SPECIAL ISSUE NO. 1

dot.pl

.pl NASK

dot.pl

dot.pl

SUMMARY REPORT 2023

SPECIAL ISSUE NO. 1
WARSAW, MAY 2024

ISBN: 978-83-65448-85-9

mail.pl
com.pl
aid.pl
auto.pl
atm.pl
edu.pl
agro.pl
gmina.pl
mil.pl
info.pl
targi.pl
gsm.pl
mil.pl
miasta.pl
media.pl
realestate.pl
shop.pl
net.pl
kolobrzeg.pl
nieruchomosci.pl
szkola.pl
org.pl
sklep.pl
sos.pl
travel.pl
gniezno.pl
turystyka.pl
nom.pl

Spis treści

Introduction

Information and communication technologies create new opportunities for widespread consumption, including the consumption of information. Today, the paradigm of the consumer is being replaced by the paradigm of the network user – a client, whose digital data and content, including those generated through Internet behavior, are commonly monetized and used for marketing purposes through profiling and targeting. Increasingly, these activities encompass a wide range of actions related to providing various digital services. However, it is important to remember that the Internet itself is no longer a uniform entity. As a fragmented space, it is a battleground for control over emerging new technologies. Besides data, a valuable commodity, there is a struggle for freedom of speech, privacy, digital property rights, and economic freedom.

Paul Baran, a scientist of Polish descent, is an example of someone who was ahead of his time. Today, we know that although his visions of the future were not appreciated in the 1960s, they have indeed come true. Through his collaboration with the Rand Corporation, a research organization affiliated with the United States Air Force, Paul Baran developed his project, described in an 11-volume monograph titled „On Distributed Communications," published in 1964. He also authored a scientific article published in the Rand Paper (P-3717) titled „Some changes in information technology affecting marketing in the year 2000" (July 1968). In it, Paul Baran described his vision of the future in the year 2000, highlighting the development of e-commerce based largely on electronic communication and the concept of virtual stores. Today, this vision is not a criticized illusion but a reality and part of our daily lives. A fundamental consequence of technological changes has been the emergence of a new space for the functioning of individuals, social groups, and even the state. This space is cyberspace. Today, its analysis and attempts to define it are practically necessary to determine the spatial scope of legal norms related to new technologies. This space is associated with the system of internet domains, as well as with other environments where we all function online, including social media. On April 20, 1992, the first national top-level domain with the .pl suffix was registered. In the early 21st century, their number reached 200,000, and by 2024, it had grown to 2.5 million.

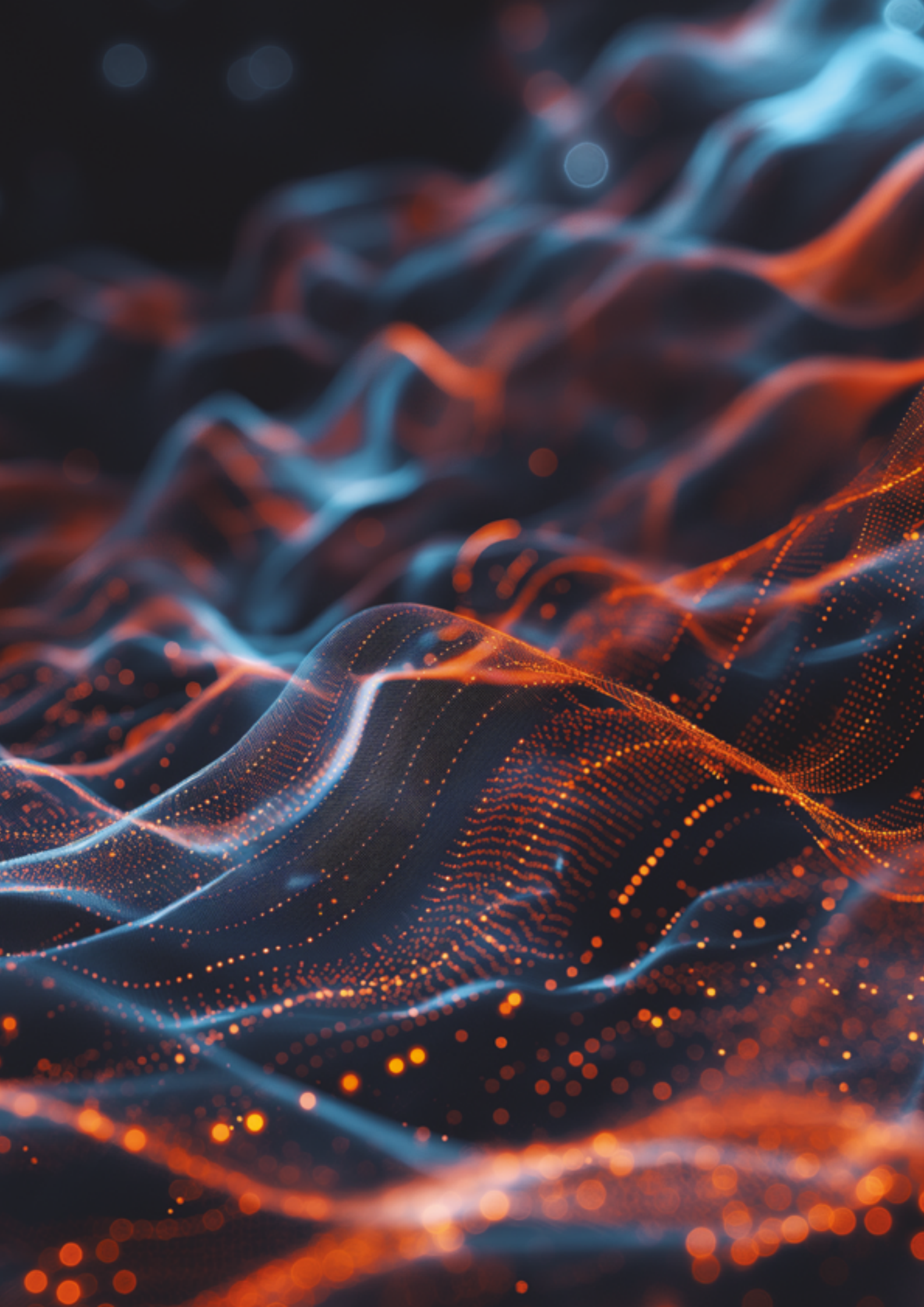
With new media come the activities of corporations – businesses whose primary goal is profit, generated among other things through online trade and the accompanying advertising activities. Therefore, analyzing these techniques will

allow for a precise determination of future problems related to the functioning of cyberspace and its associated network environment. Identifying threats related to network services and reviewing current issues related to the protection of property online will enable us to diagnose the necessity of redefining future regulatory goals in the area of proprietary rights associated with monopoly, entitlements to intangible assets such as copyright and related rights, trade secrets, know-how, objects of industrial property protection, and databases. According to Peter Weibel's idea, alongside digital thinking, whose influence and successes have already spread worldwide (after all, no airports, factories, train stations, shopping centers, hospitals, and others would function without "counting machines"), digital art is also emerging, gaining significance and popularity. It is worth adding that security is becoming a key aspect of this development. Another important element of this market's development is the need for security, which stems from the creativity unleashed by innovations and new technologies. In a practical sense, such property is an internet domain, and its key feature is its secure dimension.

Today, online activity requires prior registration of an internet domain, which allows the rightful owner to operate a website in market conditions while reserving these activities based on public order and safety. In the hydrant of information and chaos of BIG DATA, an internet domain provides certainty in identifying one's digital environment. The extraterritoriality of the network has contributed to the creation of a global internet domain registration system. The accepted principles have created opportunities for assigning various domain names on a "first come, first served" basis, giving a personalized profile to a specific digital environment.

The report prepared by the .pl domain registry at NASK-PIB on the development of the domain market, as well as an attempt to review and redefine trends in the digital world, will allow for an evaluation of the accepted standards for protecting this environment in the future. The conclusions from this analysis may serve as an introduction to an expanded diagnosis related to the new stage of digital era development.

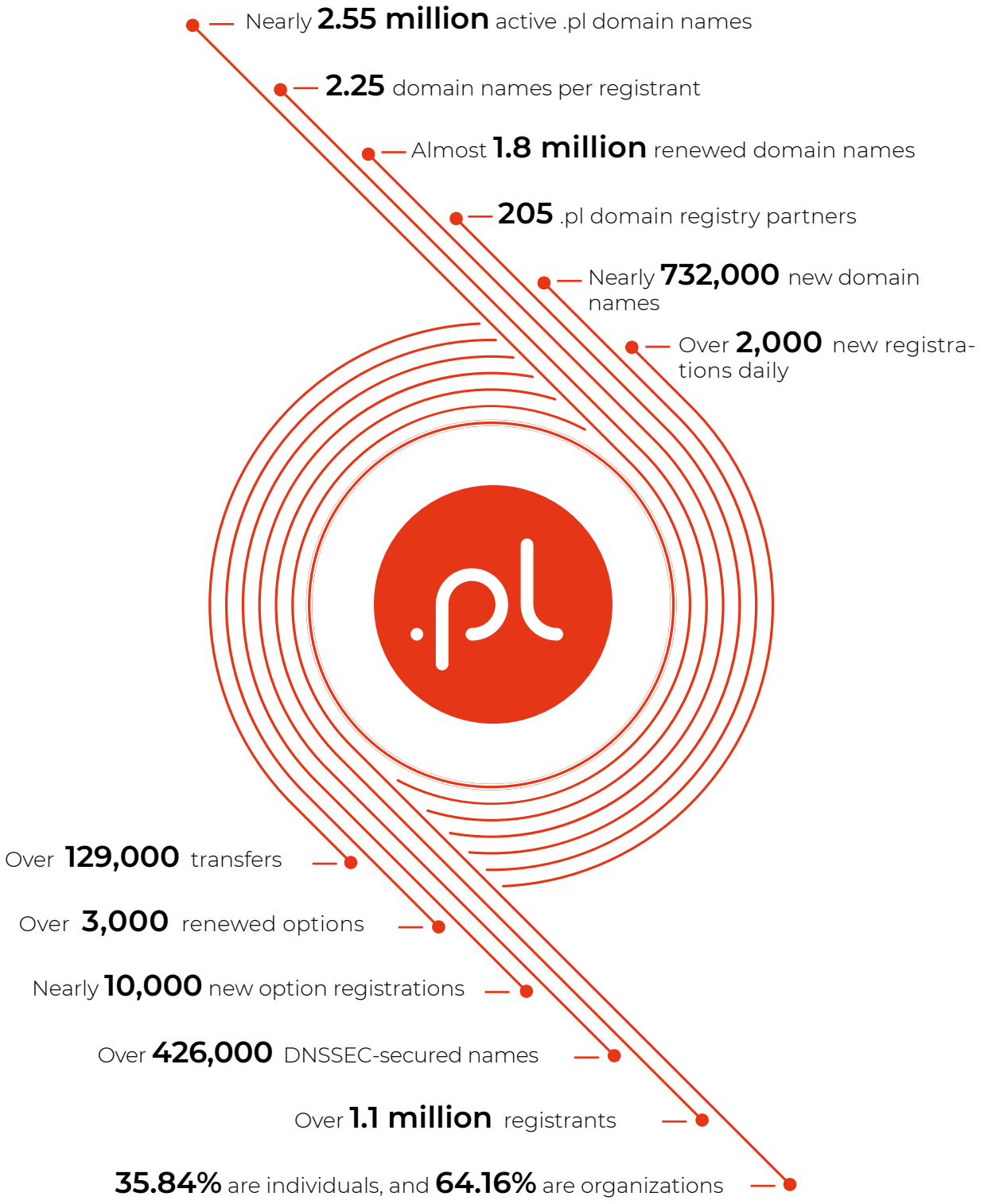
We invite you to read!



