analyses of the identified situation were carried out by UKE experts and appointed independent experts specialising in internet traffic surveillance and routing mechanisms.

Under the Decision of 3 April 2024, the President of UKE waived the imposition of a penalty and instructed to act in accordance with the law, namely to comply with the obligation laid down in Article 3(3) of the Regulation by treating data transmission equally. Considering the data on the extent of the violation (the scale and scope of the violations had a minor impact on the overall traffic and slightly affected the quality of internet access services for residential users), as well as the findings based on the conclusions of the appointed experts, the President of UKE stated that also the consequences of the identified violation did not support the imposition of a penalty. In view of the foregoing, and taking into account that the violation had ceased and that both the extent and effects of the violation were marginal, it was reasonable to decide not to impose a fine.

In the second half of 2023, an audit was conducted to verify whether the largest mobile operators providing internet access services comply with Article 3 (2) and (3) of the Regulation. The audit

covered offerings of the largest Polish internet access providers: T-Mobile Polska S.A., Orange Polska S.A., Polkomtel sp. z o.o., P4 sp. z o.o., Canal+ Polska S.A., Polsat Cyfrowy S.A., and Premium Mobile sp. z o.o.

The audit by the President of UKE confirmed that all of the providers audited sold access to selected services and content in a 'zero rating' model. In this model, an ISP applies a zero price for data traffic associated with a specific application or class of applications, and data are not counted against any data limits applicable to the internet access service. If as part of an internet access service, the provider does not charge the user for data used, for example, for streaming music in a specific application, or all applications for that matter, it means that the provider applies the zero rating model for these applications.

Under these circumstances, the President of UKE decided to issue audit recommendations to the audited undertakings, instructing them to:

1. discontinue concluding contracts and using contractual models that include services billed under the 'zero rating' model. The identified irregularities should be rectified within 30 days of the audit recommendations delivery;

2. modify existing contracts that include services billed under the 'zero rating' model so that the Company no longer provides services billed under the 'zero rating' model. Within 24 months of the audit recommendations delivery date, the undertakings should modify both contracts concluded before the audit recommendations delivery date and contracts concluded between the audit recommendations delivery date and the lapse of 30 days from the audit recommendations delivery date.

The recommendations do not apply to the cases in which the obligation to ensure access to services provided under the zero "rating model" arises from existing legislation.

3.3. Presenting information required under Article 4(1)(d) (first part) of the Regulation in contractual documents

Pursuant to Article 4(1)(d) (first part) of the Regulation, ISPs are obliged to ensure that contractual documents covering an internet access service, include clear and comprehensible information on:

- in the case of fixed networks: minimum, normally available, maximum and advertised download and upload speed;

- in the case of mobile networks: estimated maximum and advertised download and upload speed.

In 2019, the President of UKE carried out audits of the ten largest (in terms of end-users) ISPs as regards their compliance with the above information obligations set out in Article 4(1)(d) (first part) of the Regulation. The audit activities carried out in 2019 showed that the contractual documents for nine out of ten ISPs did not meet all the transparency requirements of the controlled provision of the Regulation. As a result, the President of UKE issued audit recommendations to telecommunications undertakings on the need to amend specific provisions in contractual documents.

The audit recommendations of the UKE President mostly included the following instructions:

- to remove evaluative terms that, when undefined, prevent subscribers from clearly understanding the included provisions;

- to introduce clear information indicating the time of availability of the usually available speed of the offered service;

- to introduce clear information indicating the time of availability of the maximum available speed of the offered service;

- to provide information on data transmission speeds as single numerical values in bits per second in the same units, for example, kbps or Mbps;

- to include, in a single document (contractual template), information on all upload and download speeds, i.e. minimum, normally available, maximum and advertised speeds for fixed networks or estimated maximum and advertised download and upload speeds for mobile networks;

- to discontinue using small and illegible print in contractual documents;

- to eliminate, from contractual documents, numerous references between different contractual documents.

As per the audit recommendations, the irregularities should be rectified within:

- 90 days from the delivery date of the recommendations for contractual documents and contracts covering internet access service, concluded after 90 days from the delivery date of the recommendations;

- 24 months from the delivery date of the recommendations for contractual documents and contracts covering internet access service, concluded after 90 days from the delivery date of the recommendations.

In order to verify the implementation of the audit recommendations, the President of UKE inspected the following ISPs: Multimedia Polska S.A., Vectra S.A., Orange Polska S.A., Polkomtel sp. z o.o., T- Mobile Polska S.A., Netia S.A., UPC Polska sp. z o.o., Toya sp. z o.o., and Inea sp. z o.o. The results showed that not all ISPs had implemented the audit recommendations to the extent and within the deadline specified by the President of UKE. As such, the President of UKE initiated four administrative proceedings against: Toya sp. z o.o. , Inea sp. z o.o , P4 as the legal successor of UPC Polska sp. z o.o., and Orange Polska S.A., ordering these ISPs to rectify the irregularities confirmed in the audits. By 30 April 2024, one of these proceedings (against Toya sp. z o.o.) ended with a decision calling for the rectification of the violations, and the remaining proceedings are ongoing.

The Decision of the President of UKE issued for Toya sp. z o.o orders this ISP to rectify the irregularities consisting in the violation of Article 4(1)(d) (first part) of the Regulation, namely to discontinue using, in contractual documents, numerous references between different contractual documents as this practice fails to provide clear and comprehensible explanation of download and upload speeds.

Between May and July 2021, the President of UKE also audited the scope and presentation of the information provided in the contractual documents for the internet access service by 16 local internet access service providers.

