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

Warsaw, 28 June 2023

Table of contents

1. Conclusions 2
2. List of legal acts and abbreviations 3
3. Monitoring of the Regulation 5
3.1. Information compiled from questionnaires received from ISPs 6
3.1.1. Rights to an open internet 6
3.1.2. Traffic management measures 7
3.1.3. Specialised services 9
3.1.4. Reports of end-users 12
3.2. Audit concerning Article 3(3) of the Regulation, i.e. Audit of the use of traffic prioritisation mechanisms 13
3.3 Presenting in contractual documents the information required by Article 4(1)(d) (first part) of the Regulation 14
4. Quality of internet access service 15
4.1. Certified IAS quality monitoring mechanism 26

1. Conclusions

This document presents the 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[1] for the period from 1 May 2022 to 30 April 2023.

We have analysed trade practices and traffic management measures applied by internet access providers, and specialised services as provided.

We also present data on service quality and actions taken by the UKE to provide quality monitoring tools.

The market situation analysis shows that:

1. All of the analysed 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 to the scope of information on the speed of offered services, were not introduced uniformly and do not provide a transparent source of information. This issue is to be investigated further.
2. Zero-rating services are provided in the Polish market, but ISPs are taking measures to remove such offers from the market. Services with this billing method are provided by both infrastructure operators and virtual operators.
3. The most frequently indicated specialised services by ISPs last reporting year were linear IPTV, VoIP telephony, VPN and data transmission services.
4. 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.
5. Over the analysed period, there is a clear upward trend in the area of data transmission speeds in downloading and uploading data. A large jump can be noticed in terms of the average download speed, which increased from 50.6 Mb/s in 2020 to 109.2 Mb/s in 2023 – a 116% increase in comparison to the results recorded in 2020.

[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.

2. List of legal acts and abbreviations

- The certified mechanism – a measurement system that enables certified measurements to be made and a report on certified measurements of the quality of Internet access service provided in fixed public telecommunications networks to be generated. 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;
- Telecommunications Act – Act of 16 July 2004 – Telecommunications Law (consolidated text: Journal of Laws of 2022, item 1648);
- 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;
- Act of 19 November 2009 on Gambling Games (consolidated text: Journal of Laws of 2023, item 227);
- BEREC Guidelines – BEREC Guidelines on the Implementation of the Open Internet Regulation, document number: 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;
- 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;
- 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*) – access network architecture in which fibre is brought into a building or a room in a building (e.g. a basement) and the final segment to the subscriber's premises is a physical medium other than fibre;
- FTTH (*Fiber-To-The-Home*) – access network architecture in which fibre 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 contains multimedia content such as graphics, animations, video clips or sounds in addition to text and uses packet data transmission;
- M2M (*Machine-to-Machine*) – a direct communication service between devices on wired and wireless networks;
- MPLS (*Multi-Protocol Label Switching*) – a layer 2.5 technique of the ISO-OSI model, used by routers, in which packet routing has been replaced by so called label switching, used for marking various types of traffic in the network and enabling implementation of QoS mechanisms in IP networks;
- MRTG (*Multi Router Traffic Grapher*) – software which uses the Simple Network Management Protocol (SNMP) for monitoring and measuring the traffic load on network links. It allows the user to see traffic load on a network over time in graphical form;
- 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*) – family of network protocols for managing devices such as routers, switches, computers or telephone exchanges over IP networks;
- 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 Wi-Fi*) – technology that allows users to make audio calls over wireless local 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 2022 to 30 April 2023, 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 the rules for the provision of specialised services by ISPs and their impact on the general quality of IAS;
- reports by end-users with regard to the rights and obligations as set out in Article 3 and Article and 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 performed a number of 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 twenty-one largest ISPs by number of users: Orange Polska S.A., P4 sp. z o.o., Polkomtel sp. z o.o., T-Mobile Polska S.A., UPC Polska sp. z o.o., 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., Canal+ Polska S.A., Leon Telekom sp. z o.o. spółka komandytowa, Jerzy Krempa running a business under the name Przedsiębiorstwo Produkcyjno- Montażowe Urządzeń Elektronicznych TELPOL Jerzy Krempa, Fiberlink sp. z o.o., Chopin Telewizja Kablowa sp. z o.o., Multimedia Capital One sp. z o.o., Gawex Media sp. z o.o., Oxylion S.A., Spódzielnia Telekomunikacyjna OST in Tyczyn. The ISPs that responded to the questionnaire provided internet access service in 2022 to 70,649,730 internet users, representing 95.5% of all internet users in Poland.

The questionnaire included questions on:

A. the rights of end-users to an open internet, in particular the use of commercial practices by ISPs to provide access to the services and content concerned in a zero rating model (Article 3(1)–(2) of the Regulation),

B. the ISP's traffic management measures – obligation of non-discriminatory treatment of data transmission (Article 3(3) of the Regulation),

C. the 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 general quality of which should not be degraded by the provision of services other than internet access services at a certain quality level (Article 3(5) of the Regulation),

D. the obligation to have transparent, simple and efficient procedures for processing end-users' complaints with regard to the rights and obligations set out in Article 3 and Article 4(1) of the Regulation.

2. An audit of the follow-up recommendations was carried out on contractual documents of nine ISPs in terms of the information required under Article 4(1)(d) (first part) of the Regulation.
3. An audit of one of the largest ISPs in Poland by number of users was carried out with regard to compliance with Article 3(3) and Article 5(2) of the Regulation in the period from 2017 to 2019, i.e. in terms of the application of traffic management mechanisms in the internet network.
4. Comparative monitoring of the quality of internet access services provided was evaluated.

3.1. Information compiled from questionnaires received from ISPs

3.1.1. Rights to an open internet

Twenty-one ISPs provided explanations to the President of UKE on business practices related to zero-rating offers. Under zero-rating offers, the providers apply a price of zero zlotys or flat-rate prices included in the price for other services, for data transmission associated with access to designated content and the operation of specific applications. The consumed data transfer of zero-rating services is not included in the data package limits applicable to the internet access service.