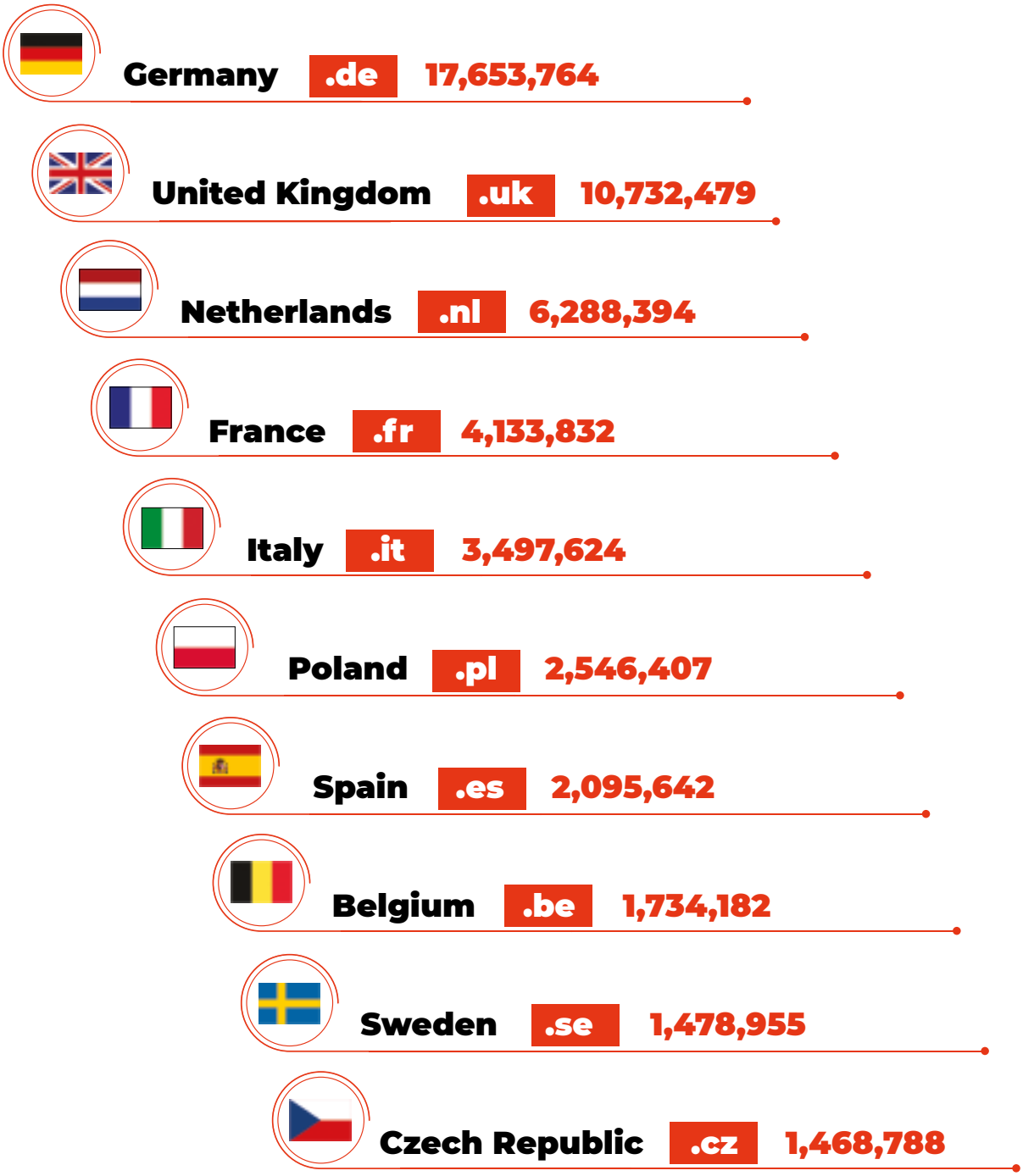
PART I

The .pl Domain Name Market

Facts and Figures



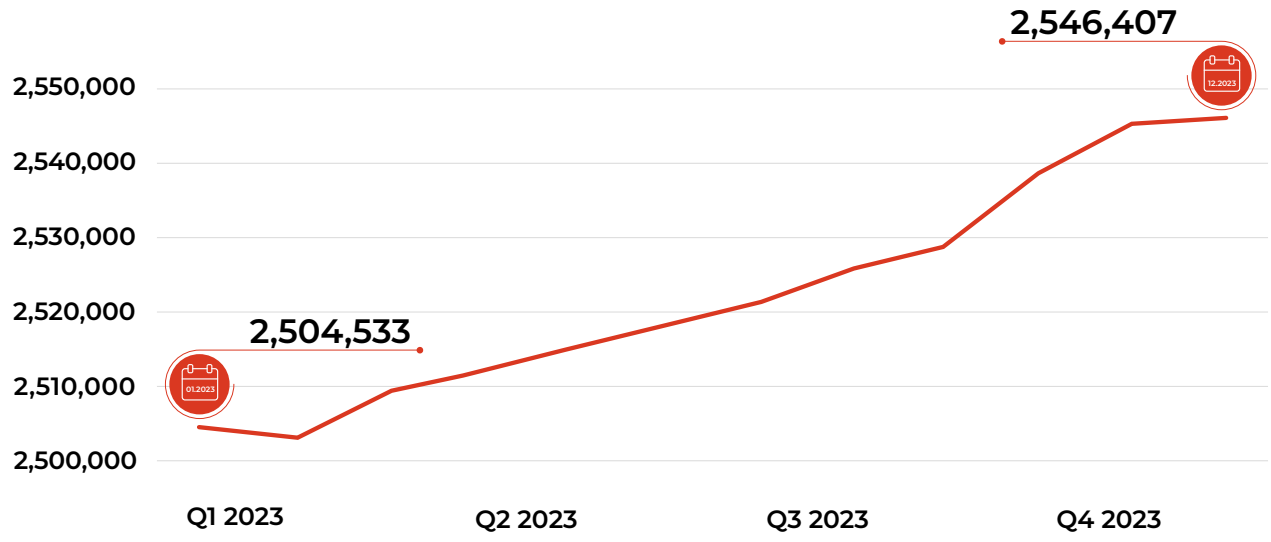
Ranking of European domain registries



Domain Management

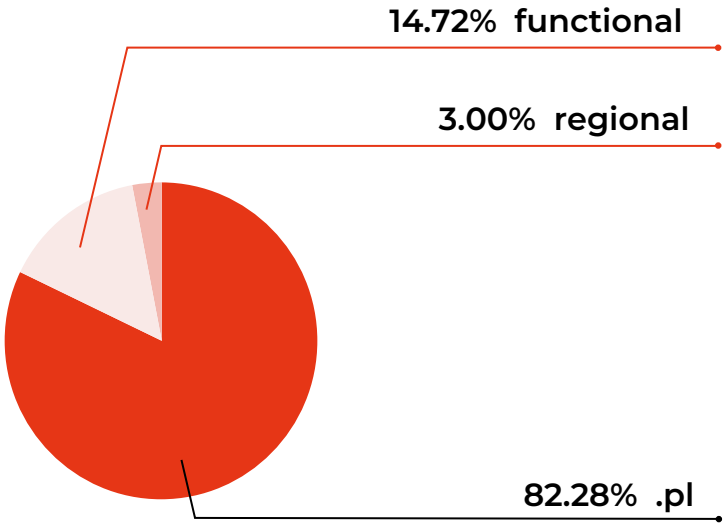
The number of names maintained in the .pl domain

In 2023, the number of domain names, active in DNS, increased by **36,151**, with an annual growth rate of **1.44%**.

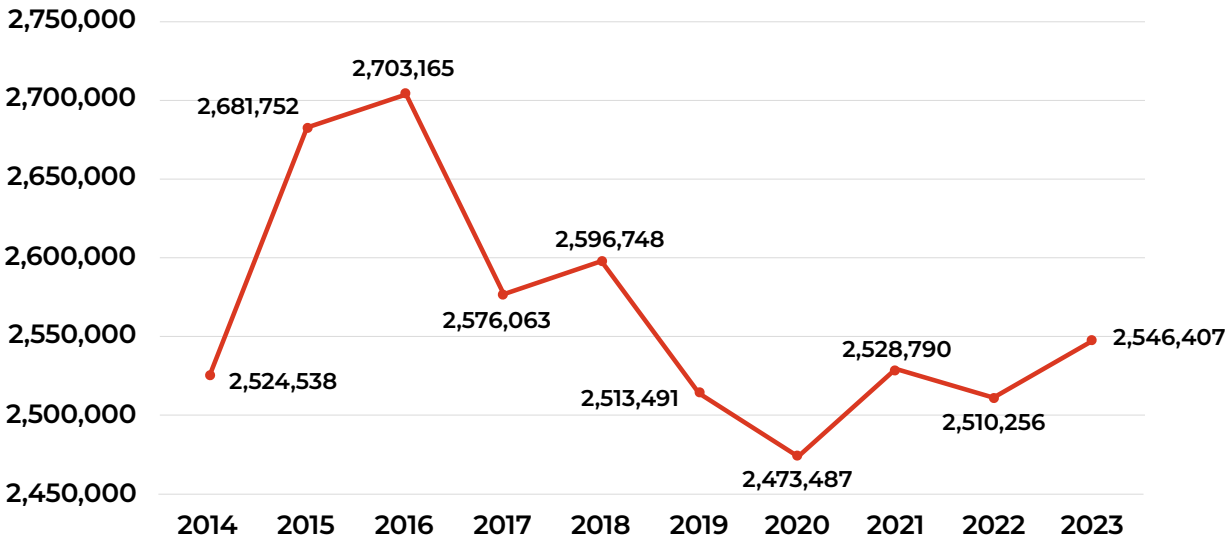


.pl domain names, active in DNS categorized by zone type

Division of names into those located directly in the .pl domain, functional domains such as .com.pl, .edu.pl, and others, as well as regional domains such as .waw.pl, .bieszczady.pl, and others.



Number of .pl domain names in DNS, 2014–2023



Number of .pl domain name registrations

year 2023

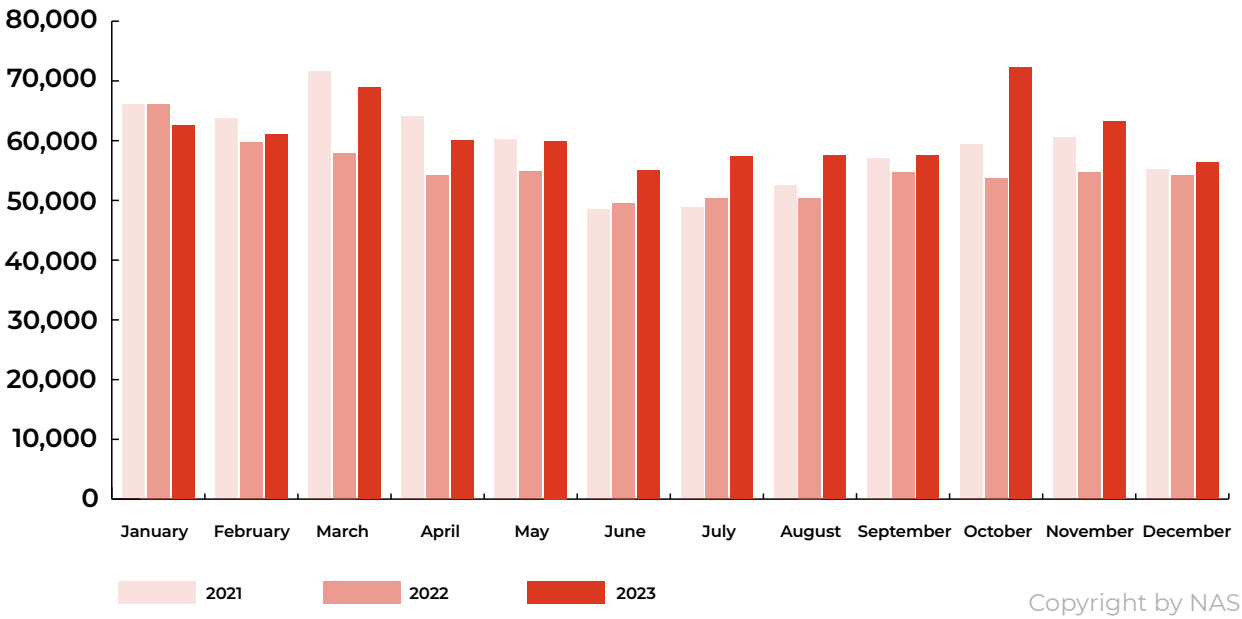
number of registrations
731,748

average daily number of name registrations
2,005

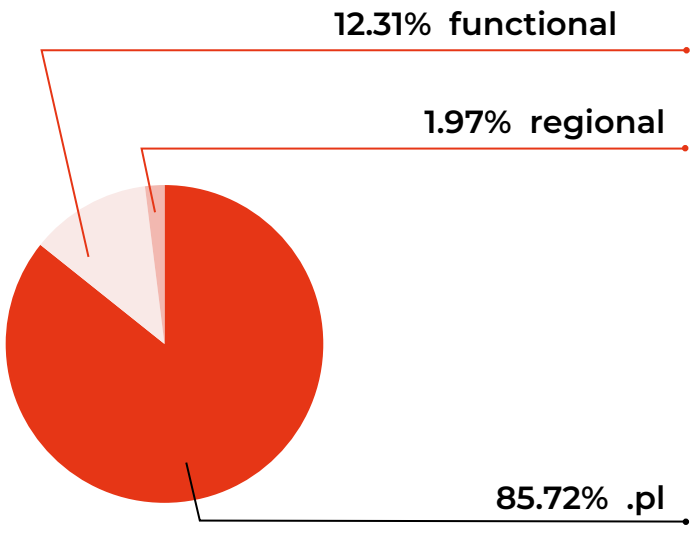
the most domains were registered in October -
72,237

the fewest domains were registered in June -
55,052

Number of .pl domain name registrations



.pl domain name registrations divided by zone type



Division of names into those located directly in the .pl domain, in functional domains such as .com.pl, .edu.pl and others, and in regional domains, e.g. .waw.pl, .bieszczady.pl and others.

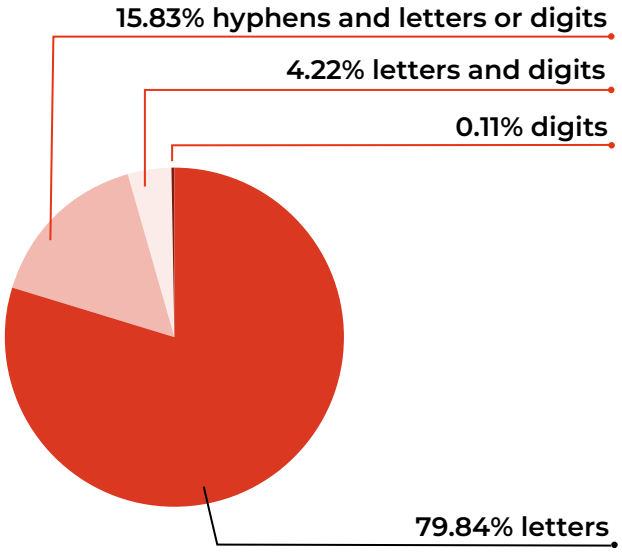
.pl domain name structure

Average number of characters used in .pl domain names at the end 2023 was **10.93.**

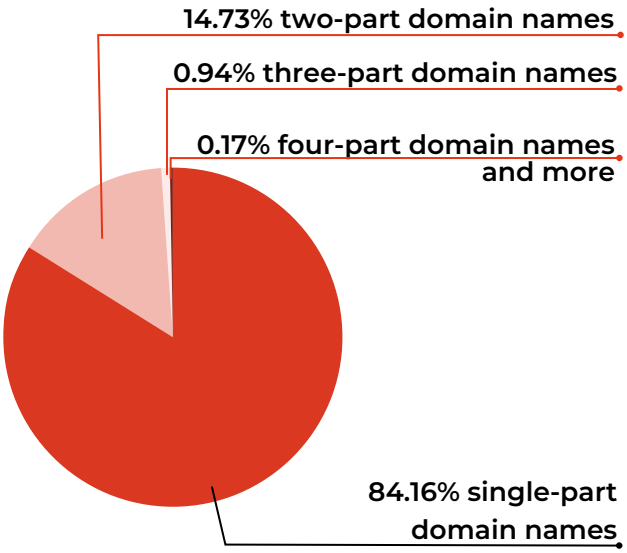
8 .pl domain names had a maximum number of **63** characters.

The most common were **nine-character** names , in the registry there were **229,390** of them.

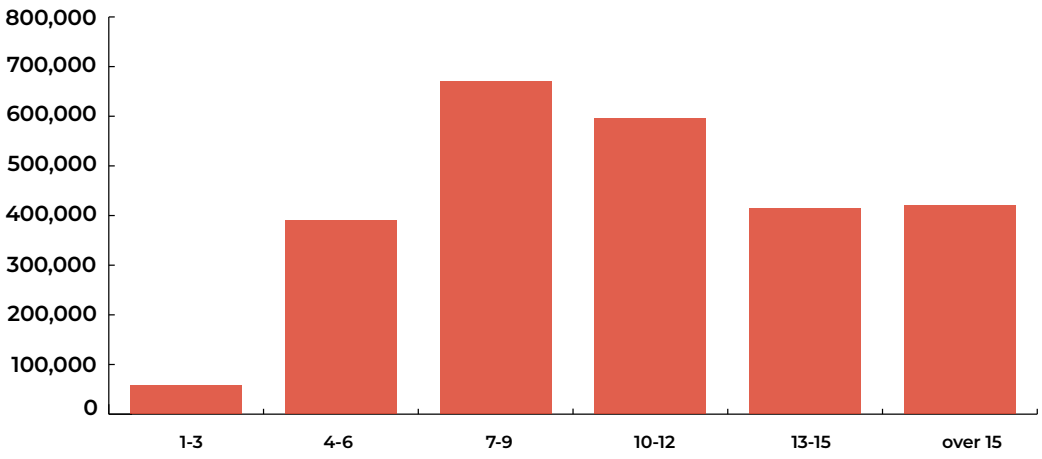
The maximum number of elements appearing in one name, recorded at the end of 2023, was **26**.