The 2021 audit revealed that the most common irregularities were as follows:

- using small and illegible print in contractual documents;

- using, in contractual documents, numerous references between different contractual documents;

- incorrect definition of maximum speed;

- absence of the correct definition of normally available speed;

- stating, in contracts and annexes to contracts (including, in particular, terms and conditions and price lists), data transmission speed as a numerical value in different units;

- in the case of fixed networks: absence of clear and comprehensible information on speeds, as required by the Regulation, in the contractual documents for an internet access service.

With regard to irregularities as identified, audit recommendations were issued to 10 out of 16 ISPs audited, obliging them to comply with the audited provision of the Regulation and to amend their contractual documents accordingly.

In 2023, the President of UKE inspected the implementation of audit recommendations issued to Koba sp. z o.o., Marcin Frątczak conducting business under the name: RFC Marcin Frątczak, Chopin Telewizja Kablowa sp. z o.o., Przemysław Żelazny conducting business under the name: Netcity Przemysław Żelazny, 'SAT-FILM' sp. z o.o. i Wspólnicy spółka komandytowa, Krapkowickie Sieci Internetowe sp. z o.o., Oxylion S.A., Jerzy Krempa conducting business under the name: Przedsiębiorstwo Produkcyjno-Montażowe Urządzeń Elektronicznych Jerzy Krempa, Centrum Telewizji Kablowej JIM-SAT sp. z o.o. and Supermedia sp. z o.o.

The audit results showed that the undertakings had mostly implemented the audit recommendations. In the case of Marcin Frątczak conducting business under the name: RFC Marcin Frątczak, administrative proceedings were initiated with regard to the introduction of a correct definition of the normally available speed, which should be specified in relation to 24 hours or a shorter period determined by the service provider in the contract by stating the availability time of this speed (as a percentage).

4. Quality of internet access service

Internet access services offered to end-users should allow and guarantee the use of on-line content, applications, and modern services at an appropriately high level.

In this chapter of the Report, the President of UKE presents data on the quality of IAS, which were collected on the basis of measurements made with measurement applications publicly available in Poland, offered by the research entity, V-SPEED sp. z o.o. The data presented in the report depict the quality of internet access services on the basis of measurements carried out in April 2024, and in order to observe the trend of changes over the years, these data were related to data from a few previous years, i.e. measurements carried out in the last seven years (from 2016 to 2023).

To evaluate the market situation and assess the quality of services, data extracted from consumer tests were carried out using

- an application accessible via a web browser available at *www.speedtest.pl*. The results pertain to all technologies available in fixed and mobile networks;

  - in April 2017, approximately 1.8 million tests were performed;

- in April 2018, approximately 1.7 million tests were performed;

- in April 2019, approximately 2.0 million tests were performed;

- in April 2020, approximately 3.8 million tests were performed;

- in April 2021, approximately 3.0 million tests were performed;

- in April 2022, approximately 2.3 million tests were performed;

- in April 2023, approximately 2.4 million tests were performed;

- in April 2024, approximately 2.3 million tests were performed.

- Internet Speed Test application available for mobile devices.

  The results pertain to all technologies available in mobile networks;

  - in April 2017, approximately 111,000 tests were performed;

  - in April 2018, approximately 250,000 tests were performed;

  - in April 2019, approximately 530,000 tests were performed;

  - in April 2020, approximately 822,000 tests were performed;

  - in April 2021, approximately 833,000 tests were performed;

  - in April 2022, approximately 843,000 tests were performed;

  - in April 2023, approximately 895,000 tests were performed;

  - in April 2024, approximately 717,000 tests were performed.

The large amount of analysed user data allows an overall evaluation of the quality of services offered by Polish ISPs. The above measurements were carried out by the internet end-users themselves. The measurements obtained were influenced by the individual conditions under which users use the relevant services. These include the technology of the terminal equipment, the limitations of tariff plans, the use of Wi-Fi technology in home networks, the number of simultaneously active devices, or the conditions of radio wave propagation.

The analysis of data from the years 2020-2022 shows unusual user behaviour caused by the then ongoing epidemiological situation related to the SARS-CoV-2 virus. The unusual behaviour was that during the pandemic, many users worked remotely from home, using home-based service volumes, very often in mobile network technologies. The suddenly higher traffic was observed then as a result of the increased use of streaming platforms offering educational and entertainment content. Even though the epidemic state came to an end, the trend continued. It is also noticeable that there has been a steady increase in the quality parameters of the services provided by the ISPs, i.e. a significant increase in the average data transfer speed (both download and upload speeds) with a simultaneous decrease in the ping parameter (reduction in data transmission latency).

The table and graph below clearly indicate that an upward trend can be seen over the years analysed in the area of data speeds, both upload and download speeds. A particularly large increase in the area of download speed is noticeable in the last three years.