The ISPs provided information on the type of services provided, the content of the contractual templates, and the relationship with zero-rating offer providers. Some of the telecommunications service providers indicated that they provide zero-rating services. These include both infrastructure operators and virtual operators. Telecommunications undertakings operating in the Polish market include zero-rating access to content and applications such as:

- music streaming services;
- video-content services;
- websites such as banking and subscriber services;
- communication applications and websites;
- applications allowing navigation or access to e-books.

In the vast majority of offers, access to zero-rating content, applications and services, once the contractually available data package has been used, is treated in the same way as access to non-zero-rating services. This is most often associated with a reduction in data transmission speed when continuing to use the mobile internet access service ('funneling'). The ISPs' responses show that the 'funneling' used in their offers consisted in limiting the maximum speed of the connection.

Bearing in mind the provisions of the Regulation, service providers began efforts directed at removing the zero-rating services from the Polish market – some services are no longer sold and there is no option to activate them.

The President of UKE's evaluation of individual practices and actions of service providers was preceded by an analysis of the terms and conditions of the offers and their potential impact on end-users' right to an open internet. The President of UKE is analysing the zero-rating offers in the market, the practices of ISPs and actions taken by the undertakings to remove zero-rating offers from the market.

3.1.2. 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.

In the period under review, ISPs applied traffic management measures allowed by way of derogations set out in Article 3(3)(a)–(c) of the Regulation.

- blocking traffic due to obligations under Article 15f(5) of the Act of 19 November 2009 on Gambling Games [2] (point a);
- blocking traffic at the request of authorised entities on the grounds of a threat to defence, state security or public security and order, Article 180(1) Pt[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);

[2]Article 15f(5) of the Law on Gambling – 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 telecommunications entrepreneurs' 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 Law; 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 authorized entities, if such connections may threaten defense, state security and 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

- managing traffic in accordance with the legislation (Article 175(1) Pt[5] and Article 175c Pt[6]) in order to preserve the integrity and security of the network, of services provided via that network, and of the terminal equipment of end-users (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 Scientific and Academic Computer Network, National Research Institute (Naukowa Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy, NASK – PIB), which are used to defraud end-users' data and funds by removing them from their ICT systems used for converting Internet domain names into IP addresses. The cooperation with operators is based on the Agreement entered into on 23 March 2020 by and among the Minister of Digital Affairs, the President of UKE, Director of NASK PIB, and Orange Polska S.A., Polkomtel Sp. z o.o., P4 Sp. z o.o., T-Mobile Polska S.A. Other ISPs can also download the above warning list and implement it in their security systems to block malicious content.

ISPs explained that they continuously monitored the level of network traffic and took necessary measures to increase network capacity and reliability. The main actions undertaken in this period included:

- increasing network capacity (network capacity was increased at the access, distribution and backbone layer as required);
- expansion of links to external operators;
- network modernisation;
- modernization of network devices, reconfiguration of devices;
- expansion of congested network nodes;
- purchase of additional bandwidth for traffic exchange nodes, increasing bandwidth to Tier 1 operators or points of connection between operators;
- renegotiation of agreements between operators;
- increase of the number of transceiver stations;
- optimization of bandwidth use;
- allocation of additional frequency resources (e.g. 5G);
- capacity expansion at selected base stations, by increasing the number of carriers, increasing the number of sectors;

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 organizational 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.

- implementation of link redundancy to traffic exchange points.

The above measures made it possible to provide top-quality services.

Some ISPs reported that they blocked TCP/UDP ports for incoming traffic, directed to the end-user devices. ISPs block the following ports: 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, TCP/UDP 161 and 162. In two cases, all ports for incoming traffic are blocked. One ISP explained that ports open to certified services, in line with the TR069 standard, which facilitate secure communication between ISP's terminal equipment are an exception. Another ISP indicated that they offer services with no such restrictions. Ports are blocked for incoming traffic due to: vulnerability of services running on these ports, ensuring 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 this port is implemented in connection with the sending of unsolicited commercial information, or information containing spyware or applications, or the use of this port to attack computer systems. The reason for blocking, provided by ISPs, is the obligation to ensure integrity, security of networks and services provided through those networks and of terminal equipment of end users.

ISPs also use DPI technology (two ISPs) to classify traffic for billing purposes and to provide services offered by ISPs. 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.

Furthermore, as explained by ISPs, the security mechanisms as implemented can potentially impact the availability of content, apps and services. Reports of end-users are monitored to minimize their adverse effects. Also, the use of NAT can impact the use of some services or availability of ports open within an active session.

The analysis of other information in UKE's possession also showed that no traffic management measures were used which consisted of: blocking, slowing down, changing, limiting, degrading or prioritising certain traffic to prevent imminent network congestion or to mitigate the effects of exceptional or temporary network congestion caused by increased levels of internet traffic due to the declared epidemic state, and as of 16 May 2022 – epidemic risk.

During the reporting period, no end users submitted complaints to the UKE with respect to blocking ports, blocking or limiting access to content, apps or services.

In Poland, during the reporting period, ISPs provided zero-rating services, whose description is provided in par. 3.1.1.

3.1.3. 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'.

The aim of the study covering the last reporting period performed based on UKE's questionnaire was to establish 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 the requirements for a given 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 used 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) a specialised service is not used by an ISP to circumvent the rules concerning traffic management measures applicable to the internet access service.

The replies of the twenty-one ISPs who answered questions on specialised services in the UKE's questionnaire show that:

1) Seven ISPs provide specialised services in their network: IPTV, VoIP, VPN and data transmission (3 ISP), VoLTE, VPBX, telemetry, private APN (2 ISP), APN Xcap, MMS, VOD, NB-IoT and VoWiFi (1 ISP);
2) Three ISPs stated that they also acted as intermediaries to offer a specialised IPTV service in the name and on behalf of another entity;
3) Thirteen ISPs stated that they neither provided nor acted as intermediaries in providing specialised services in the name and on behalf of other entities.

The most frequently indicated specialised services by 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 (Machine to Machine), telemetry, video monitoring, server backup, access to the corporate network, dedicated terminals with access only to the customer's network resources, access to the internet via the customer's network to overlay policies applied to internet access on the customer's network.