Characters in .pl domain names 2023



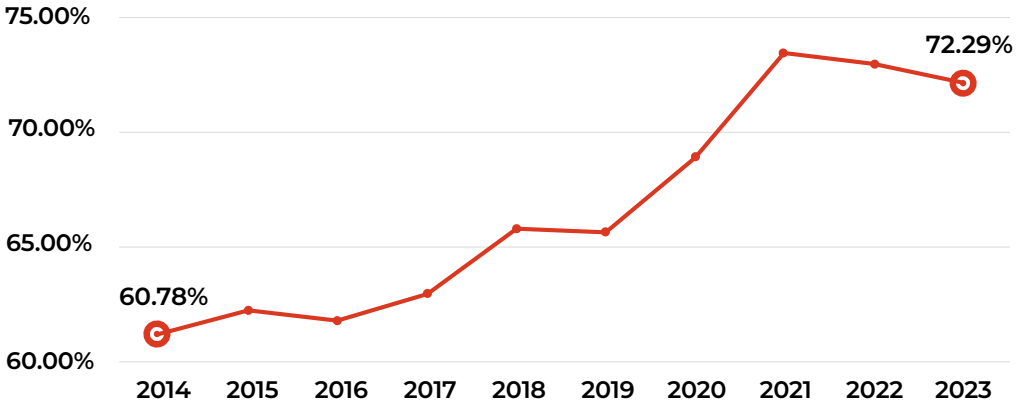
Number of parts in .pl domain names, 2023



Number of characters in .pl domain names, 2023

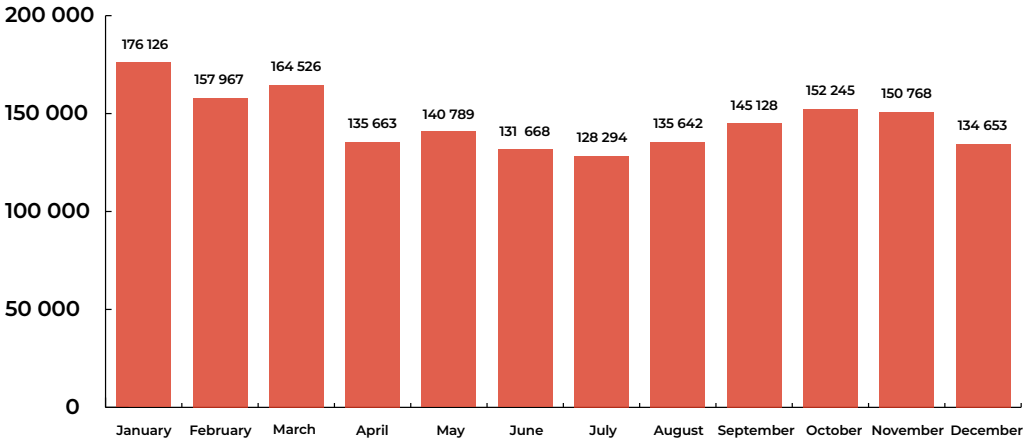
Renewal of .pl domain names for the consecutive billing period

Years 2014–2023



Percentage of .pl domain name renewals, 2014–2023

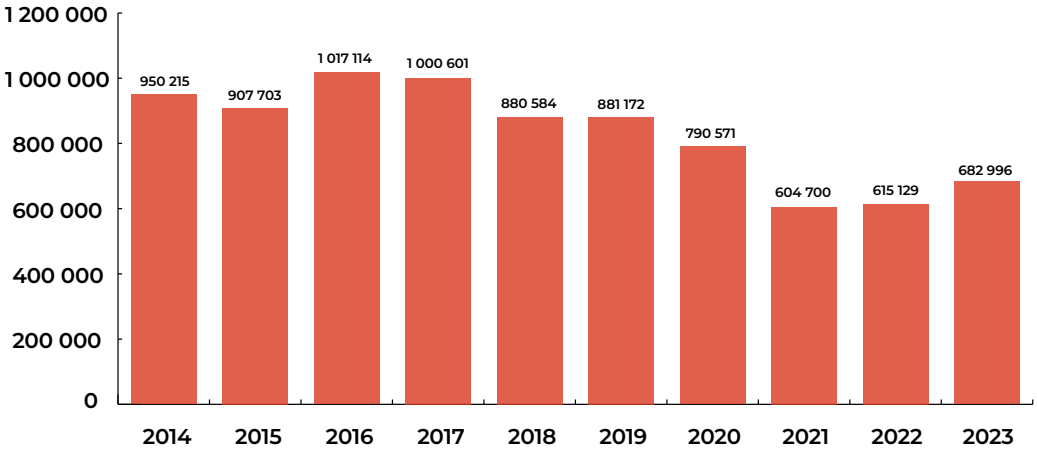
2023



Number of renewed .pl domain names, 2023

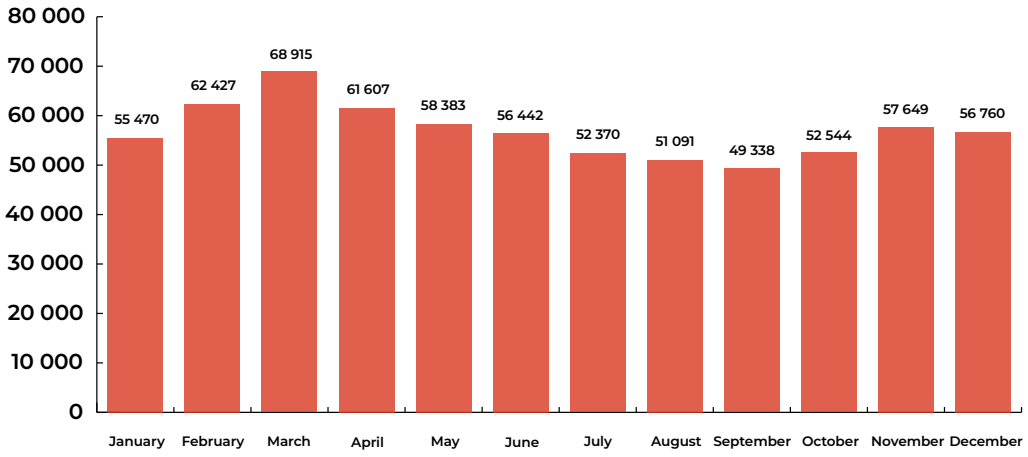
Number of not renewed .pl domain names

Years 2014–2023



Number of .pl domain names released due to lack of renewal, 2014–2023

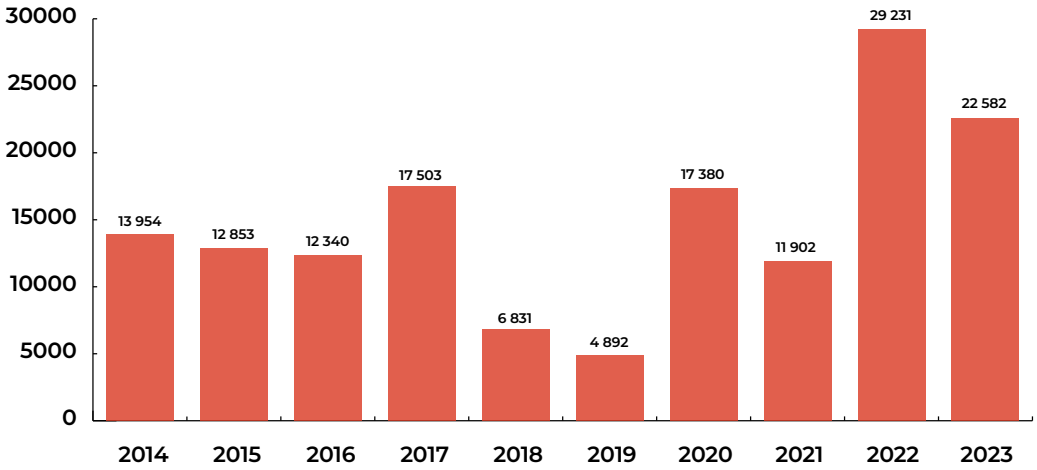
2023



Number of .pl domain names released due to lack of renewal, 2023

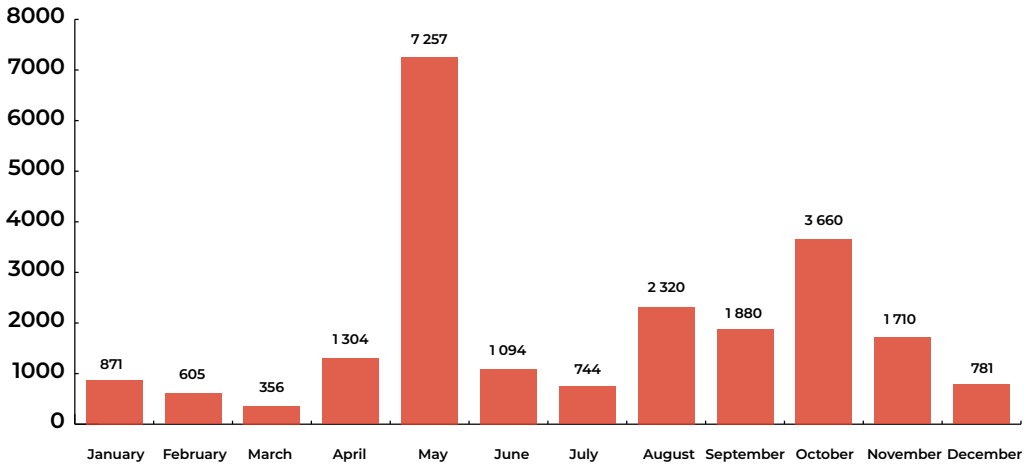
Number of deleted .pl domain names

Years 2014–2023



Number of .pl domain names released after prior deletion, 2014–2023

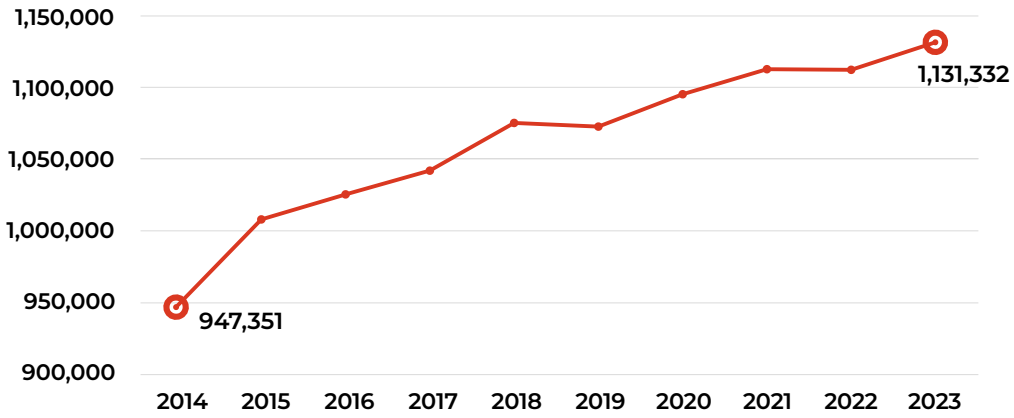
2023



Number of .pl domain names released after prior deletion, 2023

Service of .pl domain name registrants

Number of .pl domain name registrants



Number of Registrants, 2014–2023

18,983 number of registrants who joined in 2023

170,322 number of .pl domain name registrant changes in 2023

2.25 .pl domain names on average per one registrant

64.16% registrants are organizations

35.48% registrants are natural persons

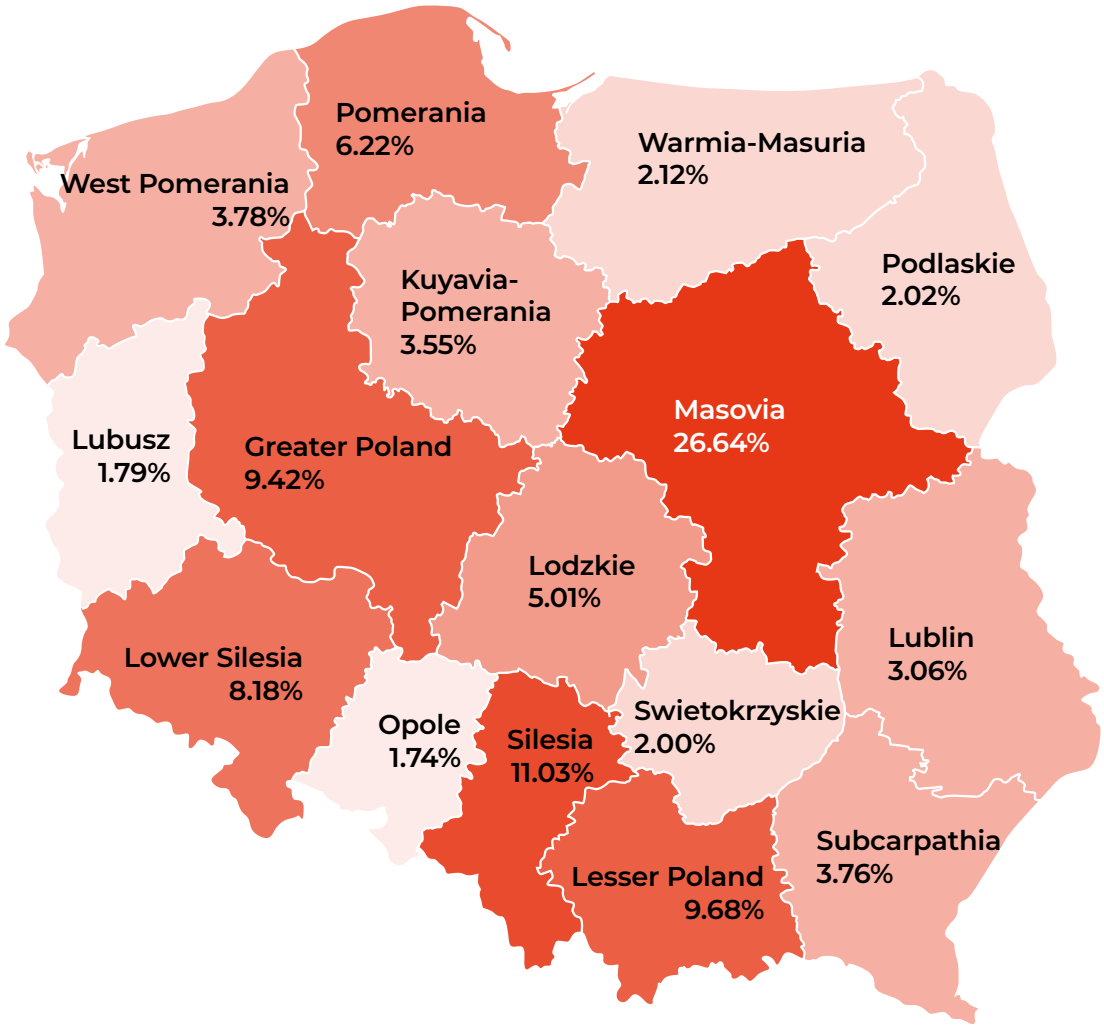
Location of .pl domain registrants

90.56% .pl domain names existing in DNS at the end of 2023, maintained for registrants from Poland

26.64% names were registered for people and organizations from the Masovian Provinces, of which as many as 18.87% were from Warsaw

Almost half of all registrants from Poland were domain users from the following provinces:

26.64% Masovian
11.03% Silesian
9.68% Lesser Poland



Location of registrants in Poland, divided into provinces, 2023

Statements of Partners of the .pl domain Registry

Home.pl S.A.

home.pl

In 2023, like in previous years, it became evident that .pl remains the favored domain among Polish registrants. The statistics clearly show that both gTLDs, nTLDs, and other ccTLDs are significantly less popular choices. .pl stands out as the most frequently used domain by Poles, reflecting a natural affinity towards one's homeland. This preference also indicates that the majority of businesses and entrepreneurial ventures remain local, primarily focused within Poland. The .pl domain holds a prestigious and established position, inspiring trust while offering transparent registration conditions. Its popularity is further bolstered by the presence of the Internet Domain Arbitration Court at the Polish Chamber of Information Technology and Telecommunications (PIIT), ensuring registrant security.

Throughout 2023, we observed a notable increase in customer interest for registering .pl domains compared to 2022, particularly at the second level, which saw the highest growth. The proportion of functional and regional domains in new registrations remained relatively stable throughout the year.

Most customers promptly utilized their purchased domains to operate websites and online stores. There is a declining trend among registrants to register large numbers of domains for speculative purposes or resale. Concurrently, we noticed an uptick in .pl domains serving as the primary internet addresses for Polish entrepreneurs and individuals in 2023. This shift may be attributed to factors such as inflation and cost optimization, encouraging users to opt for the more economical .pl domain extensions over less popular alternatives.

The .pl domain renewal market in 2023 was stable, with a high rate of renewal among domains registered in previous years. This stability underscores the maturity of the market, which is not surprising given that the .pl domain celebrated its 33rd anniversary in 2023.