The average speed rose from 50.6 Mbps in 2020 to over 130 Mbps in 2024, meaning an increase of almost 160%. Over the same period, the average upload speed increased by more than 100%, from 21.4 Mbps in 2020 to 49.1 Mbps in 2024.
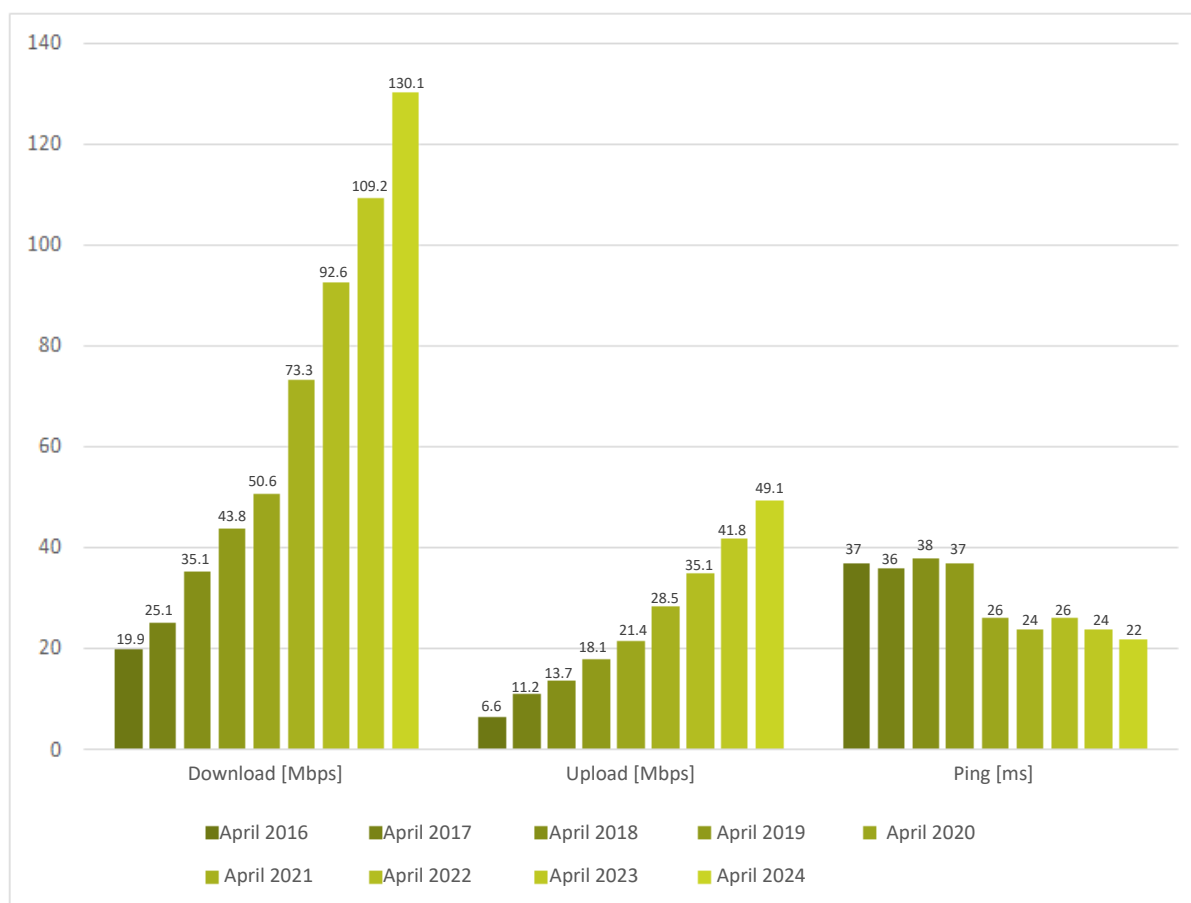
Table 1

Average download and upload speed and ping from the browser application

	04 2016	**04 2017**	**04 2018**	**04 2019**	**04 2020**	**04 2021**	**04 2022**	**04 2023**	**04 2024**
Download [Mbps]	19.9	25.1	35.1	43.8	50.6	73.3	92.6	109.2	130.1
Upload [Mbps]	6.6	11.2	13.7	18.1	21.4	28.5	35.1	41.8	49.1
Ping [ms]	37	36	38	37	26	24	26	24	22

Source: UKE

Figure 1

Average download and upload speed and ping from the browser application

Source: UKE

Since 2016, the first year analysed, there has been a steady downward trend in the PING ratio, a ratio showing transmission latency and the number of lost data packets, over the years analysed. The lower the PING ratio, the better – a high PING indicates a poor-quality internet connection and the loss of information packets that do not reach the end device. This ration dropped from 37 ms in 2016 to 22 ms in 2024.