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). The ISPs that indicated VoIP as a specialised service stated that it could not be provided within IAS, for instance, because certain QoS (Quality of Service) parameters need to be guaranteed, including low delays and ensuring that packets arrive in the order they were sent.

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

- use of equipment dedicated to a specific specialised service;

- traffic separation at the physical layer of the network via dedicated ports on the customer's terminal equipment;
- traffic separation at the network data link layer (e.g. by separating separate VLANs);
- use of the MPLS protocol 'at the interface' between the data link layer and the network layer;
- configuration of private APNs for separated data transmission;
- allocation of a specific frequency resource from the available band to a particular specialised service.

Five ISPs stated that they do not use a specialised service to provide IAS. Four ISPs indicated that the specialised service includes IAS or there is a possibility to provide this service. Parameters of this access are no different than access offered under general terms and conditions or capacity is limited (e.g. in telemetry).

Evaluation of the impact of the provision of a specialised service on IAS by ISPs is carried out by:

- controlling the throughput of connections and analysing access quality;
- network load analysis in the backbone and access segments;
- monitoring of packet/frame loss on network interfaces;
- monitoring of service quality indicators within a mobile network, i.e. CSSR call success rate and DCR call failure rate;
- carrying out a technical survey during which technical possibilities for the provision of a specialised service.

Most ISPs (six out of nine) assess the impact of specialised services on IAS. Undertakings that do not assess the impact of specialised services on IAS quality highlighted that, among others, such services had a negligible impact on network capacity during peak traffic hours, hence a detailed analysis was not conducted. The analysis of the responses of ISPs contained in the questionnaire prepared by UKE 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 dedicated 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.

Among the actions aimed at ensuring an adequate quality of IAS while providing specialised services, ISPs mentioned:

- 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;
- expansion of infrastructure aimed at increasing network capacity while exceeding certain bandwidth occupation levels by specialised services;
- dividing the area into smaller areas to lower the usage of access links;
- base station network densification in the case of mobile networks.

3.1.4. Reports of end-users[7]

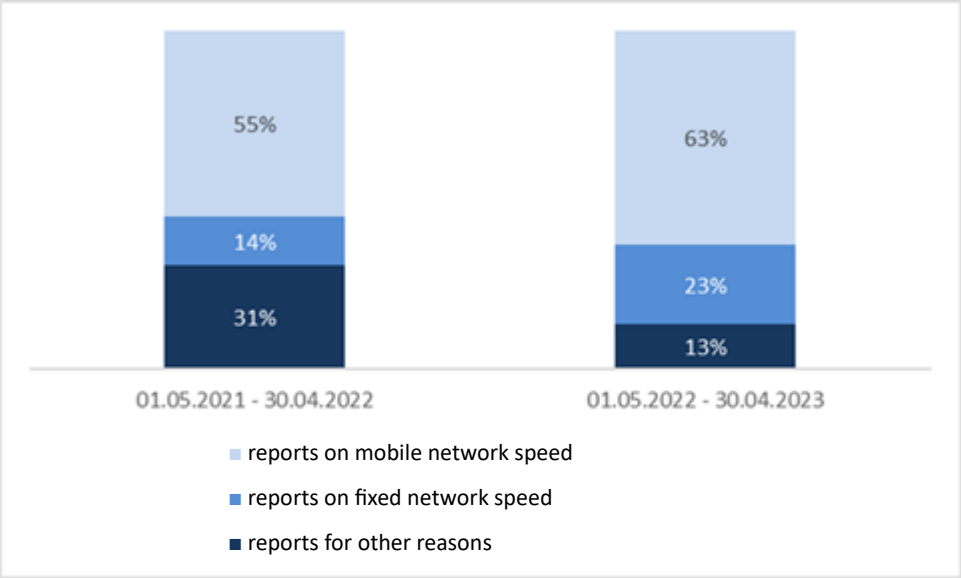
One of the tasks performed by the President of UKE is assistance provided to end users (including consumers) by taking action as a response to problems with telecommunications services reported by end users. During the period under review, i.e. from 1 May 2022 to 30 April 2023, users reported problems with, among others, the right to open internet.

Compared to the previous period, the number of reported problems in this area decreased by 11%. Customers communicated most often issues regarding the speed of internet access services as provided (as in the previous period):

1. mobile internet – problems with coverage, low data transfer: 63% of all reports on the right to open internet,
2. fixed internet – failure to reach the minimum/declared/usually available speeds set forth in contracts with providers: 23% of all reports on the right to open internet.

Out of these two categories, the greater change of dynamics in the share of total reports compared to the previous period pertained to user reports on fixed internet speed – their share increased by 64% (the share of letters concerning mobile Internet increased by 15%).

Chart: comparison of reasons for customer reports



As part of its activities, the President of UKE also analysed the subject 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 2022 and 30 April 2023 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.

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

3.2. Audit concerning Article 3(3) of the Regulation, i.e. Audit of the use of traffic prioritisation mechanisms

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 online 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 experts specialising in Internet traffic surveillance and routing mechanisms.

Currently, the President of UKE is evaluating the evidence gathered.

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

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

- in the case of fixed networks: minimum, normally available, maximum and advertised download and upload speed of the internet access services;
- in the case of mobile networks: estimated maximum and advertised download and upload speed of the internet access services.

In 2019, the President of UKE carried out inspections of 10 large ISPs as regards their compliance with the aforementioned 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 a follow-up recommendations to telecommunications operators on the need to amend specific provisions in contractual documents.

The 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, usually available, maximum and declared speeds for fixed networks or estimated maximum and declared 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.

The follow-up recommendations indicated that 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 follow-up recommendations, the President of UKE conducted an audit of 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. Currently, the President of UKE is analysing the materials gathered in the course of the audit.

4. Quality of internet access service

The level of quality of internet access services offered to end-users has to allow and guarantee the use of content, applications and modern services available on the internet.

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 depicts the quality of internet access services based on measurements carried out

in April 2023, and in order to observe the trend of changes over the years, it was related to data from a few previous years, i.e. measurements carried out in the last seven years (from 2016 to 2022).

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.
  - 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.

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 end-users themselves, i.e. by internet users. 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, the conditions of radio wave propagation, etc.