Following a highly successful year for the .pl domain in 2023, we maintain an optimistic outlook for 2024.

Consulting Service Sp. z o.o.

The past year brought a certain revival in the national domain market. This is reflected in the increasing number of newly registered .pl domain names and a rising renewal rate, resulting in a slight overall increase in active .pl domains compared to the years 2022, 2021, and 2020.

It is intriguing whether this will mark the beginning of a new positive trend for this domain segment. Additionally, one cannot overlook the .com domain, which continues to attract new registrants in our country, maintaining its top position globally in terms of registered domain names. Despite the depletion of popular names and successive annual base price increases, the .com domain remains attractive, especially for business entities.

In 2024, we anticipate the continuation of the growth trend in the .pl domain market, particularly in new registrations. Significant here are events beyond our eastern border and the increasing interest by Ukrainian businesses in Polish addresses, as they relocate their operations to Poland and invest in our national internet addresses.

At the same time, it is worth considering whether, due to the implementation of the DSA Regulation and the expected introduction of NIS 2, the number of active .pl domain names in the current year will at least maintain the levels seen at the end of 2023. This includes requirements such as updating incomplete or unreliable data of registrants maintaining their domains in the .pl registry system.

nazwa.pl sp. z o.o.

The year 2023 can be described as a year of changes in the process of registering internet domains. An essential mechanism that began to play a role in decision-making regarding the choice of a particular address is Artificial Intelligence. Observing trends in this area, nazwa.pl launched a domain name search engine based on AI technology. This engine enables finding domains based on natural language queries. Artificial Intelligence algorithms not only determine the industry based on these queries but also analyze keywords characteristic of that industry. This results in proposals for perfectly matched domains. We estimate that the significance of AI in domain registration will continue to grow, increasing its share for newly registered names.

The Polish domain market remains stable with a growing number of active websites. Registered domains, previously held for investment purposes, are increasingly used for launching websites, brand identity, and product or service promotion.

This contributes to the normalization of the market, which is reflected in domain renewal rates.

According to research by nazwa.pl, over 80% of inquiries for Polish-language websites originate from within our country. Domains indicating a business's location in Poland help build its prestige and enhance customer reach. While nazwa.pl offers registration of increasingly popular nTLD domains that relate to specific industries or business characteristics, it must be acknowledged that Polish extensions continue to enjoy unwavering popularity.

Today, the domain market is highly competitive. Among numerous offerings, clients can select those that best meet their expectations. Basic solutions generally feature prices similar to NASK wholesale rates. Premium solutions, such as the „Secure Domain" package at nazwa.pl, are also available. This package includes essential functionalities and services alongside the domain name, particularly security measures crucial in the digital world. These include DNS service on geographically dispersed Anycast servers, ensuring higher levels of protection and operational reliability. The „Secure Domain" package also encompasses DNSSEC and DNS over TLS protections. It is certainly beneficial for similar security standards, long established at nazwa.pl, to be adopted by other NASK partners.

OVH SAS

The past year in the .pl domain segment was exceptionally satisfying for OVHcloud. Looking from a broader perspective, strong domain sales results reflect robust online project health. Digital business remains robust, with an increase in e-projects driving demand and user investment in new domains.

In 2023, domain renewals at OVHcloud maintained a stable level, a metric recognized by NASK during their annual Partner Conference, where OVHcloud was awarded first place for the highest number of „.pl" domain renewals.

We were also pleased to be among the top three registrars for new domains in the country. We aim to maintain this position as we recognize that for most website registrants in Poland, a „.pl" domain is crucial for company positioning and identity. Furthermore, .pl domains continue to be bestsellers, consistently chosen as the first preference by many users. Across the Vistula, it is widely accepted that .pl provides the best recognition. This is unsurprising given its presence for over three decades, firmly establishing itself in users' consciousness to the extent that companies operating here opt for names with a Polish extension.

Furthermore, in our assessment, the growing online market also influences, as we observe, the need to ensure stability and security of digital projects. Users are seeking secure solutions, and therefore, we will consistently focus on providing

top-quality services in the domain segment and other products within our portfolio, including public cloud services.

PERSKIMEDIA Szymon Perski

In the past year, our observations have confirmed that a key aspect of our offering is not price, but rather a high level of technical support, focusing on the individual needs of our users, and consistent quality of services. We have also noticed an increase in cases of abuse related to the use of national domains. Additionally, there has been heightened interest in acquiring foreign domains, particularly European and gTLDs. Within our portfolio, which consists of over 115,000 domains, these foreign domains now constitute 17%, up from 15% in the previous year. Looking ahead, we anticipate another year of challenges, including intensifying preventive measures against the misuse of internet addresses registered through our service for illegal purposes.

DOMENY.TV MSERWIS Sp. z o.o.

In 2023, we recorded a significant, more than twofold increase in the number of .pl domain registrations on our platform compared to 2022.

We believe several factors contributed to this growth. The most important factor was the improving economic environment. Decreasing inflation dynamics led our clients to look towards the future with greater optimism. This resulted in a high number of domain registrations for new projects and a lower rate of renewal cancellations compared to the previous year.

Although we offer nearly 1100 extensions on our Domeny.tv platform where users can register their domain names, .pl domains remain the undisputed leader in terms of registrations in Poland. It is consistently the first choice for projects targeting the Polish market. Often, even if another extension is chosen as the primary address for a project, a .pl domain name is registered simultaneously to secure the brand.

Regular education of domain registrants is also a crucial aspect. For several years, we have focused particularly on naming issues. Choosing the right domain name and extension is extremely important for business strategy. We provide knowledge to our audience through articles on our blog and naming e-books to help them make informed decisions in this area.

We also educate our clients on security practices, and we see the effect in the increasingly common adoption of DNSSEC, maintaining complete and up-to-date contact information, and securing access to domain panels with 2FA applications or hardware keys. Collaboration with NASK is also crucial for swiftly

detecting and responding to incidents, such as domain names being used for phishing purposes. It is in the best interest of the entire market for our clients to have a thorough understanding of the benefits and possibilities of using their own .pl domain name. This collectively increases the likelihood of renewing domain services in the coming years.

LH.pl Sp. z o.o.

In 2023, at LH.pl, we observed a significant increase in customer interest in domain and hosting services following a challenging 2022 due to the outbreak of war. Companies were more willing to purchase additional domain extensions and opt for larger hosting packages. Among our successes last year, we achieved positive ISO 9001 and 27001 certifications, affirming our quality standards and high level of security.

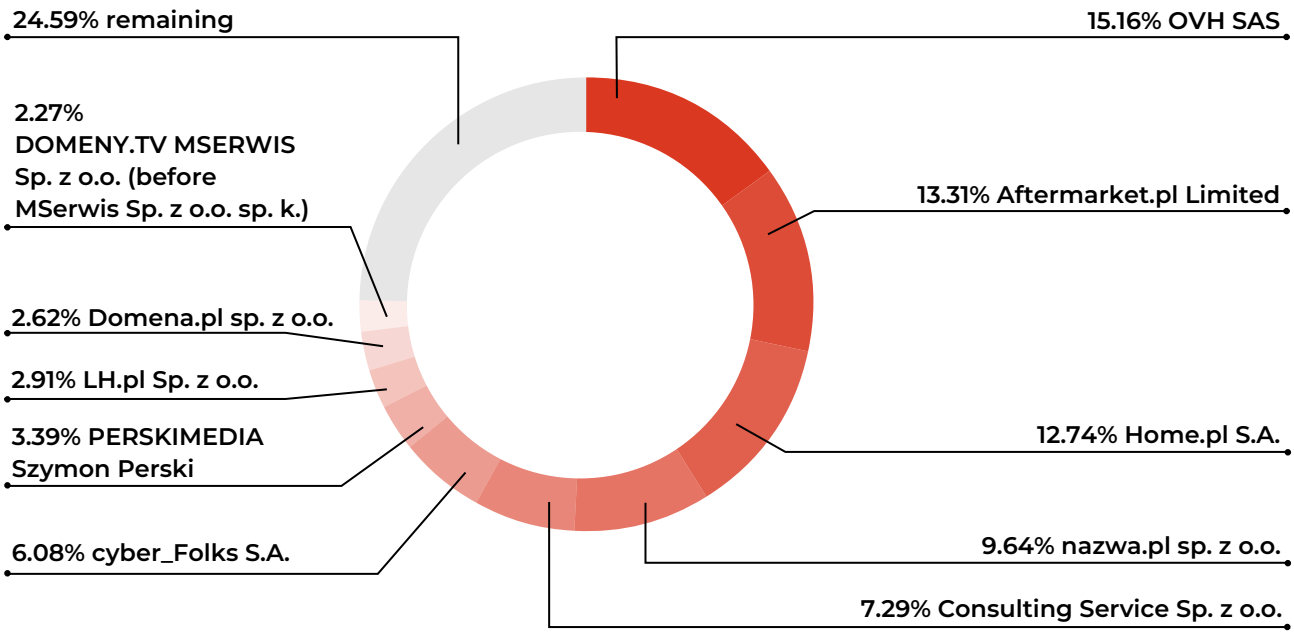
However, 2023 also brought numerous challenges. Like other companies, we faced rising operating costs primarily due to wage increases and energy prices. Domain registrars and hosting companies were burdened with various legislative obligations: the Digital Services Act (DSA), the outline of NIS2 (Directive on measures for a high common level of cybersecurity across the Union), and the Law on combating abuses in electronic communications. We also anticipate the inevitable implementation of the Electronic Communications Law, which will impose additional responsibilities.

In 2023, our security department noted an increased number of cyber attacks, such as phishing. More .pl domains were registered with the intent of conducting phishing activities. We implemented solutions to minimize associated risks.

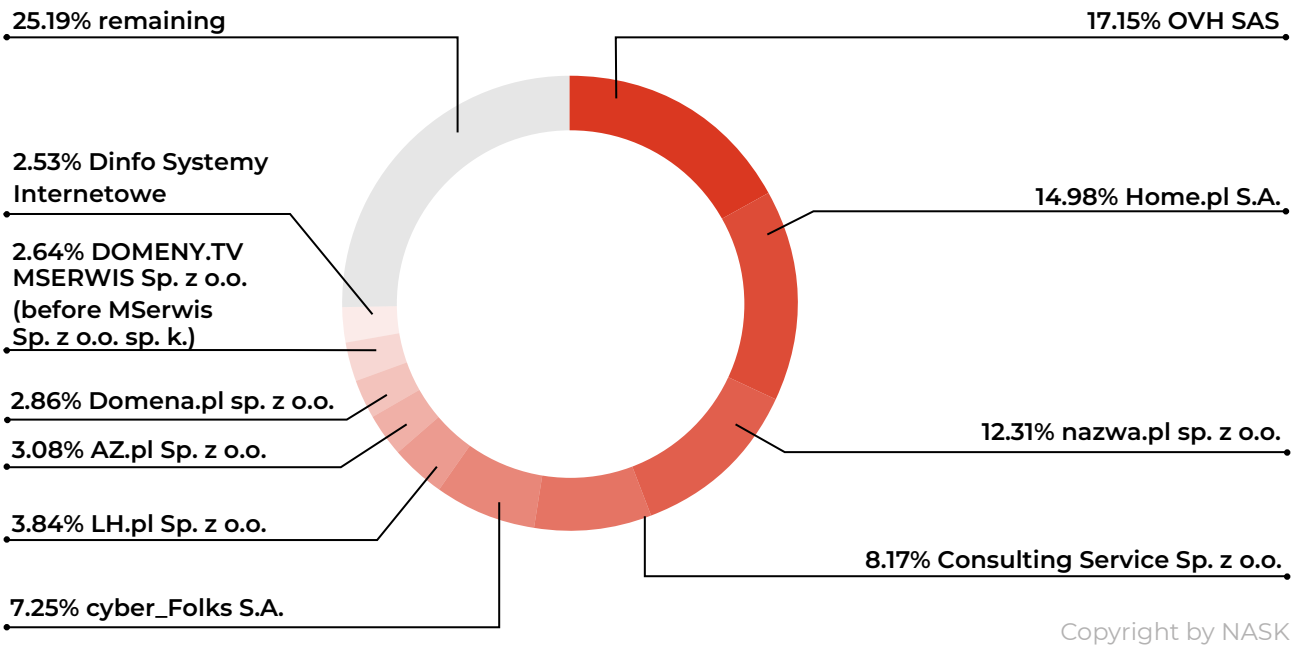
Despite these challenges, I can confirm that we are pleased with our results, and we are encouraged that our solutions continue to attract a growing number of customers. We are prepared for further growth and to tackle additional challenges to fulfill our mission of ensuring continuity of service for our clients on the Internet.

Division of the .pl domain name market

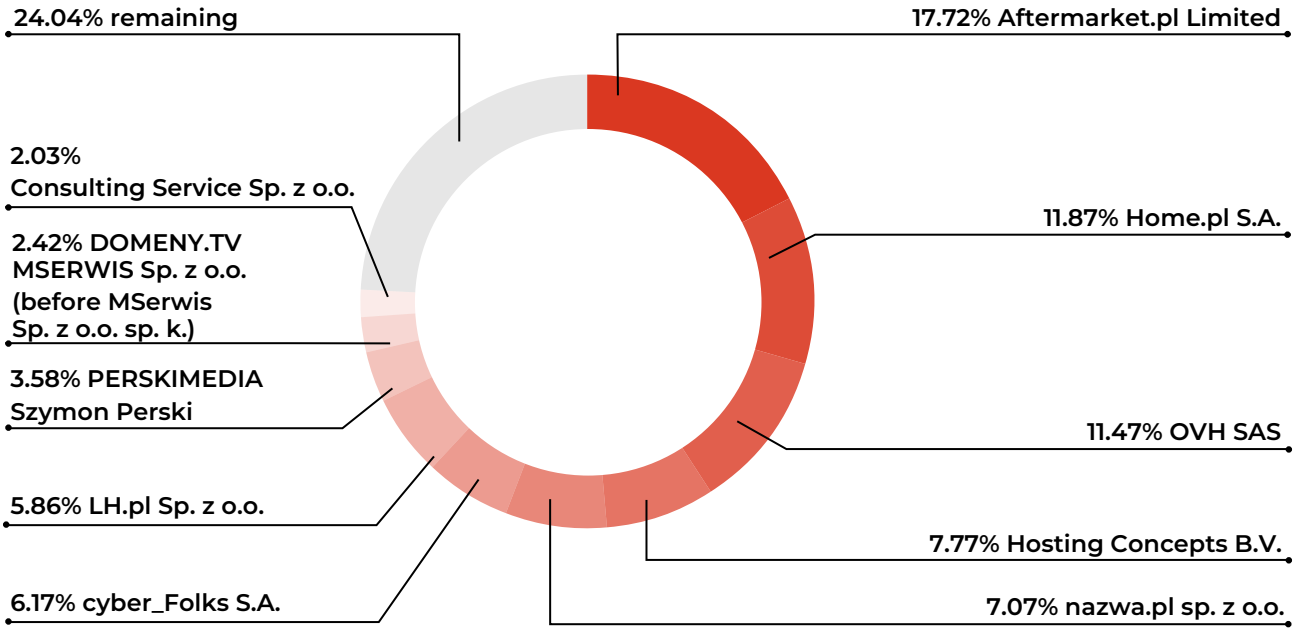
Partner's market share in the service of .pl domain names, 2023



