PERSONAL DATA PROTECTION INDEX

2023

General editing:
Vitalii Moroz

Study experts:
Tetiana Avdeieva
Pavlo Bielousov
Lidiia Volkova
Vitalii Moroz
Alina Pravdychenko

Project coordinator:
Sofiia Lavreniuk

Design and layout:
Kateryna Kysla

Literary editor:
Yevheniia Solodkova

Proofreader:
Yuliia Moroz

This expert study was prepared by the Internews Ukraine NGO in the framework of the Mainstreaming Privacy in the Digital Sphere in Ukraine project with the support of the ABA ROLI Ukraine / Rule of Law Initiative. The material presents the position of the authors and does not necessarily reflect the position of the ABA ROLI Ukraine / Rule of Law Initiative.

ABA ROLI Ukraine / Rule of Law Initiative has been working to promote human rights and the rule of law in Ukraine since 1992, including through the development of the legal profession and the fight against corruption, cybercrime and trafficking in human beings.

Website: www.americanbar.org
Facebook: www.facebook.com/abaroli.ukraine

Internews Ukraine is one of the largest NGOs in Ukraine, working in the field of strategic communications, media development and information security since 1996.

Website: www.internews.ua
Facebook: www.fb.com/internewsukraine

AMERICAN BAR ASSOCIATION
Rule of Law Initiative

INTERNEWS UKRAINE

internet freedom

Contents

Introduction

Introduction

Should we be talking about digital rights during the war, when security challenges dominate the public agenda? When the evil is visible, and russia is the enemy that daily shells civilians, destroys civilian infrastructure, and tries to seize further territories of Ukraine. Many of the projects implemented by civil society in Ukraine in 2022-2023 have been reformatted in the context of russia's armed aggression: dozens of organizations are recording evidence of the aggressor's war crimes, hundreds are helping to raise funds to support the army, and thousands are volunteering.

The team of the **Personal Data Protection Index** study also faced a choice: to continue working on the project or to reformat it. We decided to continue working. We believe that further implementation of the study launched in 2021 is necessary primarily for the users to be aware of their digital rights, the observance of which is a sign of a democratic society even in times of war. The civilized nature of the Ukrainian society is what distinguishes us from the aggressor's society and gradually brings Ukraine closer to the European choice, including through research that emphasizes respect for user rights protection from the private sector. In this study, we have taken into account the martial law conditions, and we do not publish the estimates for six companies representing the telecommunications market, namely operators and providers. Why? During the war, they are subject to government regulations, and therefore, the management of these companies has a somewhat limited ability to formulate internal policies.

We are convinced that further regulation of relations between the government, the private sector and citizens in national legislation should envisage the implementation of the human rights protection principle in the online space. This applies, in particular, to the area of privacy and personal data protection, as the interaction tools are expanding, the amount of information is constantly growing, which is well demonstrated by the rapid development of artificial intelligence technologies.

The methods of collecting and storing private information have undergone significant changes and vary even among individual companies and organizations that accumulate and manage data collected from billions of users. Despite the war, Ukrainian users interact through many Internet technologies and receive online services from the state and the private sector. The number of these services, as in the case of the **Diia** app, is only growing as millions of citizens have been granted the status of internally displaced persons, and tens or even hundreds of thousands have lost their homes and are awaiting help from the government.

All of these interactions in the world of technology involve granting user consent to the personal data storage and disposal policy. By continuing the **Personal Data Protection Index** study, the project team is once again focusing on the issue of the digital rights of users from the 'informed user' perspective. Do private companies create conditions for users to understand their rights in the online space? Do private companies envisage obtaining the user's informed consent for processing his or her personal data within their services? Does the corporate policy of a private company comply with international human rights standards and Ukrainian legislation on personal data?

When interacting with users, Ukrainian private companies are obliged to comply with the 2011 Law of Ukraine **On Personal Data Protection**. Twelve years ago, the role of online space in shaping social relations was much less than it is today: there was little knowledge of applications, online payments were rare, and social media

platforms had yet to face the major privacy issues that Meta or Twitter had in the past few years.

Today, Ukraine is on the verge of adopting a new legislative initiative that will regulate personal data protection. On October 25, 2022, the Verkhovna Rada of Ukraine registered the European integration draft law № 8153 **On Personal Data Protection**. This draft law contains many provisions that will introduce effective mechanisms for protecting users' personal data and harmonize national legislation with the approaches used in the European Union.