The analysis of data from the previous three 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 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 in both directions with a simultaneous decrease in the ping parameter (reduction in data transmission delay).

The table and graph below clearly indicate that an upward trend can be seen over the years in the area of data speeds in both directions over the years analysed – both in terms of upload and download. A particularly large increase in the area of upload speed is noticeable in the last three years. The average download speed has risen from 50.6 Mbps in 2020 to 109.2 Mb/s in 2023, which is an increase of 116 % compared to 2020.

Table 1

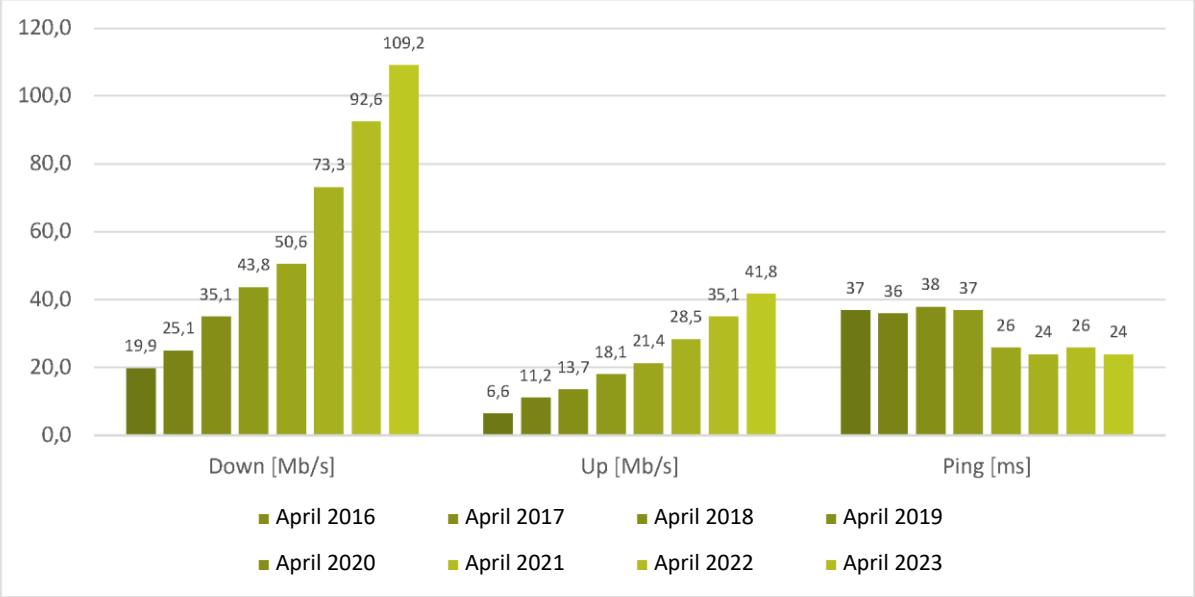
Average download and upload speed and ping from the browser application

	April 2016	April 2017	April 2018	April 2019	April 2020	April 2021	April 2022	April 2023
Download [Mb/s]	19.9	25.1	35.1	43.8	50.6	73.3	92.6	109.2
Upload [Mb/s]	6.6	11.2	13.7	18.1	21.4	28.5	35.1	41.8
Ping [ms]	37	36	38	37	26	24	26	24

Source: UKE

Figure 1

Average download and upload speed and ping from the browser application



Source: UKE

Despite a slight increase in the level of packet delay transmitted in 2022 (to a level of 26 ms), a general downward trend over the years analysed is noticeable. In 2016, the ratio was 37 ms, with a decrease to 24 ms in 2023.

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 delay times of packet transmission. In 2020, some slowdown of this trend can be observed 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

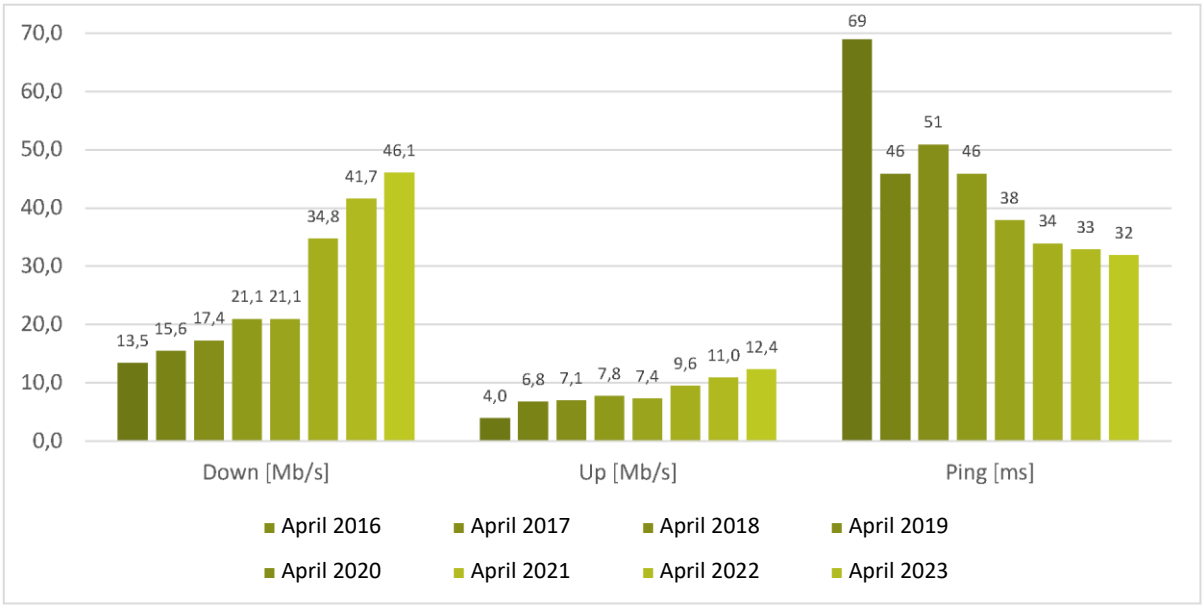
Average download and upload speed and ping from the mobile application