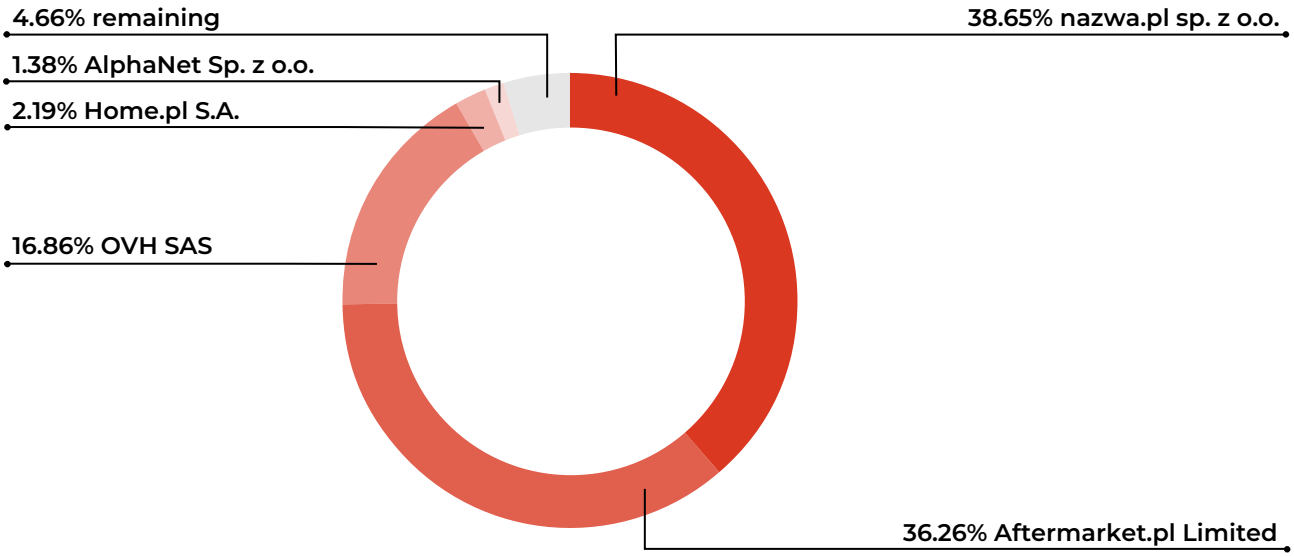
Partner's market share in the service of registrants of .pl domain names, 2023



Partner's market share in .pl domain name registrations, 2023



Partner's market share in servicing DNSSEC-secured .pl domain names, 2023



PART II

The Internet through the eyes of DNS industry experts

Information about the study

We present to you the first expert survey conducted. We asked registrars—our business partners collaborating with NASK-PIB within the Partnership Program—for their opinions on the Internet in five key areas (Popularity of e-services, Threats on the Internet, Hate on the Internet, Digital security of customers, and Online market and promotion). The goal was to understand the views of experts dealing with the Internet regarding Poland's technological development, Internet usage, network threats, and how the Internet aids in running businesses. Fifteen entrepreneurs participated in the study. The selection of representatives from this industry was deliberate due to the expert nature of the survey. The results will allow for future comparisons of the acquired knowledge and expert opinions with those of a representative group of Polish Internet users. In subsequent editions of the report, we plan to present the results of a quantitative study on Poles. Meanwhile, we hope that our first expert survey will provide you with interesting information. We warmly encourage you to read it!

STUDY METHODOLOGY Online surveys (CAWI) conducted on business partners (registrars) of NASK-PIB.	**SURVEY DURATION:** 20 minutes
	STUDY CONDUCTED: 17.01–29.02.2024

Survey Questions

1. Which e-service was used most frequently in Poland over the past 12 months?
2. Which forms of e-identification were used most frequently when accessing online services?
3. How is Poland assessed in terms of the development and implementation of e-services in the public sector compared to other European Union countries?
4. Which of the current threats associated with technological development provoke the greatest concerns?
5. Which internet browser is used most frequently?
6. How often do you encounter online aggression or negative/offensive comments on the internet?
7. What form of aggression on the Internet is most prevalent and what are its motivations?
8. How are e-services most commonly secured in Poland?
9. What data do registrars use to verify customer information?
10. What forms of advertising and promotion are most commonly used on the internet in the domain industry?

Study Conclusions

1. Online banking, online shopping, and digital communication are key areas where technology is gaining significance in everyday life.
2. For e-identification, the most frequently used methods are trusted profiles, ePUAP (electronic Platform of Public Administration Services), and the mObywatel mobile application.
3. Poland received a positive assessment in terms of the development and implementation of e-services in the public sector compared to other European Union countries.
4. The most dominant e-services in public administration are: podatki.gov.pl and ePUAP.
5. Digital identity theft and misinformation/disinformation are currently key threats in cyberspace.
6. Aggression is present in various areas of the Internet, but most notably in social media.
7. The most common source of online conflicts is political issues.
8. Companies use various communication strategies to educate their customers about online threats.
9. Phishing is becoming a real threat to businesses.
10. Among the most commonly used promotions are discounts on registrations and affiliate programs.

Popularity of e-services

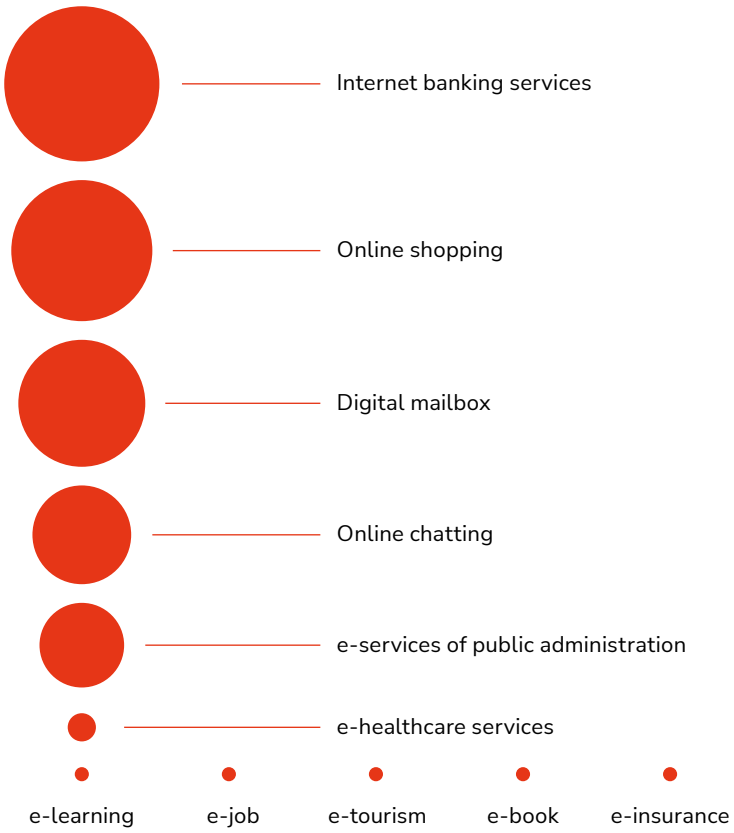
What do we need the Internet for?

The most frequently chosen service was online banking (11 out of 15 responses), suggesting that using online banking platforms has become an integral part of everyday life. Nearly as popular are online shopping (10 responses), confirming a growing trend towards preferring the convenience of online shopping.

Digital mailboxes (9 responses) and online communication (chats, messengers, etc. - 7 responses) remain consistently popular.

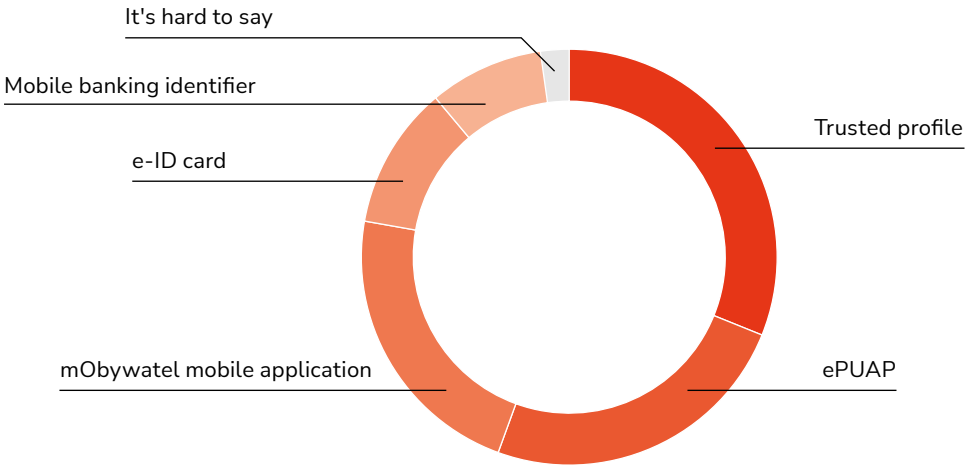
Our surveyed experts also show interest in using e-services for public administration (6 responses), but are less inclined towards e-care/healthcare services (2 responses). E-learning/e-learning services and online job search also did not attract much interest among the respondents.

Which of the following e-services do you think was most commonly used in Poland in the last 12 months?



During the use of e-services, respondents preferentially use various forms of e-identification. The most popular among them are trusted profiles (14 responses), ePUAP (11), and the mObywatel mobile application (10). Some use the less popular e-ID card (5) and mobile banking identifiers (4).

Have you used any of the following e-identifications in the past 12 months while using online services?



The practical use of e-identification is accompanied by a positive assessment of Poland regarding the development and implementation of e-services in the public sector, compared to other EU countries. Eight out of fifteen experts surveyed believe that Poland's situation is better or significantly better than that of other EU countries. Moreover, none of the respondents think that Poland is developing worse than other European countries, while two rate its development at the same level as other compared countries. A relatively large group (five respondents) was unable to take a position on this matter. Respondents particularly highlighted public administration e-services, such as podatki.gov.pl and ePUAP, as those that most prominently surpass other EU countries in development (seven responses). Online banking services (five responses) rank second, once again confirming the growing popularity of online banking in Poland. In comparison to other EU countries, Poland's development is rated lower in areas such as e-commerce, e-care services (including e-prescriptions), e-tourism (one response), and e-services related to education, work, communication, e-books, insurance, and culture (zero responses).

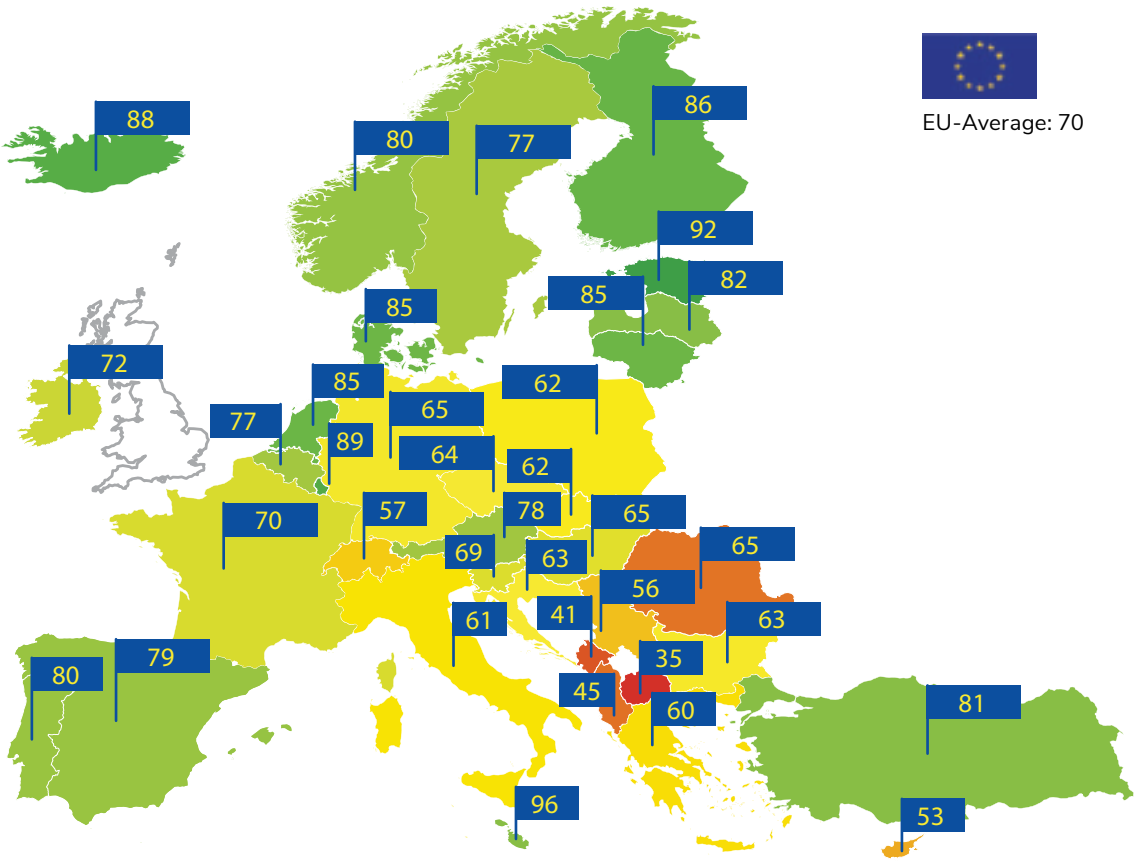
Online banking, online shopping, and digital communication are key areas where technology is gaining significance in everyday life, which may be a result of both the conveniences available to customers and digital trends. Preferring online shopping indicates trust in e-commerce platforms and the ease of making transactions over the Internet. Undoubtedly, the popularity of this e-service was also influenced by

the SARS-CoV-2 pandemic. It may be surprising that despite the changes in the healthcare sector following the pandemic, interest among the surveyed group in using e-healthcare services is very low. There is also a lack of interest in e-learning and online job searching, probably because these individuals already have stable careers and defined education levels. A lack of interest was also evident in e-books, e-insurance, e-tourism, and e-culture. Interestingly, none of the respondents stated that they do not use any form of e-identification. This may indicate a growing awareness and acceptance of the necessity of using such solutions, particularly in this specific environment, which also influences the choice of a particular form of identification by users.

The positive assessment of Poland in terms of the development and implementation of e-services in the public sector compared to other EU countries, according to the experts we surveyed, may suggest that Poland has focused on developing digital public services, which seems to be recognized by the respondents. The respondents rate government actions in this area positively, and there is considerable interest and activity among them in using online services provided by public institutions.

According to a study conducted by the European Commission, the level of e-service development in Poland is below the EU average.

Level of e-service development in the European Union



Source: European Comission, eGovernment Benchmark 2023 Insight Report. Connecting Digital Governments, European Union, 2023, p. 6.

The level of development in individual countries was assessed based on the study of four dimensions:

- user orientation (At what level are online services provided? How friendly are they to mobile devices? What online support and feedback mechanisms are available?)
- transparency (Do public administrations provide clear, openly communicated information about how they deliver their services? Are they transparent in the creation of policies and processes for designing digital services, as well as in how they handle users' personal data?)
- key facilities (What technological facilities are available for providing eGovernment services?)
- cross-border services (How easy is it for citizens from abroad to access and use online services? What online support and feedback mechanisms are available for cross-border users?).

The obtained score ranges from 0 to 100 points.

EXPERT COMMENTARY

Digitization of services in Poland, despite a relatively low level compared to other European countries, is continuously improving. The dynamics of these changes provide hope that within the next few years, the level of service digitization will be comparable to other EU countries.

Significant role in accelerating this process was played by the COVID-19 pandemic and the increasing social accessibility to the Internet. In comparison to 2015, in 2022, 870 out of 1,000 residents in Poland were Internet users (in 2015, only 680). Regarding the number of mobile phone registrants per 1,000 residents, Poland ranks fourth in Europe (after Estonia, Lithuania, and Italy). Japan leads in this regard with 1,675 mobile phone registrants per 1,000 residents, while in Poland, this indicator stands at 1,320 [International Statistics Yearbook, 2023, Central Statistical Office (GUS), Warsaw 2023].