Also in mobile networks, an upward trend in the average speeds of data streams in both directions can be observed in most IAS service providers in recent years. A clear improvement in the quality of service is also evident, reflected in a reduction in the latency of packet transmission. There was some slowdown of this trend in 2020 due to the epidemic state, which existed then, while from 2021 onwards, a clear increase in the offered bit rates can be seen again.
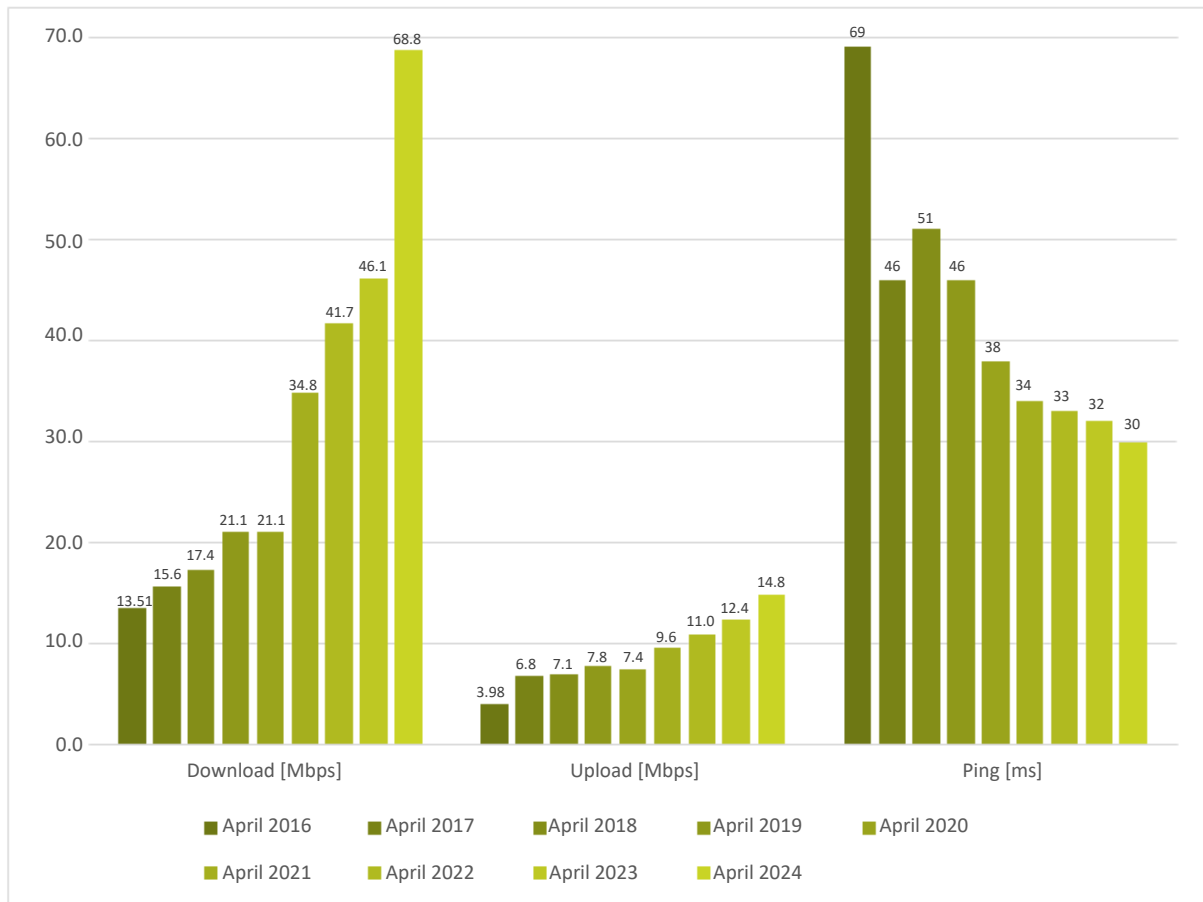
Table 2

Average download and upload speed and ping from the mobile application

	04 2016	04 2017	04 2018	04 2019	04 2020	04 2021	04 2022	04 2023	04 2024
Download [Mbps]	13.5	15.6	17.4	21.1	21.1	34.8	41.7	46.1	68.8
Upload [Mbps]	4.0	6.8	7.1	7.8	7.4	9.6	11.0	12.4	14.8
Ping [ms]	69	46	51	46	38	34	33	32	30

Source: UKE

Figure 2

Average download and upload speed and ping from the mobile application

Source: UKE

The results of the download test were also analysed, broken down into speed ranges:

‒ 0–3 Mbps;

‒ 3–10 Mbps;

‒ 10–30 Mbps;

‒ 30–100 Mbps;

‒ above 100 Mbps.

In the case of measurements performed with the use of a browser in the to-user direction (download), the results obtained prove that over the analysed years, there has been a clear increase in the share of the range speed above 100 Mbps – in 2024, this percentage was already over 30%, which is a significant increase, compared to the data from eight years ago (it was only 1.8% in 2026), The direction of these changes indicates a steady increase in the share of fibre-optic technology in fixed networks, and also points to the continued development of the potential of the services offered.

Table 3
Distribution of the number of download speed measurements in ranges (web app)

Download	04 2016	04 2017	04 2018	04 2019	04 2020	04 2021	04 2022	04 2023	04 2024
0–3 Mbps	20.5%	21.6%	17.4%	15.6%	17.8%	13.6%	11.8%	11.1%	9.0%
3–10 Mbps	30.2%	27.1%	22.8%	20.7%	20.4%	16.6%	14.7%	13.5%	11.9%
10–30 Mbps	30.2%	27.9%	29.1%	27.8%	25.5%	23.5%	22.1%	20.3%	19.0%
30–100 Mbps	17.2%	19.8%	24.1%	25.9%	24.5%	27.7%	28.4%	28.2%	28.7%
> 100 Mbps	1.8%	3.5%	6.5%	9.9%	11.8%	18.5%	23.0%	27.0%	31.4%