	April 2016	April 2017	April 2018	April 2019	April 2020	April 2021	April 2022	April 2023
Download [Mb/s]	13.5	15.6	17.4	21.1	21.1	34.8	41.7	46.1
Upload [Mb/s]	4.0	6.8	7.1	7.8	7.4	9.6	11.0	12.4
Ping [ms]	69	46	51	46	38	34	33	32

Source: UKE

Figure 2

Average download and upload speed and ping from the browser application



Source: UKE

In the case of measurements performed with the use of a browser in the user direction (download), the results obtained prove that over the analysed years there has been a clear increase in the share of speed in the user direction for services from the range above 100 Mb/s. 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

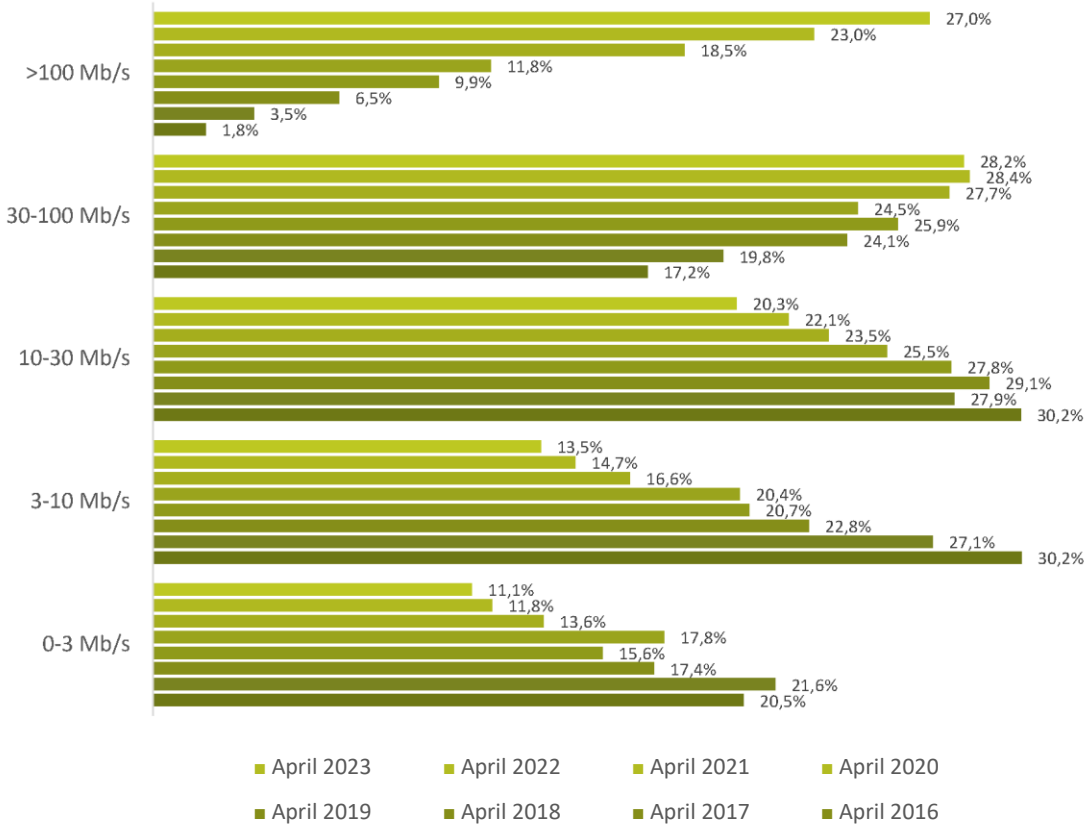
Distribution of the number of download speed measurements in ranges (web app)

Download	April 2016	April 2017	April 2018	April 2019	April 2020	April 2021	April 2022	April 2023
0-3 Mb/s	20.5%	21.6%	17.4%	15.6%	17.8%	13.6%	11.8%	11.1%
3-10 Mb/s	30.2%	27.1%	22.8%	20.7%	20.4%	16.6%	14.7%	13.5%
10-30 Mb/s	30.2%	27.9%	29.1%	27.8%	25.5%	23.5%	22.1%	20.3%
30-100 Mb/s	17.2%	19.8%	24.1%	25.9%	24.5%	27.7%	28.4%	28.2%
>100 Mb/s	1.8%	3.5%	6.5%	9.9%	11.8%	18.5%	23.0%	27.0%

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 user direction (upload), 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 upload speed, especially from the range above 100 Mb/s. 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)