Access to the Internet, including broadband connections, means that Poles are more likely to use online banking, make online purchases, and utilize various internet communication systems. The willingness to handle matters online also contributes to the increasing use of various e-identifications, ensuring a sense of security.

Prof. Joanna Ejdys, PhD

BIALYSTOK UNIVERSITY OF TECHNOLOGY, FACULTY OF MANAGEMENT ENGINEERING

e-puap

e-rozmowy

e-biznes

e-opieka

e-commerce

e-mail

e-ubezpieczenia

e-book

e-kultura

e-bankowość

e-dowód osobisty

e-biznes

e-identyfikacja

e-administracja

e-turystyka

e-płatności

e-consulting

e-recepty

e-usługa

e-learning

Threats on the Internet

What do we fear the most?

Cybersecurity threats are another area in which we wanted to gather our experts' opinions. Analyzing the research results concerning fears related to various threats, several significant trends can be distinguished:

- **HIGH AWARENESS OF DISINFORMATION** (11 indications). Concerns related to disinformation point to an increasing understanding of the crucial role that cyberspace plays in manipulating information.

- **ISSUES RELATED TO INTERNET ACCESS** also raise concerns among the respondents (9). This is understandable, as many aspects of daily life, both private and professional, depend on access to the network.

- **THREATS OF CYBERATTACKS AND ATTACKS ON CRITICAL INFRASTRUCTURE**. Concerns related to cyberattacks on Poland and the shutdown of essential infrastructure systems (6) align with the global trend of increasing cybercriminal and cyberwarfare activity.

- **THEFT OF PERSONAL DATA**. Concerns related to the theft of personal data (6) highlight that privacy protection remains a continuously important aspect of cybersecurity.

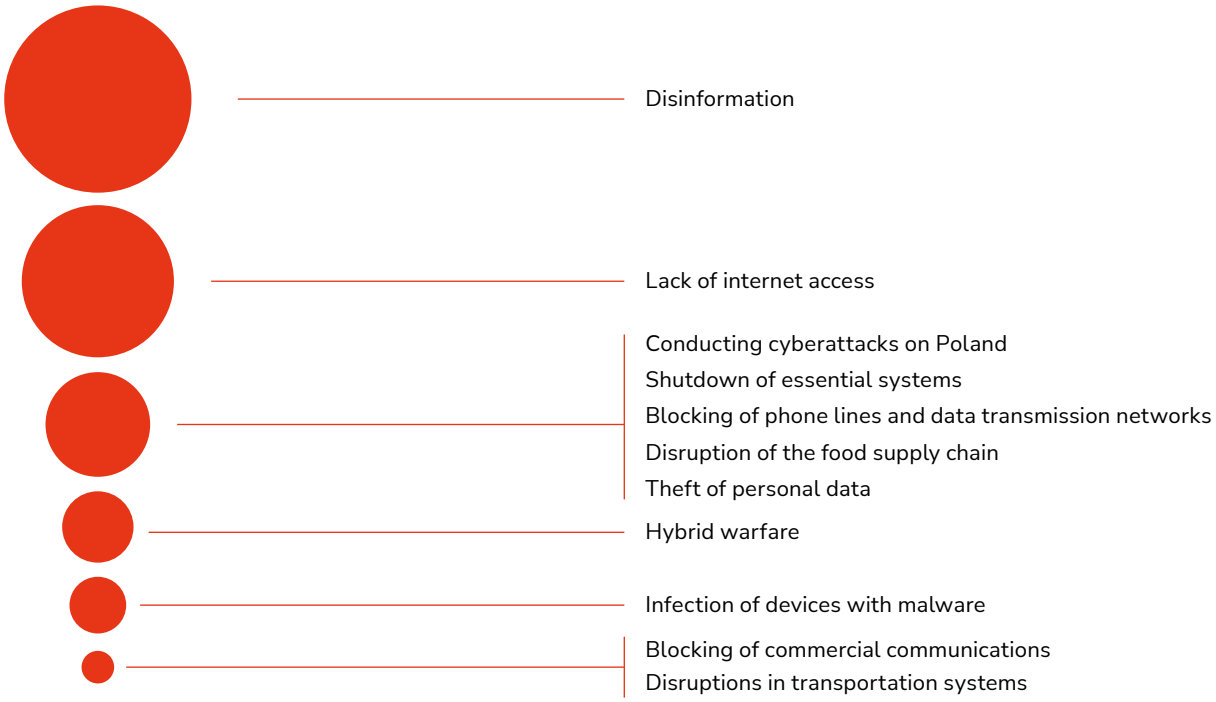
- **DISRUPTION OF THE SUPPLY CHAIN AND HYBRID WARFARE**. Concerns related to the disruption of the food supply chain (6) and the threat of hybrid warfare (4) emphasize that cybersecurity is closely linked to national security and the global supply chain.

- **INFECTION OF DEVICES WITH MALWARE** (3). This threat raises less concern among respondents, as they likely know how to defend against it.

The least concern is raised by the blocking of commercial communications, disruptions in the functioning of transportation such as trains, airplanes, buses, or actions by third countries against the nation (1). None of the respondents indicated the blocking of banking transmission networks or the stock and bond markets as a potential cybersecurity threat.

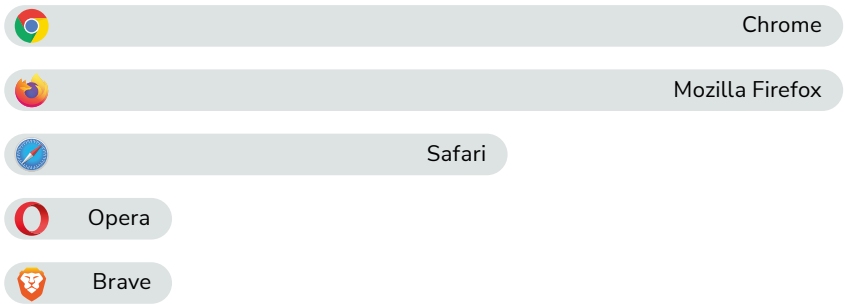
At the same time, respondents indicate that **digital identity theft** is currently one of the key threats (14 indications). This confirms the growing public awareness of the serious consequences that can result from losing digital identity. None of the respondents answered „No" or „Definitely not".

Which of the following threats do you fear the most?



We also asked our respondents which browser they use most frequently. Chrome and Mozilla Firefox are tied for first place (5 indications each), followed by Safari, mainly used by Apple system users (3 indications), and in third place, Opera and Brave (1 indication each). It is worth noting that none of the respondents indicated Microsoft Edge or Tor as their most frequently used browser.

Which browser do you use most frequently?



In the context of global cybersecurity, survey results provide a comprehensive view of various threat aspects. The increasing awareness regarding disinformation, cyberattacks, and critical infrastructure security underscores the need for global cooperation and continuous adaptation of strategies to effectively counter evolving threats in cyberspace. As technological advancements progress and the number of internet platforms grows, combating disinformation becomes a crucial challenge for global cybersecurity.

Recent studies conducted by the Digital Poland Foundation and the fact-checking organization Demagog titled „Disinformation through the Eyes of Poles (Warsaw, 2024)" confirm that the level of disinformation in Poland remains very high.

Network security has become a fundamental aspect of maintaining the stability and integrity of society, with the security of critical infrastructure such as energy, water, and heat supplies emerging as an international priority. Many aspects of daily life, both private and professional, depend on access to the internet. Additionally, internet access is not only a convenience but also a crucial tool for communication, education, and accessing information. Privacy protection in cyberspace is also a significant concern. Digital identity theft is currently one of the key threats, highlighting society's growing awareness of the serious consequences of identity loss. Safeguarding online identities has become a priority, and efforts to improve cybersecurity and education in this area are crucial for society.

EXPERT COMMENTARY

Research on the opinions of experts from the Domain Division of NASK, conducted within 15 firms regarding network threats, presents another insightful perspective on current trends in this area. The results clearly indicate that experts are aware of specific threats posed by networks (it would be highly concerning if they were not). Of particular interest is the prioritization of these threats. Experts' concerns primarily revolve around disinformation (which has received much attention recently due to the COVID-19 pandemic and conflicts beyond the eastern border), followed by concerns about lack of internet access, and then equally concerning shutdown of critical systems (electricity, gas, heat, blocking of phone lines and data transmission). Disruption of the food supply chain and theft of personal data also raise significant concerns. Interestingly, none of the respondents indicated concerns about the blocking of banking transmission networks or the stock and bond market operations.

However, digital identity theft is clearly perceived as a key threat. Because that's what it truly is. Among the most commonly used browsers indicated by respondents were Chrome, Mozilla Firefox, followed by Safari (for Mac users), with one person choosing Opera, while Tor and Microsoft Edge were not chosen by any respondents. These are very interesting studies and their results. I recommend reading the entire report. It would be worthwhile to conduct similar studies among a broader group of non-expert users (with specifications on basic demographic data such as age, gender, education, profession, role within institutions or companies, etc.) and compare their responses with those of experts. Based on this, recommendations can be formulated regarding existing deficits and the implementation of necessary mechanisms and educational programs to mitigate these deficits, ultimately leading to informed, responsible, and safe internet usage.

Assoc. Prof. Barbara Wiśniewska-Paź, PhD

DIRECTOR OF THE CENTER FOR SECURITY STUDIES AND EDUCATION AT THE UNIVERSITY OF WROCŁAW

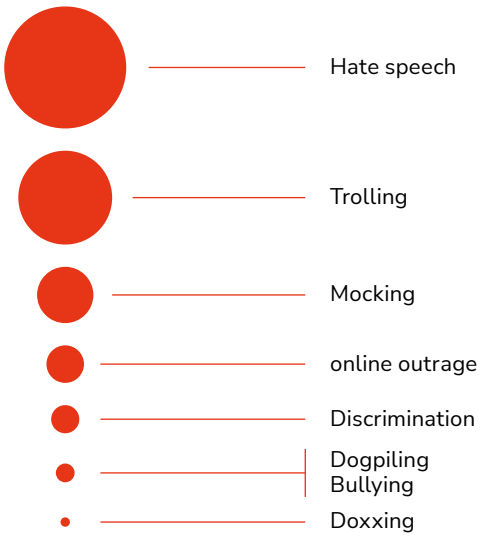
Hate on the Internet

Aggression as a phenomenon in the network

Our respondents rarely experience aggression on the Internet. Only 4 respondents reported experiencing it in the last 12 months, and 1 person was unsure whether they had encountered aggression or not. Similarly, when it comes to aggression directed towards companies on the Internet, only 2 experts responded affirmatively, while 3 had difficulty identifying whether behavior directed towards the company was aggression or not, indicating uncertainty in identifying or monitoring potential negative online situations. However, a total of 13 respondents confirmed that in the past 12 months, they had seen someone else become a victim of aggression on the Internet or write something negative or offensive online. Only 1 person responded negatively to this question, and 1 had difficulty properly identifying the observed behavior.

Most frequently, it was aggression related to hate speech - 13 indications, trolling (provoking conflicts, disinformation) - 10, and mocking - 6. Slightly fewer people observed online outrage - 4, discrimination (based on race, religion, sexual orientation, or others) - 3, bullying and dogpiling - 2, and doxxing - 1.

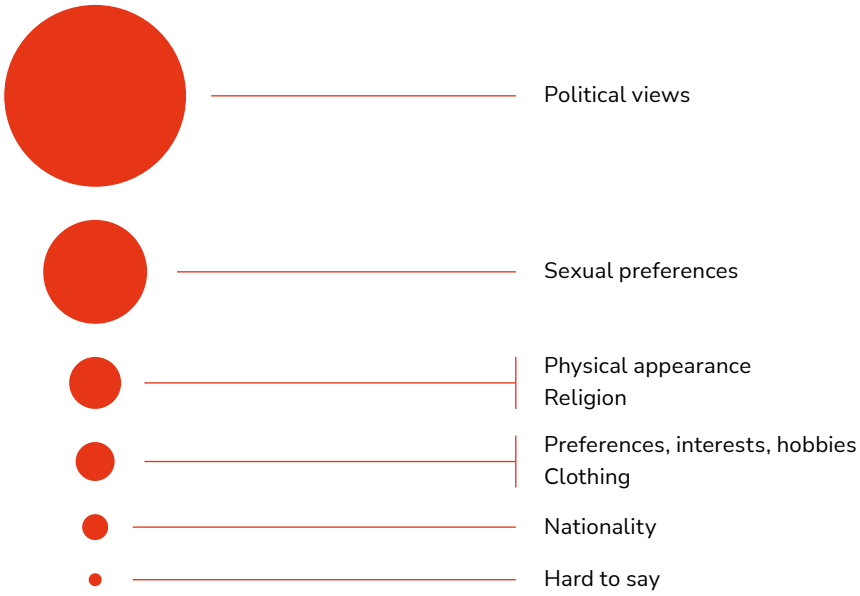
What type of aggression on the Internet do you think is the most common?



As the cause of aggression, the respondents identified political views (14 out of 15). Slightly fewer mentions (8) were related to sexual preferences, while physical appearance and religious beliefs had 4 mentions. This underscores the diversity of areas where online aggression occurs. Occasionally, cited reasons

also include preferences, interests, hobbies, nationality (3), or style of dress (2). Interestingly, there were no mentions regarding gender or skin color, which may indicate progress in social awareness and acceptance of differences in these areas.

What do you think is the most common reason for aggression on the Internet?



According to the respondents, the most frequent aggression on the Internet occurs on social media platforms such as Facebook, Instagram, and YouTube (12 mentions), on news portals like Onet, WP, and Interia (4), on messaging apps like Messenger and WhatsApp (2), in online games, and in comments under news articles on news portals (1). According to our respondents, aggression is most commonly encountered on platforms such as Facebook - 9 responses, X (Twitter) - 5, YouTube - 4, Instagram, TikTok, and Wykop.pl - 2, and Twitch - 1.

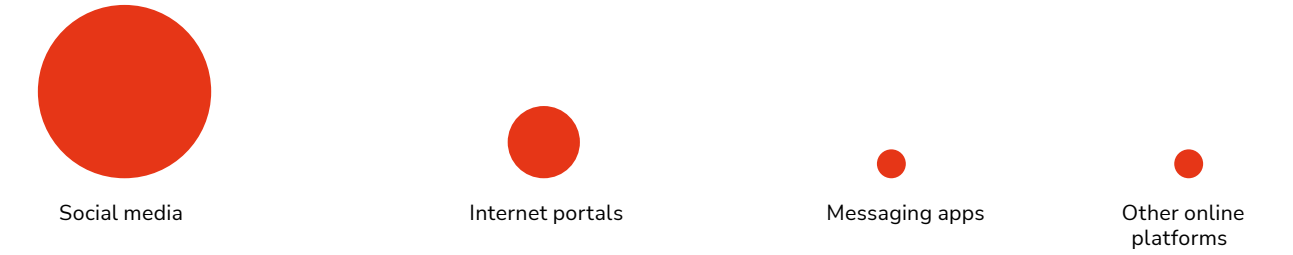
Among messaging apps, Messenger from Facebook was most frequently mentioned (2 responses), followed by Skype, Discord, Telegram, and Teams (1 response each). This lower number of mentions may be due to the lesser public exposure of private communications compared to interactions on social media.

Similarly with internet portals, the maximum number of mentions among respondents was 1 and included portals such as Onet.pl, TVN24.pl, Gazeta.pl, Pudelek.pl, Plotek.pl, TVP.pl. Although there are differences in preferences evident here, as respondents mentioned various news and entertainment portals, the number of mentions is low.