Source: UKE

Figure 3
Distribution of the number of download speed measurements in ranges (web app)
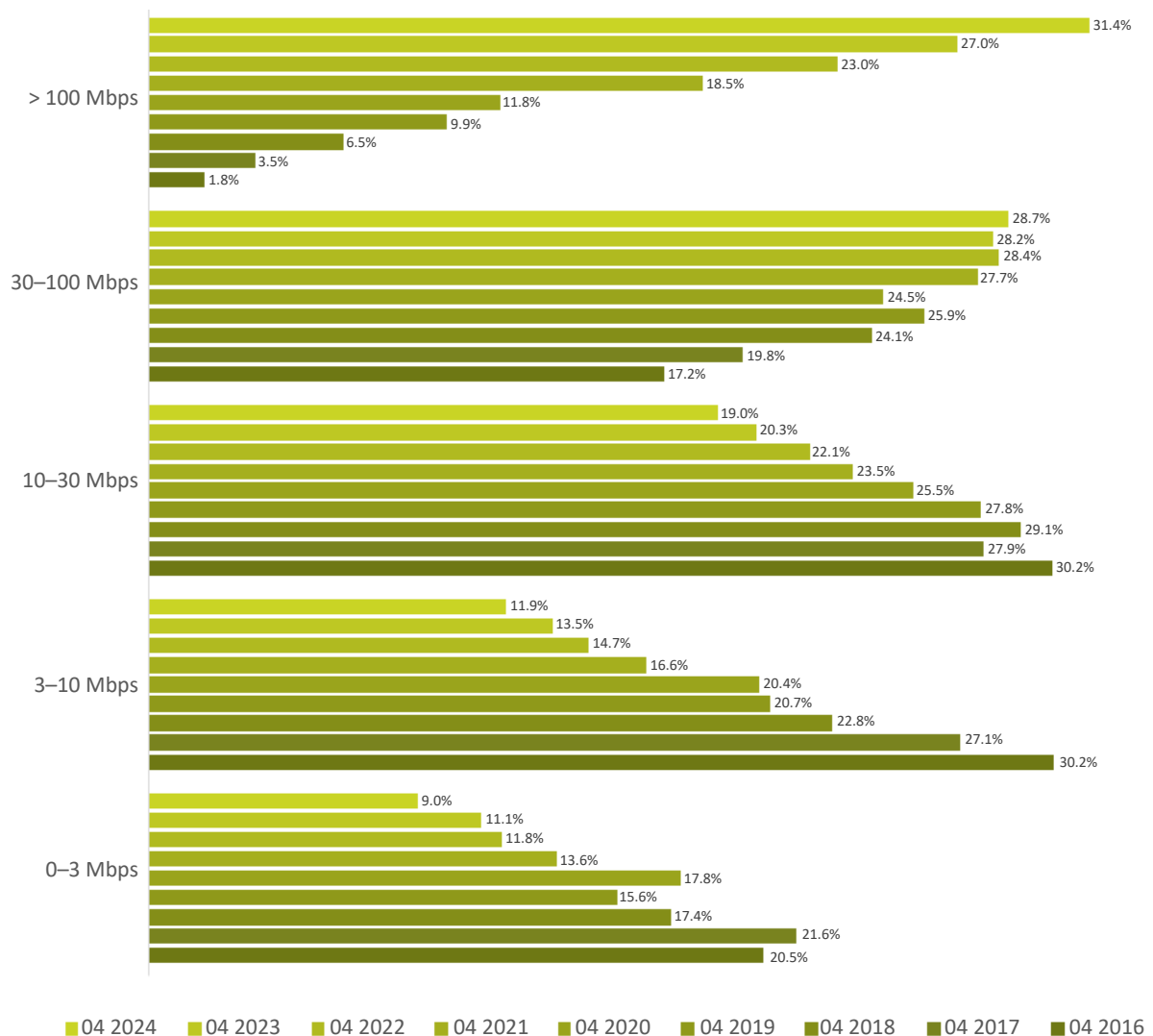
Source: UKE

Similar growth trends can be seen for measurements performed using an application in mobile networks. In the case of measurements performed with the use of a browser in the to-user direction (download), the results obtained prove that over the last years, with the use of mobile technologies, there also has been a clear increase in the share of the download speed, especially from the range above 100 Mbps. This direction of change is in line with the increase in the share of LTE technology in mobile networks.
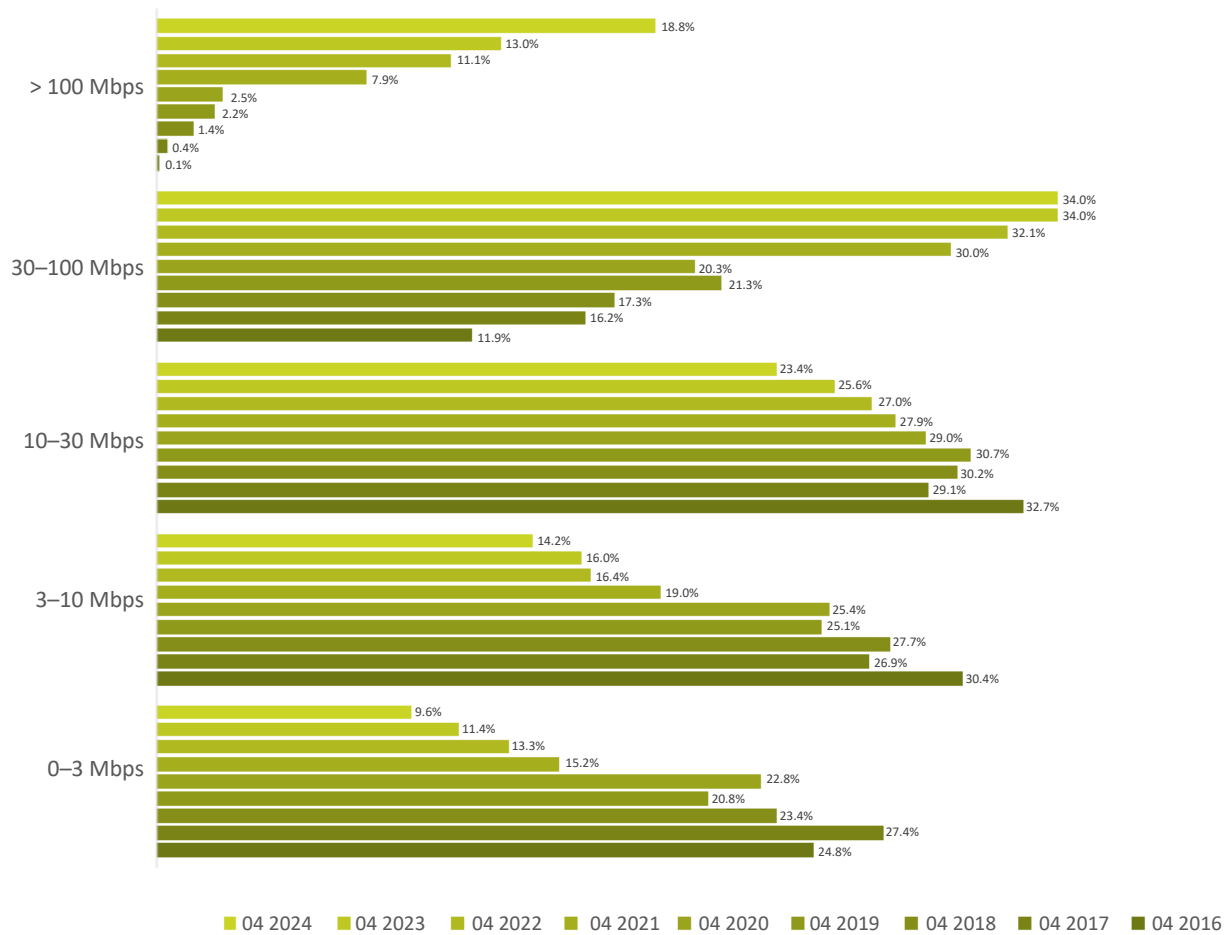
Table 4