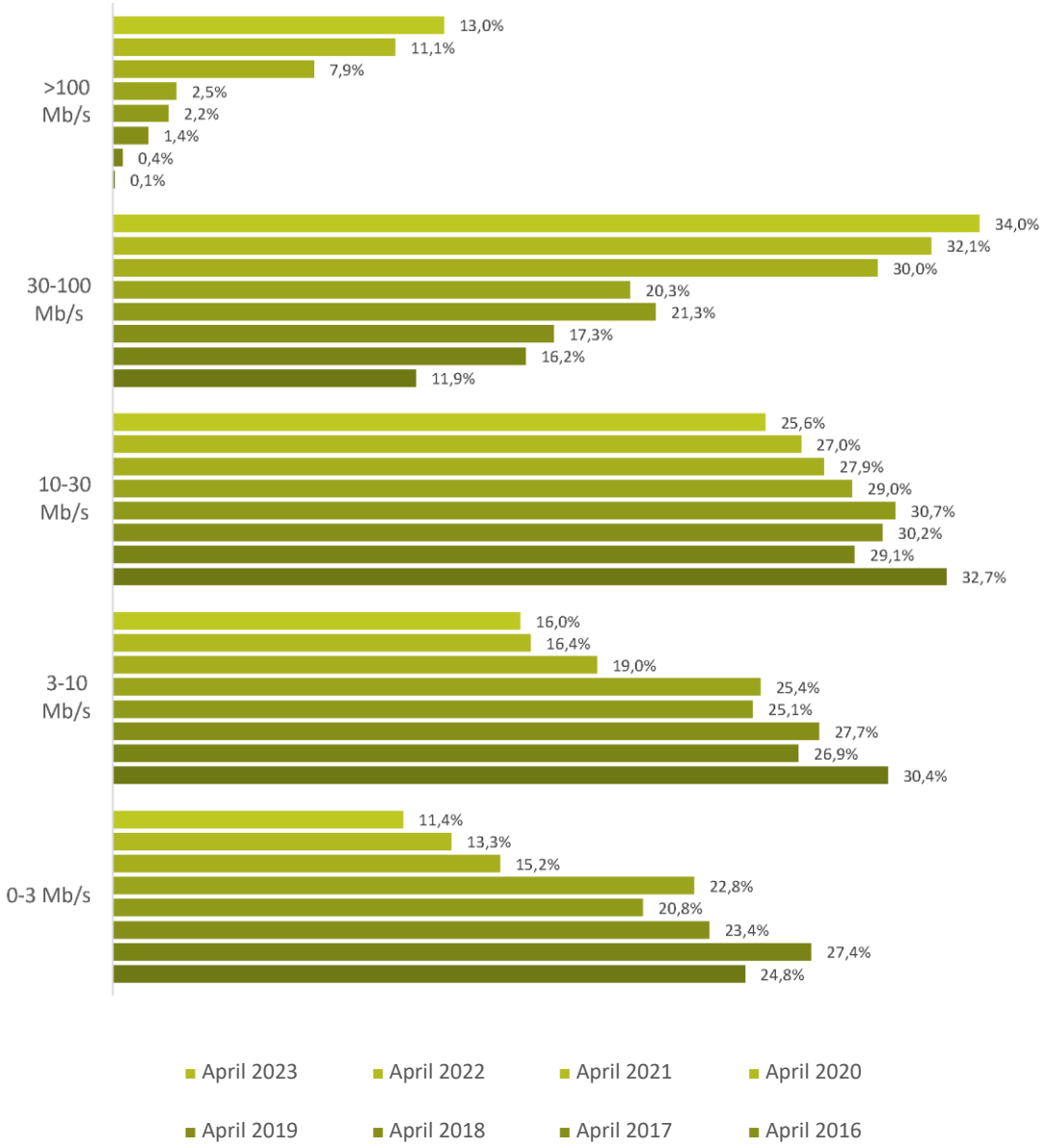
Download	April 2016	April 2017	April 2018	April 2019	April 2020	April 2021	April 2022	April 2023
0-3 Mb/s	24.8%	27.4%	23.4%	20.8%	22.8%	15.2%	13.3%	11.4%
3-10 Mb/s	30.4%	26.9%	27.7%	25.1%	25.4%	19.0%	16.4%	16.0%
10-30 Mb/s	32.7%	29.1%	30.2%	30.7%	29.0%	27.9%	27.0%	25.6%
30-100 Mb/s	11.9%	16.2%	17.3%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

Source: UKE

It is important to be aware that especially in 2021 it was mostly the pandemic condition that suddenly increased mobile data traffic (from 2.5% to 7.9%).

Figure 4

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



Source: UKE

Table 5

Average download speed [Mb/s] and change in 2023 compared to 2022 [%] from browser application for all fixed providers

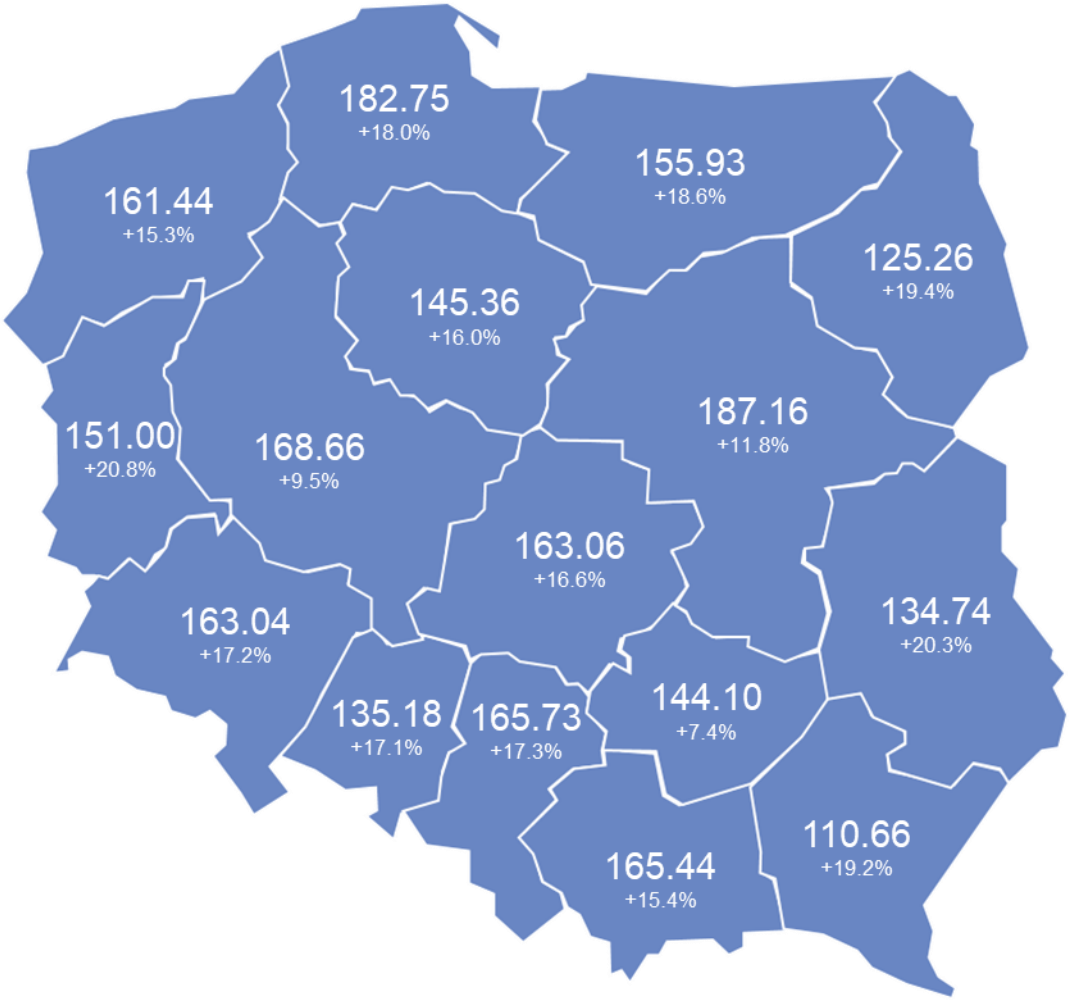
No.	Voivodeship	Average result [Mb/s]	Increase compared to 2022
1	Mazowieckie	187.2	11.80%
2	Pomorskie	182.8	18.03%
3	Wielkopolskie	168.7	9.46%
4	Śląskie	165.7	17.34%
5	Małopolskie	165.4	15.39%
6	Łódzkie	163.1	16.62%
7	Dolnośląskie	163.0	17.17%
8	Zachodniopomorskie	161.4	15.26%
9	Warmińsko-mazurskie	155.9	18.57%
10	Lubuskie	151.0	20.75%
11	Kujawsko-pomorskie	145.4	16.03%
12	Świętokrzyskie	144.1	7.44%
13	Opolskie	135.2	17.10%
14	Lubelskie	134.7	20.33%
15	Podlaskie	125.3	19.38%
16	Podkarpackie	110.7	19.22%