At the same time, only 6 out of the experts surveyed do not refrain from expressing their opinions online due to fear of becoming victims of digital aggression. 5 individuals refrain from commenting on social media posts of people they do not know, 4 are concerned about posting their own content on social media,

3 avoid commenting on posts in social media groups, and 2 refrain from commenting on posts from acquaintances on social media and do not comment on articles/news on social media platforms.

Where on the Internet have you noticed someone else becoming a victim of online aggression?



In which social media platforms have you most frequently witnessed someone else becoming a victim of aggression?

- Facebook
- Twitter (X)
- Youtube
- Instagram
- TikTok
- wykop.pl
- Twitch

In which messaging apps have you most frequently witnessed someone else becoming a victim of aggression?

- Messenger
- Skype
- Discord
- Telegram
- Teams

On which internet portals have you most frequently witnessed someone else becoming a victim of aggression?

It can be assumed that aggression is present in various online media, but at the same time, it may not be a common phenomenon in respondents' experiences. It is worth emphasizing that these results may be subjective and depend on the individual experiences of respondents, as well as on which platforms are popular within a specific social group.

The respondents exhibit a considerable caution towards strangers, which may stem from concerns about potential negative reactions or aggression from unknown users. Similarly, this caution extends to groups within social media. It's interesting to note the observation regarding refraining from commenting on posts from acquaintances on social media, suggesting that even among people known personally, there exists a certain apprehension about potential aggression in response to expressing opinions.

Companies may have limited visibility in this area or difficulties in tracking online communications. Most companies reported no negative experiences, which may indicate that the majority maintain a positive reputation in cyberspace ew and do not experience public attacks or negative comments. The results confirm the thesis that political issues are often a source of online conflicts, highlighting the long-standing and widely discussed societal polarization in this area.

The dominance of Facebook as a platform where respondents observed online aggression may indicate that this largest social network is particularly susceptible to negative interactions. This thesis is supported by the fact that Twitter and YouTube, also known for their wide reach, follow closely in the rankings.

EXPERT COMMENTARY

The current development of technology is increasingly displacing the real world with the virtual world. People are transferring more and more of their activities to the Internet. Therefore, researching social life conducted in the virtual world is important. Preliminary expert studies on HATE in the Internet, especially AGGRESSION as a phenomenon in the network, indicate that fear of unjustified negative reactions from Internet users does not block the presentation of their views in only 33% of respondents. The remaining 67% have doubts and probably limit themselves in their statements.

Therefore, it can be assumed that a large group of Internet users actually refrain from participating in public discussions out of fear of aggression from others - they are excluded from actively participating in social life on the Internet. It would be worthwhile to investigate precisely which group of Internet users this is and what they need in order not to be marginalized.

Aggression, according to experts, is mainly manifested on social forums and internet platforms. This suggests that the tools used so far to eliminate hate and aggression are ineffective. It is necessary to seek new solutions that protect freedom of speech and allow those currently excluded by others' aggression to participate in discussions and social life happening online.

Assoc. Prof. Bohdan Rożnowski, PhD
The Catholic University of Lublin John Paul II, Department of Work Psychology, Institute of Psychology

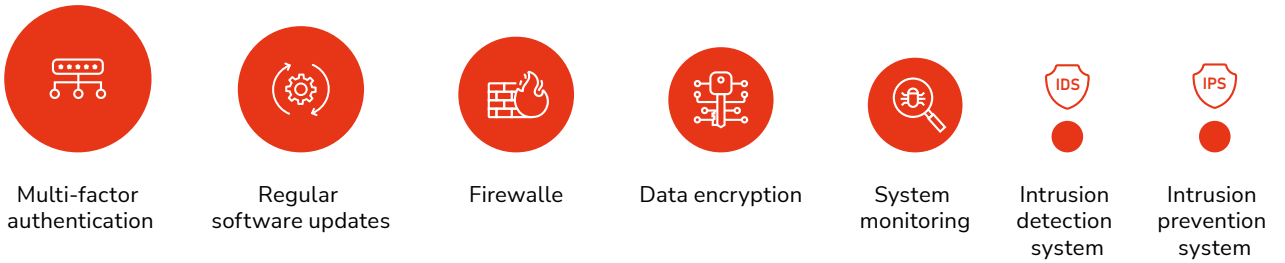
trolling
wyśmiewanie
race
osaczanie
stalking
dezinformacja
dręczenie
hate
dyskryminacja
doxxing
mocking
hate speech
szczucie
cyberbulling
dogpiling
mowa nienawiści
fake news
bullying
trole internetowe
discrimination
on-line outrage
religion
nękanie
disinformation

Digital security of clients

The most popular safeguards for e-services

We asked respondents whether they conduct **risk analysis** concerning the security of digital services to ensure the safety of their clients. Most (10) confirmed that their company conducts risk analysis specifically related to the security of digital services. In 3 companies, such analysis is not conducted, and 2 had difficulty providing an answer to this question. This area requires attention because the absence of such analysis can expose the company to security threats concerning the services provided or processed data, as well as to negative regulatory consequences (e.g., administrative penalties). The survey results on **e-service security measures** show that respondents are taking various conscious steps to minimize risks in cyber security. The most popular measures include multi-factor authentication (14 mentions), regular software updates (12), firewalls (11), data encryption (10), and system monitoring (9). Some of the surveyed firms also utilize Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) (3).

How do you most often secure your e-services?

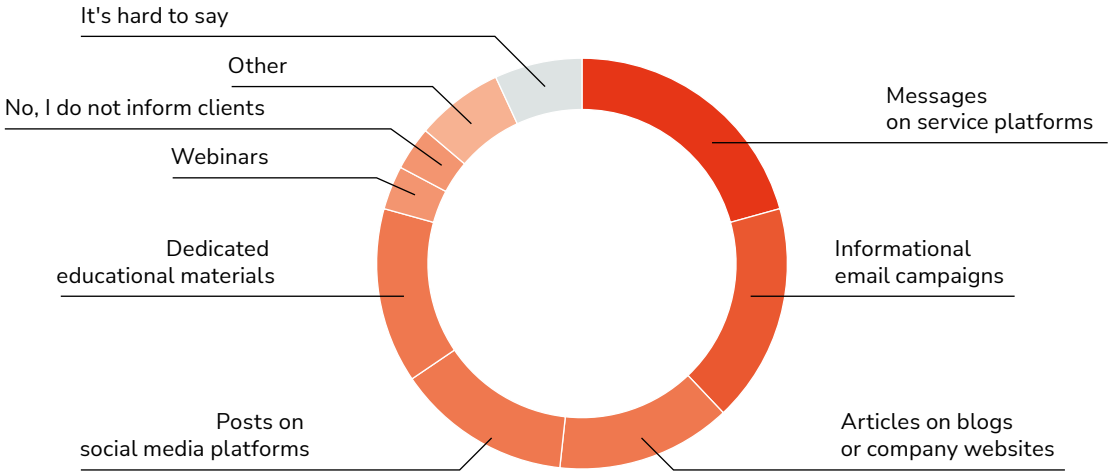


At the same time, the majority of respondents (11 responses) do not keep **statistics on violations of regulations regarding the illegal nature of content**. Only 3 companies collect such statistics (1 had a problem answering this question) This may indicate that most respondents do not provide hosting or other services that allow end customers to share content. 6 out of 15 surveyed companies confirmed that their services were subjected to **phishing attacks**.It indicates a certain level of experience and awareness among the respondents regarding cybersecurity, and underscores the real risk and occurrence of such attacks.

7 experts declared that their services were not subjected to phishing attacks, while 2 had difficulty responding to this question. Regarding efforts to raise awareness in cybersecurity, 9 out of 15 firms stated that they inform clients about online threats, 4 do not engage in such activities, and 2 were unsure how

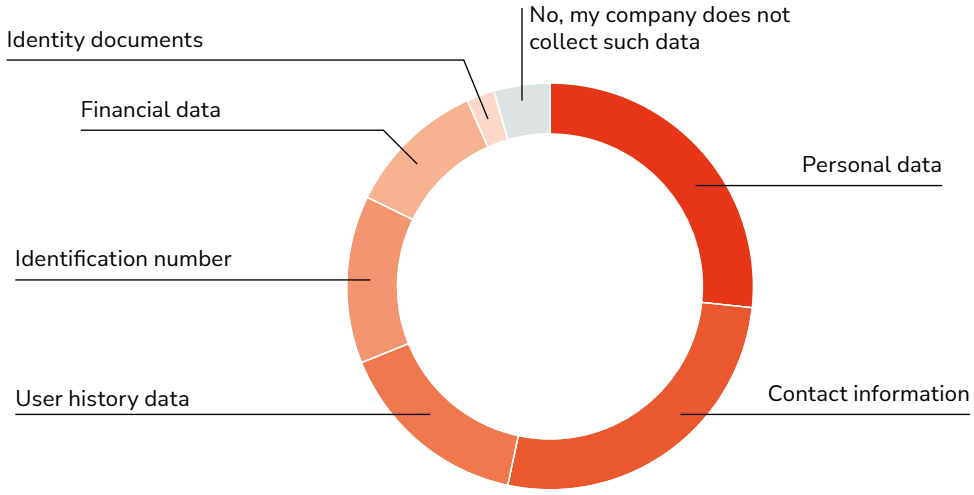
to respond to this question. Among these nine firms, the most common methods of informing include messages on service platforms (6 responses), informational email campaigns (5 responses), articles on blogs or company websites (4 responses), and posts on social media platforms (4 responses). Less frequently used methods include educational materials and webinars, client discussions, and directly pointing out threats and methods to counteract them, often during phone conversations (1 response each).

Do you inform clients about online threats?



Those results indicate that companies employ diverse communication strategies to educate their customers about online threats. However, there is potential for further development in customer education, especially in the context of the rapidly changing cybersecurity landscape. Out of the 13 companies we surveyed, 2 do not collect data for customer verification. The most commonly collected types of data are personal and contact information such as phone numbers and email addresses (12 responses), user history data like purchase history and account logins (7), identification numbers such as national identification numbers or other unique government-issued identifiers (6), and financial data such as bank account numbers or credit/debit cards (5). The least common method is the scan or photo of identity documents (1), which can be used for more detailed identity verification, but processing it has been repeatedly pointed out by the Personal Data Protection Office as excessive. It's worth noting that only one company declared collecting date of birth.

Does your company collect data for customer information verification purposes?



EXPERT COMMENTARY

First and foremost, it is worth appreciating the fact that such a survey was conducted by NASK among its partners. The significant increase in the scale of threats in the area of digital services and the changes in the regulatory environment (Digital Services Act, NIS2, DORA, CER, and AI ACT), which we are currently in the midst of, present an excellent opportunity to capture the state of knowledge and practices of entrepreneurs responsible for such a crucial element of the digital economy as the process of registering and maintaining an internet domain.

In the area of applied security measures, the results show that multi-step (but is it multi-factor?) authentication has become a standard for authorization, which should be viewed very positively, considering the state of the market 3–4 years ago. Software updates, the use of firewalls, data encryption, and even system monitoring are also encouraging and may indicate that the surveyed entrepreneurs either certify their operational activities or could prepare to do so. It seems that this thesis is supported by the fact that 10 out of 15 conduct risk analyses related to the security of provided digital services. Of course, the devil is in the details as always, and it would be worthwhile to delve deeper into this topic in subsequent editions of the study. The upcoming implementation of the NIS2 Directive will provide a good pretext for this, although its literal reading does not seem to encompass the registration service of internet domains itself (although the DNS maintenance service certainly falls under NIS2).

The responses to the question about „statistics on violations of regulations regarding illegal content" indicate, in my opinion, that either the majority of respondents do not provide hosting services (which from the perspective of domain registration services may not be necessary), or they did not recognize that the survey pertained to such services.

It is worth noting at this point that hosting providers (but not domain registration intermediaries) have been required since the beginning of this year to comply with the European Digital Services Act (Regulation of the European

Parliament and of the Council (EU) 2022/2065), which introduces significantly greater responsibility than in previous years for content provided through hosting services or digital platforms.

I also positively assess the survey results regarding the data collected by providers for verifying customer information.

The results indicate, in my opinion, that the majority of respondents limit this data to the minimum necessary for identifying and handling business-related aspects of domain registration services. An exception includes data that could be considered excessive, such as images or date of birth.

Mariusz Busiło

PARTNER AT BĄCAL BUSIŁO SP. K.,

MEMBER OF THE POLISH CHAMBER OF INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

vishing
szyfrowanie
IPS
encryption
software
analysis
ryzyko
oprogramowanie
system
IDs
security
authentication
antywirus
risk
firewall
monitoring
uwierzytelnianie
phishing
spoofing
monitoring
update
aktualizacja

Market and online promotion

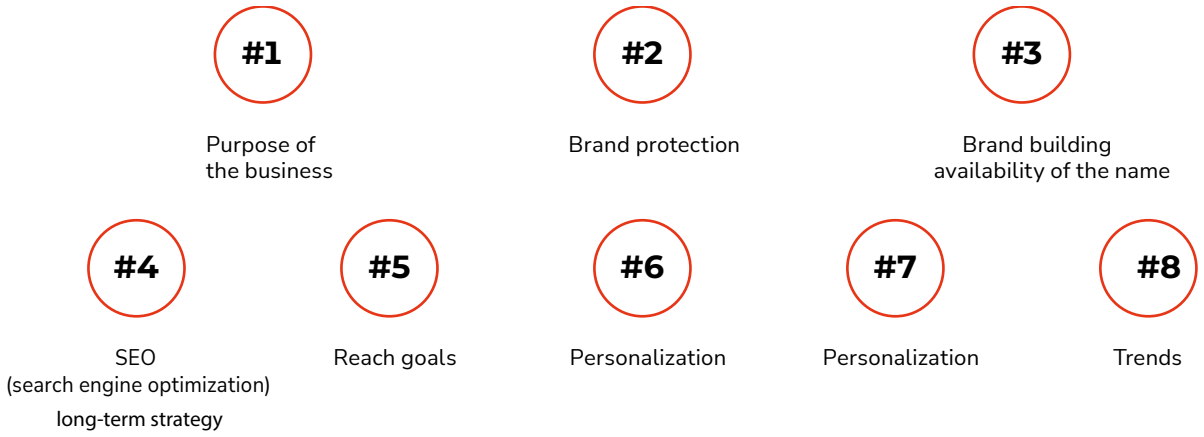
How to Advertise on the Internet – An Overview of Practices with Selected Examples

A survey shows that 11 out of the 15 companies we studied use some form of internet advertising or other forms of online promotion. The most common are social media ads (9 mentions), search engine marketing (SEM) (7), email marketing campaigns (6), content marketing (e.g., sponsored articles, e-books, videos) (5). Less frequently used are display ads (e.g., banners, pop-ups) (3), video ads (e.g., short commercials, instructional videos, promotional content), mobile ads (e.g., in mobile apps), interactive or native ads (2), and internet forums (1).

What forms of internet advertising or other types of online promotion does your company use?