With the new law, one can expect significant improvements in terms of the protection of digital rights of users, while the implementation of provisions of the draft law is likely to change the culture of personal data use in Ukraine. At the same time, one should remember that the provisions of national legislation do not necessarily reflect the full scope of international human rights standards. That is why the role of civil society in actualizing these international standards is significant, and why projects such as the **Personal Data Protection Index** expand understanding of the protection of digital human rights and the range of their application in Ukraine.

Two years ago, the 2021 **Personal Data Protection Index** study was, perhaps, the first in Ukraine to launch a broad public discussion on the private sector's role in shaping policies and practices of respect for the personal data of Ukrainian users.

The study has already identified key challenges in protecting users' personal data, and this year's survey allowed us to determine what responses private companies have given to the problematic aspects identified in the previous study. We are convinced that, despite the challenges of war, cultivating respect for personal data through corporate policy is a strategic choice for responsible businesses that plan to continue operating in Ukraine and build long-term relationships with their customers.

In 2022-2023, ten applications of private service companies and 20 websites of large private companies in Ukraine that provide online services and operate in the field of telecommunications and Internet access became the subject of the **Personal Data Protection Index** study.

The following companies / brands were included in the list of studied applications:

MEEST MPPV LLC – Meest	GLOVOAPP UKRAINE LLC – Glovo
PHARMA STUDIO LLC – Tabletki.ua	FISHKA LOYALTY LLC – Fishka (OKKO)
LIKI24 LLC – Liki24	WEST PETROL MARKET LLC – Pride (WOG)
BOLT.UA LLC – Bolt	I-TRAVELS LLC – Busfor
UKLON UKRAINE LLC – Uklon	EPICENTER K LLC – Epicenter

The following companies/brands were included in the list of studied websites:

Kyivstar PJSC — Kyivstar.ua	LANET TELECOM LLC — Lanet.ua	Nova Poshta LLC — Novaposhta.ua	ALLO LLC — Allo.ua
Lifecell LLC — lifecell.ua	ROZETKA.UA LLC — Rozetka.com.ua	COMFY TRADE LLC — Comfy.ua	MAKEUP GLOBAL / Makeup Trading LLC — Makeup.com.ua
VF Ukraine PJSC — Vodafone.ua	UAPROM LLC — Prom.ua	GoC FOXTROT LLC — Foxtrot.com.ua	KASTA GROUP LLC — Kasta.ua
Datagroup PJSC — Datagroup.ua	TYEMARKET UKRAINE LLC / OLX Global BV — Olx.ua	ID ELDORADO LLC — Eldorado.ua	SILPO FOOD LLC — Silpo.ua
TRIOLAN LLC — Triolan.com	Ukrnet LLC — Ukr.net	Citrus Group of Companies— Ctrs.com.ua[1]	ZAKAZ UKRAINE LLC — Zakaz.ua

[1] In the 2021 study, the project team analyzed the website citrus.ua, which was associated with the Citrus trademark and was a key platform for user interaction. In 2023, the Citrus trademark is now used by www.ctrs.com.ua, while the previous website does not exist. It was this website that was the subject of the study. For an explanation of the legal status and the Citrus trademark, please see www.ctrs.com.ua/about

The purpose of this year's **Personal Data Protection Index** is to analyse corporate policies on the observance of digital rights of users with a focus on personal data protection. We deliberately do not draw any particular attention to the companies that received low scores, but we suggest that all companies should once again review their approaches to personal data protection and improve their customer focus. At the same time, we pay more attention to companies that have done a lot to respect users' digital rights, although even the 'champions' of the study can still improve the protection of users and their inalienable rights in online space.

Back in 2021, the project team based their approach on the methodology of the globally recognized Ranking Digital Rights (RDR) project, which operates as part of the activities of the American non-governmental organization called New America. This year, the RDR celebrated its 10th anniversary, and it continues to research global tech giants. The Ukrainian study is only two years old, and we are closely following the methodology updates of our international colleagues. Two years ago, we adapted RDR to the Ukrainian realities of digital rights protection policy, and **Internews Ukraine** became the first NGO in Europe to carry out a similar study.

Summary of the Study Findings

Summary of the Study Findings

In this year's study, the project team evaluated both the websites and applications of 30 private companies operating in Ukraine. In terms of website research, our assessment shows that less than a quarter of private companies demonstrate a high level of personal data protection for their customers, which can be used as an indicator that the digital rights of users are mostly respected.