Source: UKE

Average download speeds in fixed networks across the country exceed 100 Mb/s. For several years now, the highest value has always been recorded in the Mazowiecke Voivodeship, including 187.2 Ms/s this year.

Map 1

Average download speed [Mb/s] and change in 2023 compared to 2022 [%] from browser application for all fixed providers



Source: UKE

In April 2023, compared to the same period of the previous year, a definite increase in the average download speed was recorded in all voivodeships. The largest increase in average download speed was achieved in the Lubuskie Voivodeship (to 151 Mb/s – a 20.75% increase compared to 2022), while the smallest increase was achieved in the Świętokrzyskie Voivodeship (to 144.1 Mb/s – a 7.4% increase compared to 2022).

A similar tendency was recorded in all voivodeships in terms of the average upload speed – an increase of 29% on average in comparison to the previous year.

Table 6

Average upload speed [Mb/s] and change in 2023 compared to 2022 [%] from browser application for all fixed providers

No.	Voivodeship	Average result [Mb/s]	Change
1	Wielkopolskie	63.84	20.27%
2	Podlaskie	39.29	25.55%
3	Mazowieckie	36.7	31.99%
4	Śląskie	36.5	26.74%
5	Dolnośląskie	34.41	24.64%
6	Zachodniopomorskie	33.6	42.89%
7	Pomorskie	33.33	27.90%
8	Świętokrzyskie	31.34	31.72%
9	Małopolskie	30.47	31.97%
10	Łódzkie	27.76	19.31%
11	Opolskie	27.55	29.04%
12	Lubuskie	26.58	33.97%
13	Kujawsko-pomorskie	25.14	33.25%
14	Lubelskie	24.9	34.10%
15	Warmińsko-mazurskie	24.06	24.23%
16	Podkarpackie	23.35	27.28%

Source: UKE

The vast majority of voivodeships also saw a decrease in the average delay value of data streams. Similarly to the previous year, the largest decrease was recorded in the Lubuskie Voivodeship, down to 19 ms.

Table 7

Average download speed [Mb/s] and change in 2023 compared to 2022 [%] from mobile application for all mobile providers

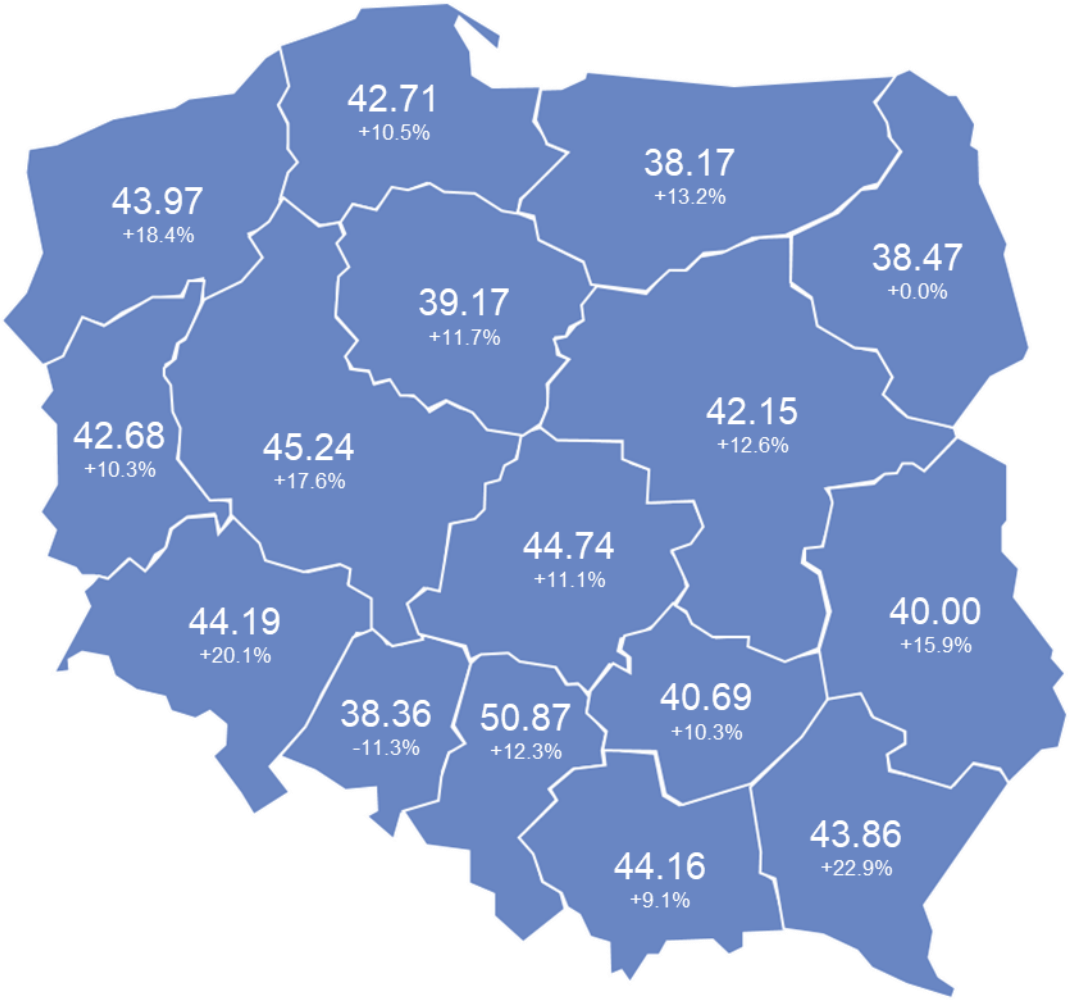
No.	Voivodeship	Average result [Mb/s]	Change
1	Śląskie	50.9	12.3%
2	Wielkopolskie	45.2	17.6%
3	Łódzkie	44.7	11.1%
4	Dolnośląskie	44.2	20.1%
5	Małopolskie	44.2	9.1%
6	Zachodniopomorskie	44.0	18.4%
7	Podkarpackie	43.9	22.9%
8	Pomorskie	42.7	10.5%
9	Lubuskie	42.7	10.3%
10	Mazowieckie	42.2	12.6%
11	Świętokrzyskie	40.7	10.3%
12	Lubelskie	40.0	15.9%
13	Kujawsko-pomorskie	39.2	11.7%
14	Podlaskie	38.5	0.0%
15	Opolskie	38.4	-11.3%
16	Warmińsko-mazurskie	38.2	13.2%