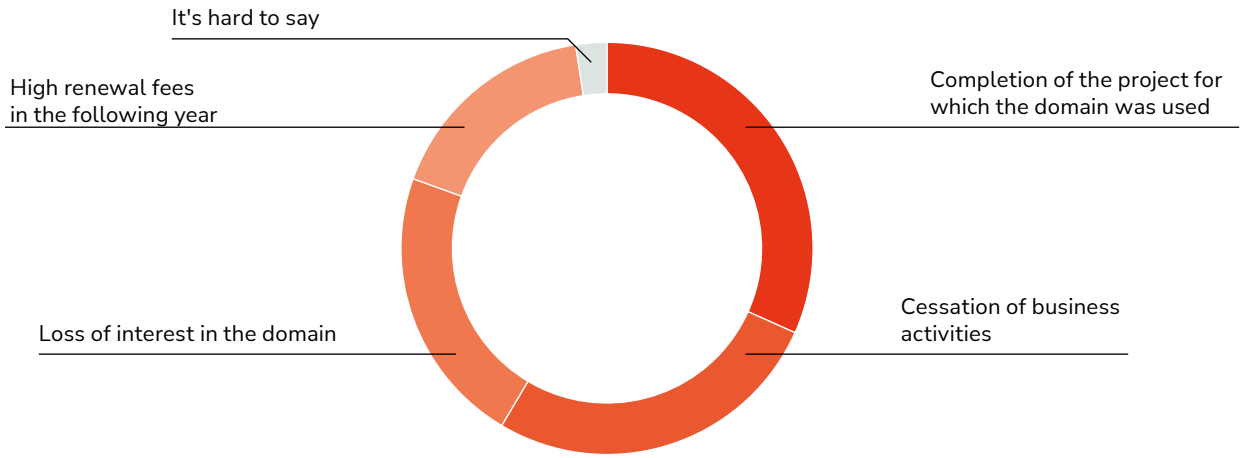
According to the experts we surveyed, there are several factors that influence clients' decisions to register new domains. The most important factors include the purpose of the business (new company, new project, etc.) – 12 mentions, brand protection – 11, brand building – 9, availability of the name – 9, SEO (search engine optimization), long-term strategy – 7, reach goals (regional, global) – 6, personalization – 4, and trends – 3. One company had difficulty answering this question.

What factors most frequently influence your clients' decisions to register new domains?



The companies surveyed often face the issue of clients not renewing their domains. The most common reasons cited are the completion of the project for which the domain was used (13), the cessation of business activities (11), loss of interest in the domain (9), and also high renewal fees in the following year (7). One company had difficulty answering this question.

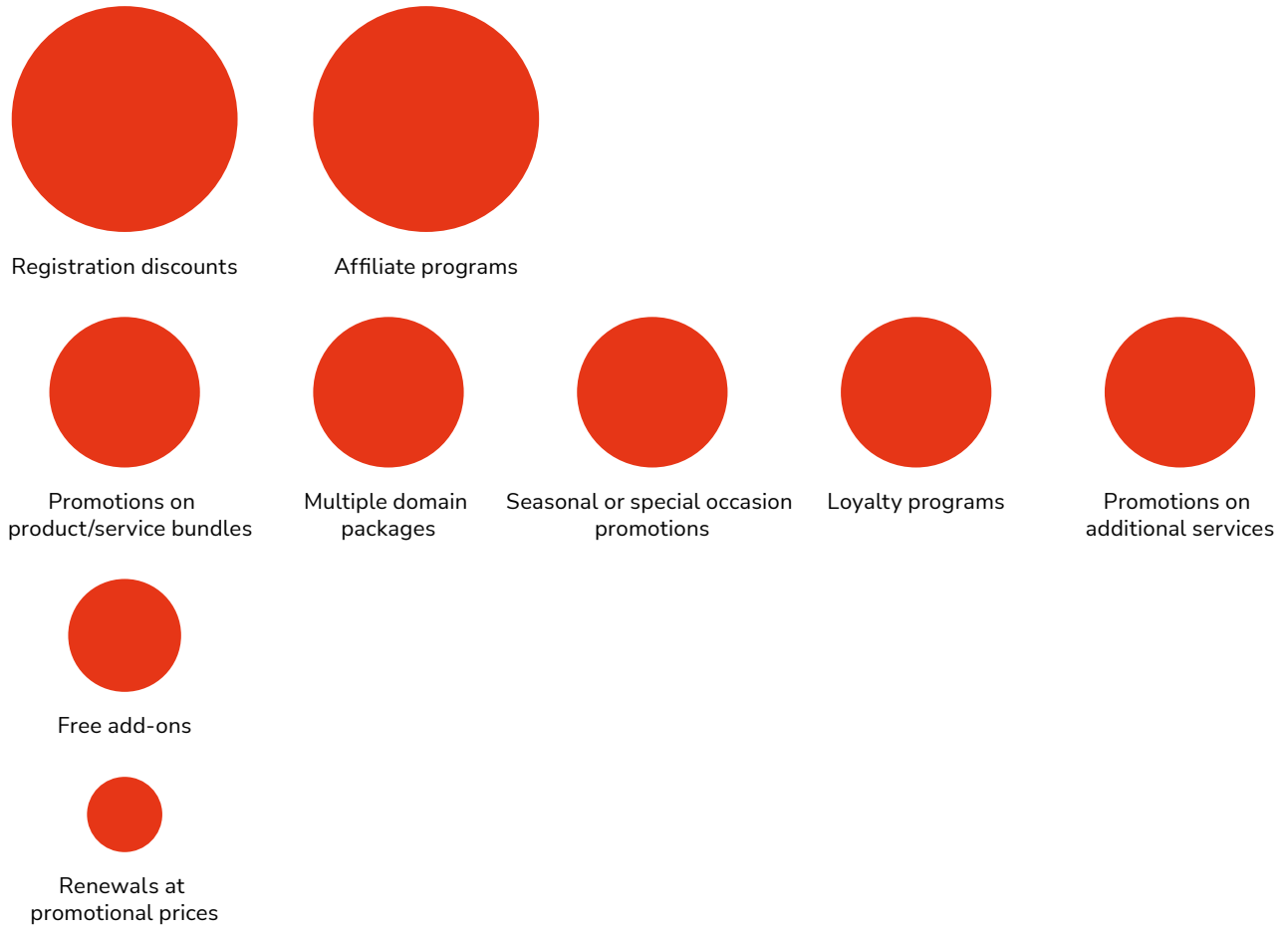
What do you consider to be the main reasons why registrants choose not to renew their domains?



To address the issue of domain non-renewal, some companies offer promotions to their clients. Nine out of the 15 companies we surveyed do this. However, the frequency is not high. Only 2 companies do this several times a month, 4 do it several times a year, and 3 do it once a year or less frequently.

The most commonly used promotions by the surveyed companies include discounts on registration and affiliate programs (6), promotions on product/service bundles, multiple domain packages, seasonal or special occasion promotions, loyalty programs, and promotions on additional services (4). Less frequently used are free add-ons (e.g., SSL certificates, email, WHOIS privacy protection) (3) and renewal at promotional prices (2).

What are these promotions?



EXPERT COMMENT

The above statements indicate that domestic companies use a set of the most effective tools for acquiring leads, commonly employed worldwide by B2B-focused entities. According to the June 2023 report by eMarketer, „The State of the Digital Marketing Channels and Tools," IT sector marketers identified the most effective sources and platforms as follows: SEO – 69.7%, content marketing – 50.6%, social media – 37.8%, referral marketing – 30.7%, and email marketing – 27.0%. Fewer mentions were given to display advertising (7.5%) and video advertising (6.2%). Thus, the expert sample from Poland largely reflects global observations. This hierarchy of touchpoints primarily arises from the nature of B2B marketing activities, including relatively more frequent (compared to consumer campaigns) performance-driven campaigns designed to generate desired interactions with both new and existing clients.

In the future, we can expect:

- an increasing role of social media, with a growing presence of younger decision-makers among B2B clients who were raised with social media. This will be accompanied by the continued significant engagement with SEM and SEO tools, which are efficiency pillars of many B2B activities,
- an increasing importance and investment in content marketing, which enables targeted and contextually relevant communication to selected, specific audiences within the B2B sector.

Paweł Orkwiszewski

CHIEF STRATEGY OFFICER, IPG MEDIABRANDS

Index of Terms

Related to Internet Advertising

SOCIAL MEDIA ADVERTISING – Utilizes the popularity of platforms such as Facebook, Instagram, and LinkedIn to reach a broad audience.

SEARCH ENGINE MARKETING (SEM) – Encompasses marketing activities conducted through search engines, including SEO (Search Engine Optimization) and paid links (PPC – Pay Per Click). These techniques influence each other; using sponsored links increases site traffic, which can positively impact the position in organic search results. This is particularly important for companies aiming to be visible in search results for specific keywords.

EMAIL MARKETING CAMPAIGNS – A form of direct marketing that uses email as a communication tool. It is one of the most cost-effective and efficient methods for reaching current and potential customers, with the goal of building and maintaining relationships and driving sales of offered services or products.

CONTENT MARKETING – A strategy focused on acquiring potential customers through the publication of appealing content tailored to a specific audience. As an alternative form of marketing, it aims to establish a relationship with the customer through engagement and interaction. This marketing concept is based on creating and delivering valuable and useful content in engaging formats (such as articles, guides, e-books, videos, podcasts, webinars, and more), thereby gaining the trust that is crucial in the sales process.

DISPLAY ADS – In the form of graphical banners or videos, are an online promotion method aimed at capturing users' attention on websites.

VIDEO ADS – Such as short commercials or instructional videos, are used by some companies to capture attention through dynamic video content.

MOBILE ADS – Including ads in mobile applications and native ads on mobile devices, are becoming increasingly popular due to the growing number of users accessing content on mobile devices.

Related to Factors Influencing Domain Registration

PURPOSE OF THE BUSINESS (NEW COMPANY, NEW PROJECT, ETC.) – The choice of a domain related to the company's purpose, a new company, or a project is one of the key factors for clients. They want the domain to reflect the nature and goals of their business.

BRAND PROTECTION – Introducing new domains as part of a brand protection strategy is important for clients who aim to safeguard their unique names against potential misuse.

BRAND BUILDING – Choosing a domain with the goal of brand building is crucial for clients who aim to effectively communicate their brand image and marketing message.

AVAILABILITY OF THE NAME – The availability of a chosen name is a crucial deciding factor. Clients may select domains that are easily accessible and not conflicting with others.

SEO (SEARCH ENGINE OPTIMISATION) – The process of optimizing a website or online store for search engines to attract as many visitors as possible from organic Google search results. SEO is important for clients who want to ensure their domains are easily discoverable in search results.

LONG-TERM STRATEGY – Domain decisions are often made in the context of a long-term business strategy. Clients consider the growth prospects and evolution of their company.

REACH GOALS (REGIONAL, GLOBAL) – Clients consider the scope of their business when choosing domains that best reflect their regional or global plans.

PERSONALIZATION – Customizing the domain name to better fit the specifics of the business or industry is an important aspect for some clients.

TRENDS – Some clients choose domains that reflect current trends in their industry or society.

Related to Promotion Forms

REGISTRATION DISCOUNTS – One of the most commonly used types of promotions. This is an attractive offer for clients who want to take advantage of reduced prices when registering new domains.

AFFILIATE PROGRAMS – Allow clients to earn benefits by referring the company's services to other potential clients. This is an effective way to expand reach and acquire new customers.

PROMOTIONS – Targeted at clients who use various offers from the company. These promotions encourage selecting a comprehensive range of services.

MULTI-DOMAIN PACKAGES – offers that include multi-domain packages are attractive to clients who need to register several domains at once. This can include different domain extensions or different names.

SEASONAL OR OCCASIONAL PROMOTIONS – sthese are tailored to specific periods, such as holidays or special days. They are a way to attract customers' attention during particular moments.

LOYALTY PROGRAMS – these reward long-term customers by offering additional benefits for their continued use of the company's services.

PROMOTIONS ON ADDITIONAL SERVICES – discounts on extra services serve as an incentive for customers who want to take advantage of the various features or options available in the company's offerings.

FREE ADD-ONS – (e.g., SSL certificates, email, WHOIS privacy protection) – offering free add-ons such as SSL certificates, email services, or WHOIS privacy protection can enhance the value of the primary services and attract more customers.

Bibliography

1. Baran P., *On Distributed Communications Networks*" in: *IEEE Transactions on Communications Systems*, vol. 12, no. 1, pp. 1–9, March 1964, doi: 10.1109/TCOM.1964.1088883.

2. Baran P., *Some changes in information technology affecting marketing in the year 2000*, The Rand Corporation 1968.

3. *Content marketing – koncepcja marketingu alternatywnego na przykładzie firm kurierskich*, [Content marketing – en alternative marketing concept on the example of courier companies], „Zeszyty Naukowe Politechniki Śląskiej" 2015, no. col. 1929, https://yadda.icm.edu.pl/baztech/element; access: 05.04.2024.

4. *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555; access: 05.04.2024.

5. *Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance)*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2557; access: 05.04.2024.

6. Emarketer, *The State of the Digital Marketing Channels and Tools*, 2023.

7. European Union, *European Comission, eGovernment Benchmark 2023 Insight Report. Connecting Digital Governments*, 2023.

8. Fundacja DigitalPoland, *Dezinformacja oczami Polaków [Disinformation Through the Eyes of Poles]*, Warszawa 2024.

9. *Funkcjonalność narzędzi Google w search engine marketingu, [The Functionality of Google Tools in Search Engine Marketing]*, „Studia i prace Wydziału Nauk Ekonomicznych i Zarządzania" no. 39, Vol. 2; 2015; US; https://wneiz.pl/nauka_wneiz/sip/sip39-2015; access: 05.04.2024.

10. GUS, *Rocznik Statystyki Międzynarodowej [Yearbook of International Statistics]*, Warszawa 2023.

11. *Rola e-mail marketingu w komunikacji z interesariuszami szkoły wyższej [The Role of Email Marketing in Communication with Higher Education Stakeholders],„Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach", no. 255, 2016*, https://cejsh.icm.edu.pl; access: 05.04.2024.

12. *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance)*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2065; access: 05.04.2024.

13. *REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*, https://eur-lex.europa.eu/legal-content/ENG/TXT/HTML/?uri=CELEX%3A32022R2554; access: 05.04.2024.

14. Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206; access: 05.04.2024.

15. Weibel P., *The Post-media Condition, in: AAVV*, Postmedia Condition, Centro Cultural Conde Duque, Madrid 2006.

About the report publisher

NASK is a state research institute supervised by the Ministry of Digital Affairs.

NASK-PIB currently engages in multifaceted activities, operating at the intersection of science and business. One of NASK's main activities is ensuring a secure Internet and protecting its users. **Cybersecurity and User Protection** – a key focus of NASK's activities is ensuring Internet security. The Cybersecurity Center, which includes the CERT Polska team (www.cert.pl), handles responses to events that compromise network security in Poland and coordinates activities in this area. According to the Act on the National Cybersecurity System, NASK-PIB has been designated as one of the Computer Security Incident Response Teams (CSIRTs) responsible for coordinating the handling of incidents reported by critical service operators, digital service providers, and local government authorities. The CSIRT NASK also accepts incident reports from all users. Additionally, NASK contributes to the analytical and research-development support for the national cybersecurity system.

Science and Innovation – NASK engages in research and development activities aimed at creating solutions that enhance the efficiency, reliability, and security of telecommunication networks and other complex network systems (https://science.nask.pl/). What distinguishes our research institute from strictly commercial enterprises is our approach to developing solutions for current and future client needs. At NASK, researchers frame commercial problems within scientific contexts, using tools that are often broader and more abstract to achieve results that are not only satisfactory but also innovative. The primary focus of research at NASK is cybersecurity, which encompasses detecting, warning, and responding to incidents, as well as acquiring, analyzing, processing, and transferring data. Research also extends to complex network systems, including IoT systems and mobile ad hoc networks. Significant research is dedicated to biometric methods for identity verification in service security. As a telecommunications operator, NASK offers innovative ICTsolutions for financial clients, businesses, public administration, and academic institutions. Additionally, NASK manages the .pl domain name registry (www.dns.pl).

An important aspect of NASK's activities is also user education and the promotion of the information society concept, primarily aimed at protecting children and young people from the dangers associated with using new technologies. The institute implements key projects crucial for the digital transformation of the country, including the Nationwide Educational Network (OSE) and Electronic Document Management (EZD RP).

NASK

EDITORIAL BOARD

NASK