In the 'websites' category, Olx.ua and Ukr.net demonstrated the best results among the 20 companies studied, with 80% and 75% of the points respectively, which reflect the status of the corporate policy on privacy and protection of users' personal data. In the previous study conducted in 2021, these companies were likewise among the leaders, having scored 77.5% and 70%, respectively.

At the same time, it is still important for Olx.ua to ensure adherence to the principle of minimizing the data that the company collects about users, to provide them with the opportunity to view and manage authorizations on the site, and to indicate clearly how long it stores user data (currently it states "for as long as necessary", which is not a standard for respecting users' digital rights).

There is room for Ukr.net to improve its policies, including providing users with the possibility to read previous versions of privacy policies on the site, explaining in more detail about the data storage security, and indicating the geographical location of its servers (EU countries or Ukraine).

Under the conditions of martial law, the project team decided not to publish assessments of six companies representing the telecommunications industry – Kyivstar, Vodafone, and Lifecell, as well as Internet service providers Datagroup, Triolan, and Lanet – given the specific features of legislative regulation of telecommunications companies during the wartime. Read more in the **Complete Methodology of the Study section**.

Ten out of 20 private companies in the websites category received at least 50% of the maximum number of points for personal data protection criteria. We assess the corporate policies of these companies as average and above average in terms of ensuring effective protection of the personal data of their customers. These are Kasta.ua Foxtrot.com.ua, Novaposhta.ua, Rozetka.com.ua, Prom.ua, Allo.ua, Silpo.ua, Zakaz.ua, as well as the above-mentioned Olx.ua and Ukr.net.

The remaining ten private companies received less than 50% of the maximum number of points for personal data protection criteria. Compared to the 2021 study, there has been a regression, as previously only eight out of 20 private companies received scores below 50% of the maximum. This may indicate a deepening gap in personal data protection, as reflected in the current corporate policies of the companies.

When assessing these ten out of 20 private companies, the researchers identified shortcomings in all four categories of the study: compliance with the national legislation, compliance with the European standards, to a lesser extent, technological aspects of website functioning, and website usability and inclusiveness.

At the same time, the assessment of ten private company applications demonstrated better results in terms of personal data protection compared to websites: 80% of applications (8 out of 10) received at least 50% of all possible points according to personal data protection criteria under the study methodology.

The highest scores were received by Bolt (82.3%), Liki24 (76.5%), and Uklon (73.5%). They are followed by Fishka (67.76%) and Tabletki.ua (56 %).

Furthermore, Bolt received 100% of the points in the **compliance with European standards on personal data category**, presumably because the company is an EU resident: its headquarters is located in Estonia. Liki24 and Uklon received 80% in the same category. At the same time, Bolt, Liki24, and Uklon scored high 80% in the category of **compliance with Ukrainian legislation on personal data**, while Tabletki.ua is the leader in this category with 90%.

Epicenter (47%) and Busfor (38.2%) received the lowest scores among applications. Each of the companies represented by these applications had low scores, which affected the overall score, in two categories: **compliance with European standards on personal data and technological aspects of the application**. These results indicate significant room for improvement in the respective companies' policies and technological improvements in their applications.

The team of the **Personal Data Protection Index** 2023 project recommends that company management should make an effort to improve corporate privacy and personal data protection policies and involve lawyers in the implementation of a plan to strengthen their privacy policies.

Brief Description of the Study Methodology

Brief Description of the Study Methodology

The purpose of the **Personal Data Protection Index** study is to examine the corporate accountability and transparency policies of leading private sector companies in Ukraine regarding their compliance with digital human rights in terms of the right to privacy and the culture of personal data storage and management.

The study is based on applied analysis and ranking using open data sources and official responses from companies regarding their privacy and personal data protection policies. The stages of field research and analysis include the following:

1. collecting information on the corporate policy of companies available from open sources, namely the official websites of private business companies;
2. drafting and sending an information request to private business companies to clarify their privacy policies;
3. development of a questionnaire for evaluating the collected data, which envisages classification of questions according to four categories of the study;
4. studying the collected data and assigning scores in accordance with the approved evaluation scale.

The project team focused on four key aspects of the corporate policy of private sector companies:

1. compliance with the requirements of the applicable Ukrainian legislation on personal data;
2. compliance with the European standards on personal data;
3. technological aspects of the website;
4. ease of use of the website and inclusiveness.