Distribution of the number of download speed measurements in ranges (mobile app, all technologies)

Download	04 2016	04 2017	04 2018	04 2019	04 2020	04 2021	04 2022	04 2023	04 2024
0–3 Mbps	24.8%	27.4%	23.4%	20.8%	22.8%	15.2%	13.3%	11.4%	9.6%
3–10 Mbps	30.4%	26.9%	27.7%	25.1%	25.4%	19.0%	16.4%	16.0%	14.2%
10–30 Mbps	32.7%	29.1%	30.2%	30.7%	29.0%	27.9%	27.0%	25.6%	23.4%
30–100 Mbps	11.9%	16.2%	17.3%	21.3%	20.3%	30.0%	32.1%	34.0%	34.0%
> 100 Mbps	0.1%	0.4%	1.4%	2.2%	2.5%	7.9%	11.1%	13.0%	18.8%

Source: UKE

Figure 4

Distribution of the number of download speed measurements in ranges (mobile app, all technologies)

> 100 Mbps
- 18.8%
- 13.0%
- 11.1%
- 7.9%
- 2.5%
- 2.2%
- 1.4%
- 0.4%
- 0.1%

30–100 Mbps
- 34.0%
- 34.0%
- 32.1%
- 30.0%
- 20.3%
- 21.3%
- 17.3%
- 16.2%
- 11.9%

10–30 Mbps
- 23.4%
- 25.6%
- 27.0%
- 27.9%
- 29.0%
- 30.7%
- 30.2%
- 29.1%
- 32.7%

3–10 Mbps
- 14.2%
- 16.0%
- 16.4%
- 19.0%
- 25.4%
- 25.1%
- 27.7%
- 26.9%
- 30.4%

0–3 Mbps
- 9.6%
- 11.4%
- 13.3%
- 15.2%
- 22.8%
- 20.8%
- 23.4%
- 27.4%
- 24.8%

■ 04 2024 ■ 04 2023 ■ 04 2022 ■ 04 2021 ■ 04 2020 ■ 04 2019 ■ 04 2018 ■ 04 2017 ■ 04 2016

Source: UKE

Table 5

Average download speed [Mbps] and change in 2024 compared to 2023 [%] from browser application for all fixed providers, by voivodeships (regions of Poland)

No.	Voivodeship	Average result [Mbps]	Change compared to 2023
1	Mazowieckie	215.98	13.34%
2	Pomorskie	212.14	13.85%
3	Warmińsko-mazurskie	200.81	22.35%
4	Śląskie	199.87	17.08%
5	Wielkopolskie	198.78	15.15%
6	Zachodniopomorskie	195.73	17.52%
7	Łódzkie	187.81	13.18%
8	Małopolskie	186.66	11.37%
9	Dolnośląskie	185.60	12.16%
10	Podlaskie	178.64	29.88%
11	Lubuskie	173.26	12.85%
12	Świętokrzyskie	172.73	16.58%
13	Opolskie	165.70	18.42%
14	Kujawsko-pomorskie	165.44	12.14%
15	Lubelskie	159.06	15.29%
16	Podkarpackie	131.13	15.61%

Source: UKE

Average download speeds in fixed networks across the country exceed 130 Mbps. For several years now, the highest value has always been recorded in the Mazowieckie Voivodeship – the average result for this voivodeship in 2024 was almost 216 Mbps, an increase of more than 13% on the previous year (from 187 Mbps).

The above data are illustrated on a map of Poland divided into voivodeships.

Map 1

Average download speed [Mbps] and change in 2024 compared to 2023 [%] from browser application for all fixed providers

Source: UKE

The analysis of the data presented above, on the map of Poland and in the table, shows that all voivodeships have seen a definite increase in the average download speed. The largest increase in the average download speed was achieved in the Podlaskie Voivodeship (to 178.64 Mbps – an increase of almost 30% compared to 2023). In the same period, the smallest increase was recorded in the Małopolskie Voivodeship (to 186.66 Mbps – an increase of 11.4% compared to 2023).