Source: UKE

Average download speeds in mobile networks across the country are similar and do not differ very significantly from each other. Similar to the results of the average download speed from the browser application for all fixed providers, for mobile providers in April 2023, there was a definite increase in the average download speed in almost all voivodeships compared to the same period last year. It was only the Opolskie Voivodeship where there was a drop of the average data download speed compared to 2022 – down to 38.4 Mb/s (the speed was 43,3 Mb/s in 2022).

Map 2

Average download speed [Mb/s] and change in 2023 compared to 2022 [%] from mobile application for all mobile providers



Source: UKE

The highest increase in average download speed was achieved in the Podkarpackie Voivodeship (22.9%), the lowest in the Małopolskie Voivodeship (9.1%). The growth trend indicates that telecommunications undertakings are trying to respond to user demand associated with more intensive use of mobile network technologies.

Table 8

Average upload speed [Mb/s] and change in 2023 compared to 2022 [%] from mobile application for all mobile providers

No.	Voivodeship	Average result [Mb/s]	Change
1	Śląskie	13.5	12.3%
2	Mazowieckie	12.7	14.5%
3	Łódzkie	12.3	15.0%
4	Dolnośląskie	11.9	17.1%
5	Wielkopolskie	11.6	16.1%
6	Zachodniopomorskie	11.4	11.5%
7	Lubuskie	11.3	7.1%
8	Pomorskie	11.2	9.5%
9	Małopolskie	11.1	8.7%
10	Podkarpackie	10.9	18.2%
11	Świętokrzyskie	10.7	17.0%
12	Opolskie	10.4	6.2%
13	Kujawsko-pomorskie	10.1	14.1%
14	Warmińsko-mazurskie	9.7	5.1%
15	Lubelskie	9.6	18.4%
16	Podlaskie	9.2	-1.5%

Source: UKE

As in the case of average download speeds in mobile networks, the average upload values in mobile networks across the country are also similar and not significantly different from each other. With the exception of the Podlaskie Voivodeship, there was an increase in all voivodeships in average upload speeds compared to the same period last year.

4.1. Certified IAS quality monitoring mechanism

The President of UKE, acting under Article 4(4) of the Regulation 2015/2120, with a view to supporting the rights of end-users, as well as creating market conditions supporting the activities of ISPs in improving the quality of telecommunications services, took steps to further provide end-users with a tool to measure the quality of IAS (certified IAS quality monitoring mechanism).

In November 2022, the UKE President extended the certificate for the PRO Speed Test internet access quality monitoring mechanism for another two years (until the end of November 2024). The application for personal computers (for Windows and macOS operational software) allows for certified measurements to be performed and a Certified Internet Access Service Quality Measurement Report to be generated. The report can be used, among other things, in complaint proceedings to demonstrate consistent and recurring discrepancies between the actual performance of the Internet access service and the contractually indicated values.

The aim of the mechanism is to contribute to increasing the protection of users and providing information on the parameters of the services provided to them, as well as increasing competition between suppliers based on the quality of the services provided.

The tool performs a certified measurement, and also allows for independent measurement of the speed of fixed and mobile Internet (non-certified measurement).

When performing a measurement, the mechanism verifies under what conditions the measurement was performed. Among other things, it checks such elements as CPU load, type of network card, presence of active VPN links, volume of background traffic generated, number of devices in the user's home network. Therefore, according to the law, the measurement of a fixed line taken through the mechanism makes it possible to determine the improper performance of the contract and effectively pursue consumer claims against the service provider.

The tool also allows the UKE President to assess the quality of internet service offered by telecommunications operators in Poland.

The *https://pro.speedtest.pl* website 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.

The PRO Speed Test measurement system consists of the following components:

- website with a user panel;
- desktop application for Windows and macOS computers;
- mobile applications;
- WEB applications.

Between 1 May 2022 and 30 April 2023, users using the mechanism performed the following numbers of measurements:

- certified – application for Windows – 56,047,
- non-certified – application for Windows – 122,695,
- certified – application for macOS – 409,
- non-certified – application for macOS – 2,572,
- non-certified – Web application – 47,447,
- non-certified – application for Android – 328,830,
- non-certified – application for iOS – 86,082.

Office of Electronic Communications

Department of Monitoring
T +48 22 534 9158
F +48 22 534 9310
sekretariat.dk@uke.gov.pl

Department of Technology
T +48 22 534 9320
F +48 22 534 9306
sekretariat.dt@uke.gov.pl

Department of Consumer Policy
T +48 22 534 9225
F +48 22 534 9175
sekretariat.dpk@uke.gov.pl

www.uke.gov.pl