The study is based on publicly available documents that can be found on the official websites of the companies and in Android applications available on Google Play. Any user can access these documents. The researchers also studied the technical aspects of the companies' official websites and applications.

The **Personal Data Protection Index 2023** is the second edition of the study, which was expanded to include ten applications of technology companies operating in Ukraine. In the first edition of the **Personal Data Protection Index 2021**, we studied 20 large private companies operating in Ukraine. All 20 companies represented telecom and providers that deliver online services to the users. This year, the list of 20 companies whose websites we studied remained the same, which allows us to determine the progress / regress in the scores.

To evaluate the corporate policies of companies in the defined categories, the project team developed an evaluation questionnaire. The questionnaire contains 20 questions for websites and 17 for applications. Project experts assigned a score for each of the indicators choosing between three possible scores:

1. Score 0

information is absent or unavailable / undetectable. It indicates that the company ignores the issue / possibly does not comply with the digital rights protection criteria.

2. Score 0.5

information is incomplete. It indicates that the company partially discloses the policy in a specific aspect / possibly partially complies with the digital rights protection criteria.

3. Score 1

information is available, comprehensive and understandable for the user. Therefore, the company complies fully with the digital rights protection criteria.

The scores for each indicator were assigned by one of the experts. The results for each indicator were approved by two more experts. They were adjusted based on the information received from companies in response to an official request from **Internews Ukraine** NGO. The final scores were compared with each other and expressed as a percentage (%) of the maximum number of points that each company could have received.

The study was carried out by **Internews Ukraine** NGO involving lawyers and digital experts. The project's working group included Tetiana Avdeieva, Pavlo Bielousov, Lidiia Volkova, Vitalii Moroz and Alina Pravdychenko.

Findings of the Study

Findings of the Study

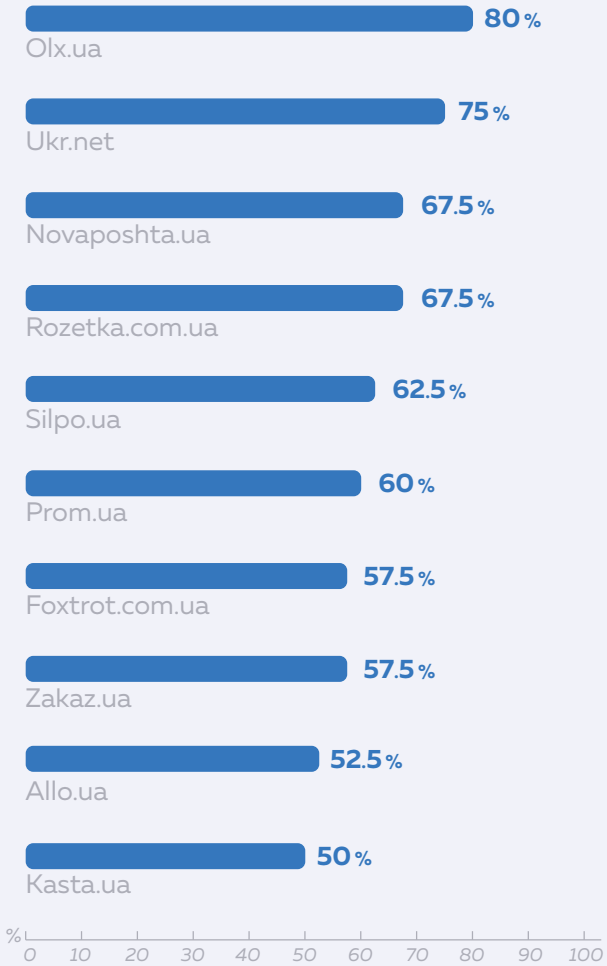
WEBSITES

The summarized results of the study with respect to the digital rights of users in terms of the privacy policy and personal data protection of private companies show that Olx.ua and Ukr.net are the 'champions' among the 20 companies in the category of websites selected for this study. They received the highest aggregate scores – 80% and 75% of the maximum possible points, respectively, reflecting the status of corporate privacy and personal data protection policies.

There is still room for improvement in these companies' corporate policies on privacy and personal data protection, since the researchers did not assign 20-25% of the points. At the same time, compared to other companies, the current privacy policies of Olx.ua and Ukr.net stand out for their reasonableness and balance.