A similar upward trend was observed in all the voivodeships with regard to the average upload speed – by approximately 16% on average compared to the previous year, as shown below, in the table and on a map of Poland divided into voivodeships.
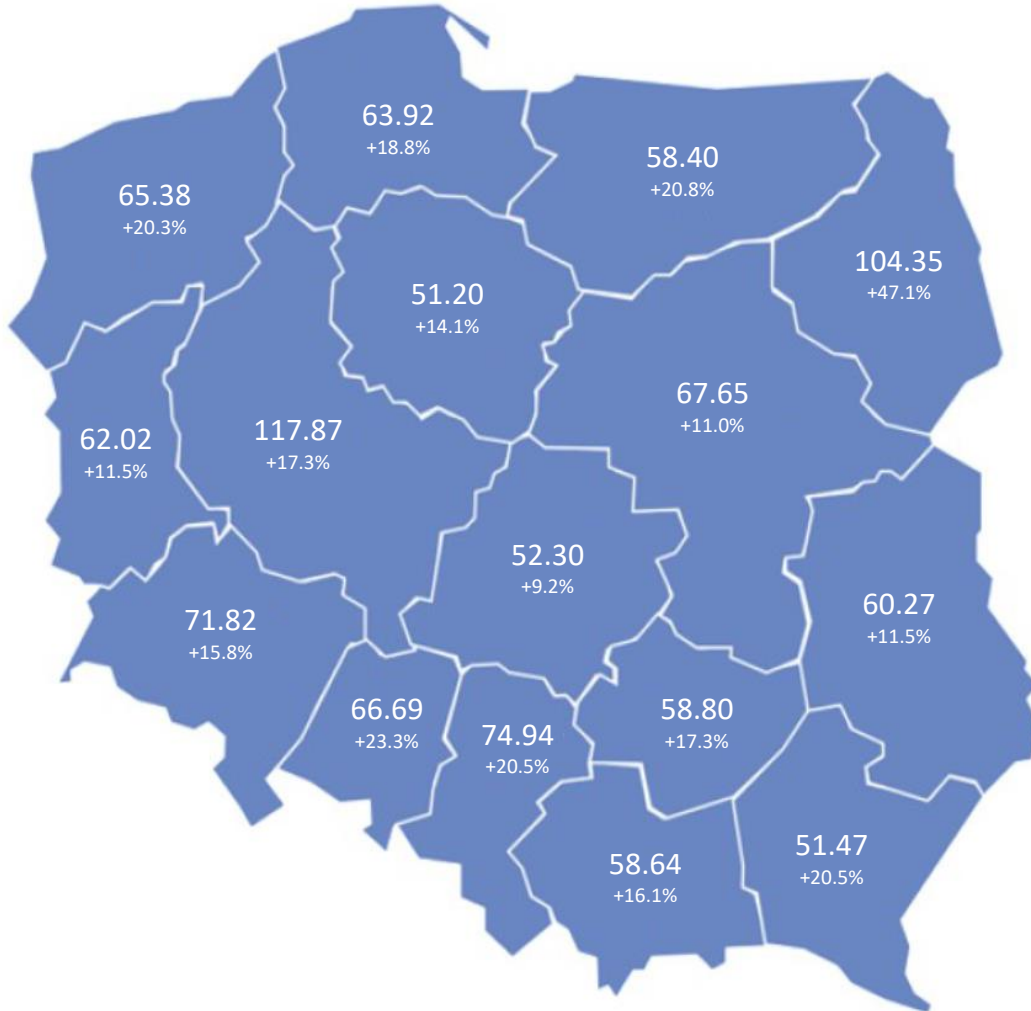
Table 6

Average upload speed [Mbps] and change in 2024 compared to 2023 [%] from browser application for all fixed providers

No.	Voivodeship	Average result [Mbps]	Change compared to 2023
1	Wielkopolskie	117.87	17.28%
2	Podlaskie	104.35	47.06%
3	Śląskie	74.94	20.48%
4	Dolnośląskie	71.82	15.76%
5	Mazowieckie	67.65	11.01%
6	Opolskie	66.69	23.26%
7	Zachodniopomorskie	65.38	20.28%
8	Pomorskie	63.92	18.80%
9	Lubuskie	62.02	11.45%
10	Lubelskie	60.27	11.53%
11	Małopolskie	58.64	16.08%
12	Warmińsko-mazurskie	58.40	20.80%
13	Świętokrzyskie	56.80	17.32%
14	Łódzkie	52.30	9.16%
15	Podkarpackie	51.47	20.54%
16	Kujawsko-pomorskie	51.200	14.14%

Source: UKE

Map 2

Average upload speed [Mbps] and change in 2024 compared to 2023 [%] from browser application for all fixed providers

Source: UKE

The vast majority of voivodeships also saw a decrease in the average latency of data streams. The largest decrease was recorded, in the case of mobile technology, in the Opolskie Voivodeship (down more than 11%), while in the case of web technology, in the Podlaskie Voivodeship – down 20% to 12 ms.

Table 7

Average download speed [Mbps] and change in 2024 compared to 2023 [%] from mobile application for all mobile providers