In general, according to the study methodology only 10 out of 20 private companies meet the criteria for personal data protection by at least 50% of the maximum number of points. Consequently, the corporate policies of these companies were assessed as average and above average in terms of ensuring efficient protection of the personal data of their clients.

Personal Data Protection Index 2023
Results for the sites



The websites of the following three private companies demonstrated the greatest progress in the scores compared to the 2021 study:

+ 32.5 %
Silpo.ua

+ 22.5 %
Rozetka.com.ua

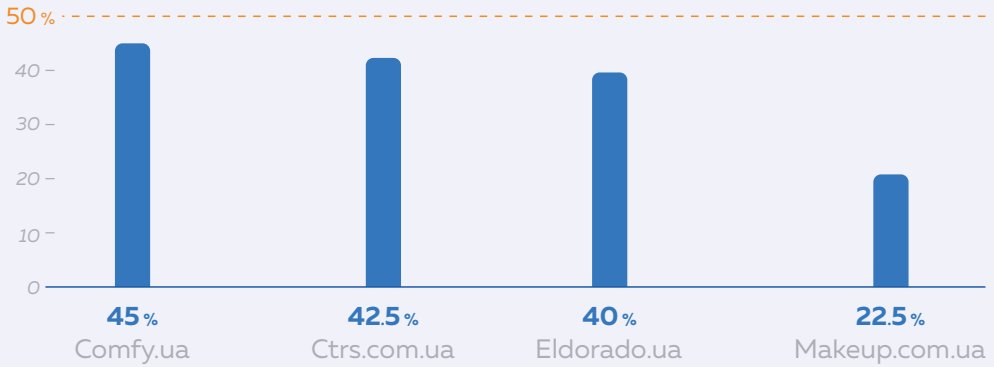
+ 15 %
Novaposhta.ua

Companies that scored above average should pay attention to minimizing the data they collect about users and publish a privacy policy in a simple and accessible form on their websites. For online services that sell goods and services, it is worth clearly stating how data is transferred to third parties. There is often a lack of comprehensive information about the secure storage of data on servers and the geographical location of these servers. Companies rarely inform users whether they have developed internal policies/regulations on personal data handling and protection.

The researchers note that most of these companies have significant shortcomings in all four categories, from compliance with national legislation to website usability and inclusiveness.

The management of these companies should review their corporate privacy and personal data protection policies to develop and implement a plan to strengthen their privacy policies.

The rest of the companies did not reach the mark of 50% of all possible points according to the criteria for personal data protection in accordance with the study methodology:



APPLICATIONS

The study of ten private companies' applications demonstrates that a significant number of companies focus on developing privacy policies: eight out of ten applications received at least 50% of all possible points for personal data protection criteria under the study methodology.

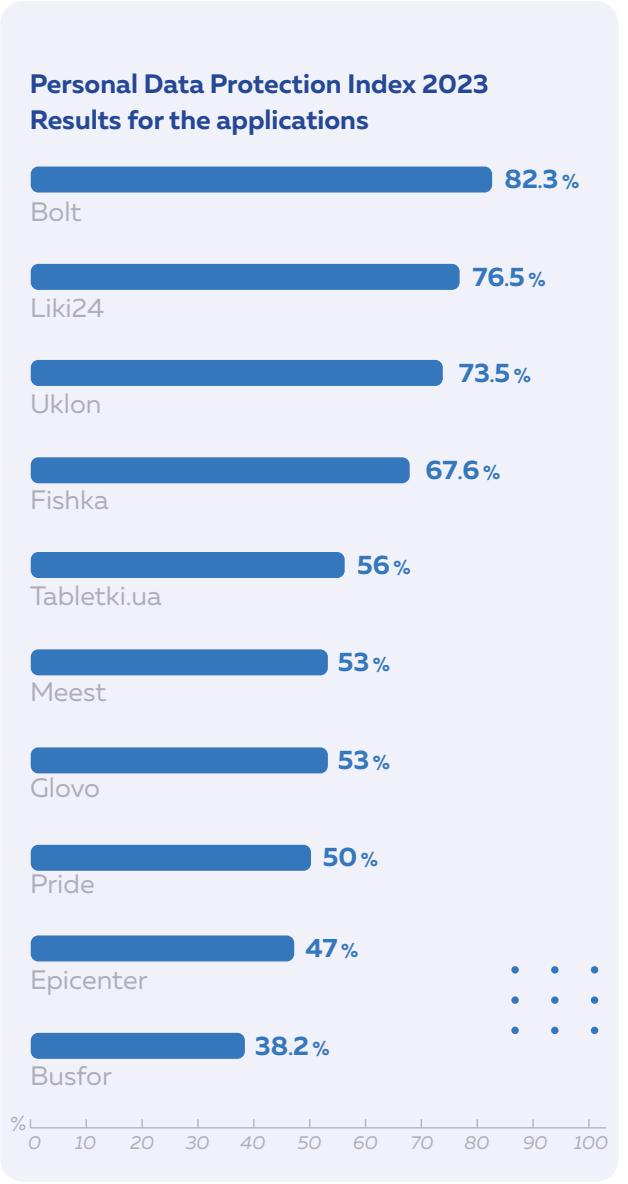
The leaders among the applications were the transportation services Bolt (82.3%), Uklon (73.5%), and drug delivery service Liki24 (76.5%). At the same time, Bolt received full points in the Compliance with the European standards on personal data category. Bolt is a company founded and headquartered in Estonia, and, therefore, is obliged to comply with all EU regulatory principles. Uklon is a Ukrainian company that scored 80% of the points in the European standards category, the same as Liki24.

In addition to this, Bolt, Liki24, and Uklon scored high 80% in the **Compliance with the Ukrainian legislation on personal data** category, while Tabletki.ua is the leader in this category with 90%.

In the final results of the study, Bolt, Liki24, and Uklon are followed by Ukrainian companies whose applications have demonstrated above-average scores: Fishka (67.6 %) and Tabletki.ua (56 %).

In turn, Busfor (38.2%) and Epicenter (47%) received the lowest scores among the companies' applications. Each of the companies had their overall scores affected by low scores in the following two categories: **Compliance with the European standards on personal data and Technological aspects of the application**. All of this leaves considerable room for improvement in these companies' policies and technological upgrades to their applications.

Detailed results of the survey can be viewed in the context of each of the four categories according to the survey methodology (read more about the methodology on page 25).



Results in Category 1
Compliance with the Ukrainian legislation on personal data

RESULTS FOR WEBSITES

In this category, a significant number of companies received mostly higher scores than in other categories. Such high scores reflect the fact that companies operate within the Ukrainian legal framework, and their lawyers are generally well acquainted with the provisions of respective regulatory acts.

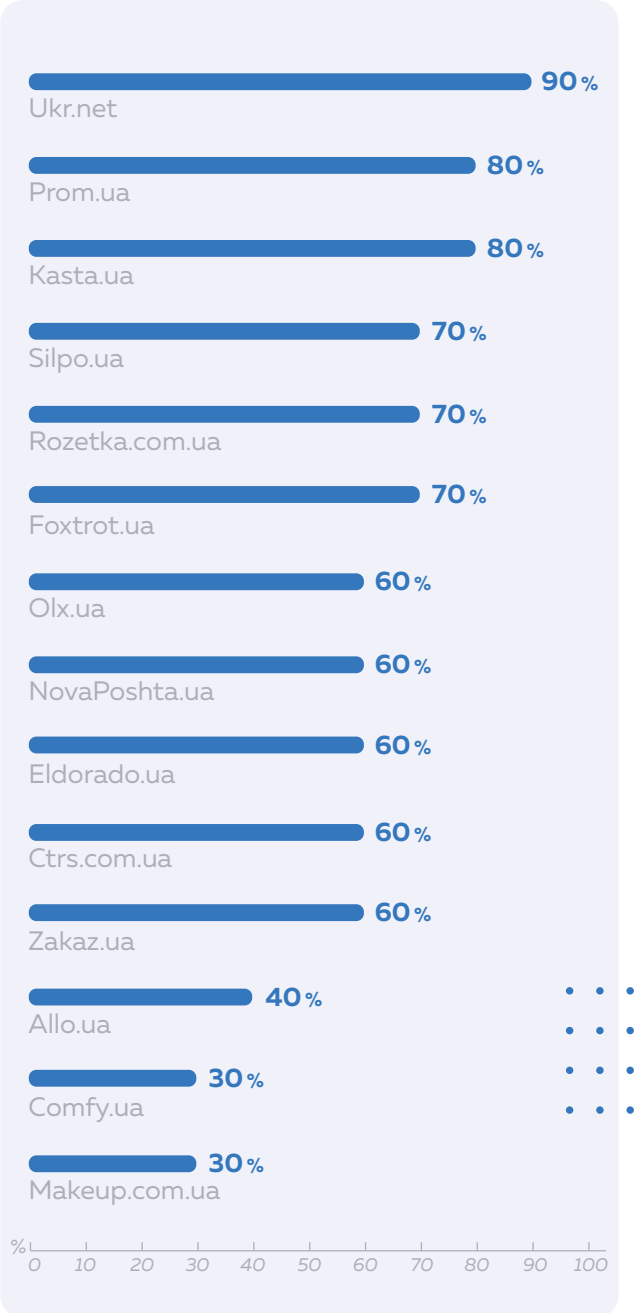
Ukr.net scored 90% of the possible points in the first category, while Prom.ua and Kasta.ua scored 80%. Three services scored slightly less (70%): Rozetka.com.ua, Foxtrot.com.ua, and Silpo.ua. Olx.ua, Novaposhta.ua, Ctrs.com.ua, and Zakaz.ua received 60% of all possible points each.