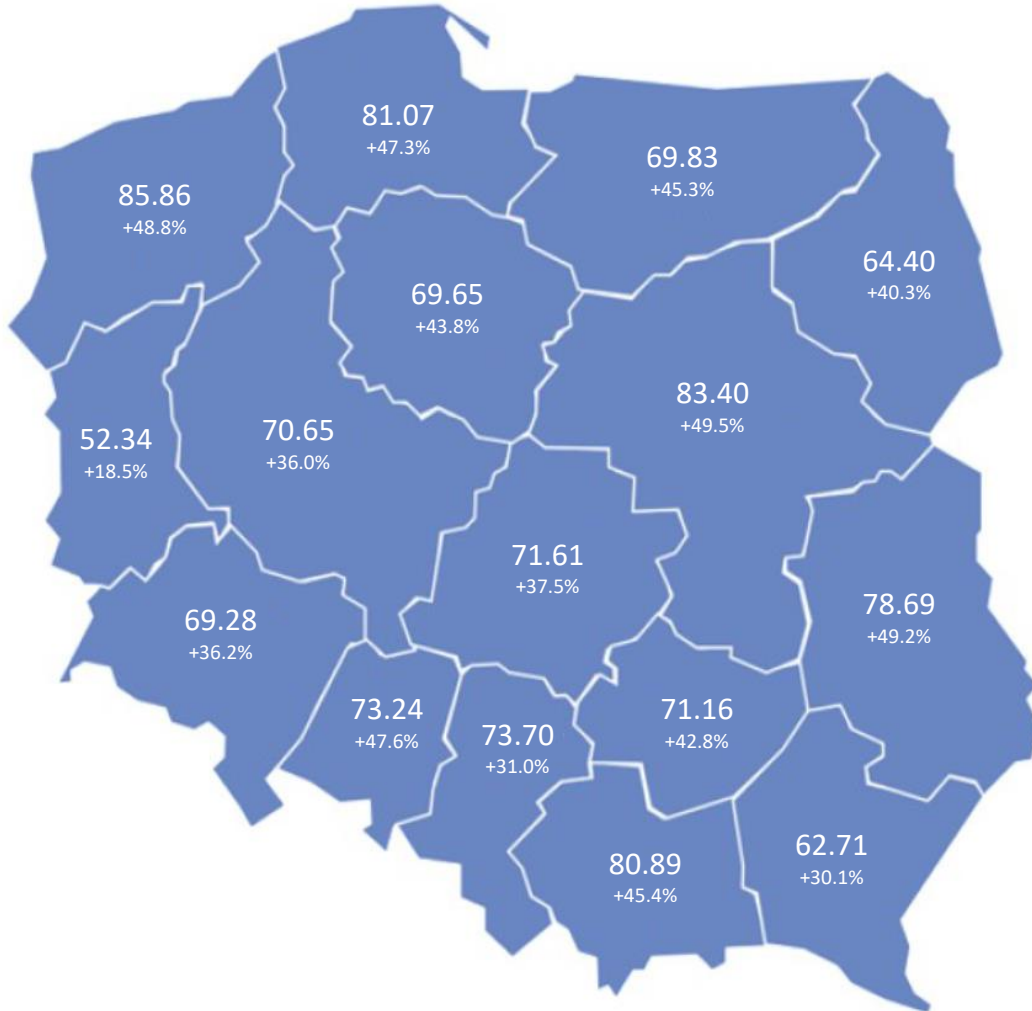| No.	Voivodeship	Average result [Mbps]	Change compared to 2023
1	Zachodniopomorskie	85.86	48.79%
2	Mazowieckie	83.40	49.46%
3	Pomorskie	81.07	47.32%
4	Małopolskie	80.89	45.41%
5	Lubelskie	78.69	49.17%
6	Śląskie	73.70	30.98%
7	Opolskie	73.24	47.62%
8	Łódzkie	71.61	37.52%
9	Świętokrzyskie	71.16	42.82%
10	Wielkopolskie	70.65	35.97%
11	Warmińsko-mazurskie	69.83	45.34%
12	Kujawsko-pomorskie	69.65	43.76%
13	Dolnośląskie	69.28	36.22%
14	Podlaskie	64.40	40.26%
15	Podkarpackie	62.71	30.06%
16	Lubuskie	52.34	18.46%

Source: UKE

Similar to the results of the average download speed from the browser application for all fixed providers, also mobile providers saw a definite increase in the average download speed in 2024 in almost all voivodeships compared to the same period last year.

The highest increase in average download speed was achieved in the Mazowieckie Voivodeship (49.5%), and the lowest in the Lubuskie Voivodeship (18.5%). The growth trend indicates that telecommunications undertakings are trying to respond to user demand associated with more intensive use of mobile network technologies.

Map 3

Average download speed [Mbps] and change in 2024 compared to 2023 [%] from mobile application for all mobile providers

Source: UKE

Table 8

Average upload speed [Mbps] and change in 2024 compared to 2023 [%] from mobile application for all mobile providers

No.	Voivodeship	Average result [Mbps]	Change compared to 2023
1	Śląskie	17.10	20.88%
2	Mazowieckie	16.77	24.15%
3	Opolskie	16.49	36.87%
4	Zachodniopomorskie	15.89	28.26%
5	Łódzkie	15.62	21.19%
6	Małopolskie	15.01	25.92%
7	Pomorskie	14.96	25.33%
8	Świętokrzyskie	14.34	25.17%
9	Wielkopolskie	13.60	14.56%
10	Dolnośląskie	13.49	12.01%
11	Kujawsko-pomorskie	13.46	24.89%
12	Podkarpackie	13.24	17.75%
13	Lubuskie	12.69	10.64%
14	Lubelskie	12.18	21.35%
15	Warmińsko-mazurskie	11.88	18.60%
16	Podlaskie	11.26	18.38%

Source: UKE

Map 4

Average upload speed [Mbps] and change in 2024 compared to 2023 [%] from mobile application for all mobile providers

14.96
+25.3%
11.88
18.6%
15.89
+28.3%
13.46
+24.9%
11.26
+18.4%
16.77
+24.2%
12.69
+10.6%
13.60
+14.6%
15.62
+21.2%
12.18
+21.4%
13.49
+12.0%
16.49
+36.9%
17.10
+20.9%
14.34
+25.2%
15.01
+25.9%
13.24
+17.8%

Source: UKE

As in the case of average download speeds in mobile networks, the average upload speeds in mobile networks across the country also increased in all voivodeships in comparison to the previous year.

4.1. Certified IAS quality monitoring mechanism

As in previous years, the President of UKE, acting under Article 4(4) of the Regulation 2015/2120, invariably takes measures to provide end-users with an IAS quality measurement tool. In this respect, he certified the PRO Speed Test mechanism for monitoring the quality of internet access. The tool is available at: *https://pro.speedtest.pl.* It is fully compliant with web content accessibility guidelines – WCAG 2.1 AA, as confirmed by the Widzialni Foundation with the 'Barrier-Free Website' Certificate. The certificate provides a guarantee that the website is accessible to people with disabilities.

www.uke.gov.pl