Comfy.ua and Makeup.com.ua received low scores in terms of compliance with national legislation (30% each). These companies should find a balance between the desire to attract customers with the ease of signing up for their services and compliance with the provisions of the applicable Ukrainian legislation on personal data protection.

Low scores in this category for both websites and applications may indicate that companies partially fail to comply with the Ukrainian legislation, but we cannot say for sure, as the information for the study was collected only from open sources and voluntary responses to our inquiries. Many companies did not respond, which makes it impossible to cross-check information from open sources. In any case, the results of assessment in this category should be seen as a path towards improvement of internal policies.

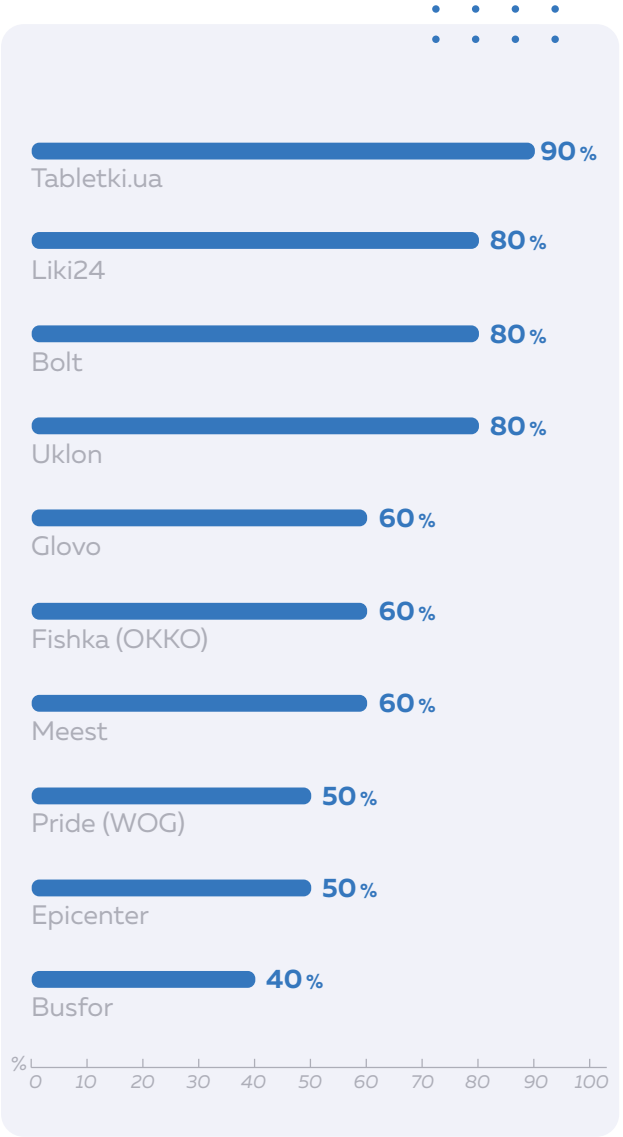
In Category 1, the researchers evaluated the companies' websites according to the following questions formulated for the study:

1. Does the website have a way for the user to give permission to process their personal data?
2. Does the company inform the user about what information it collects about him or her and how it is being used?
3. Does the company indicate the duration for which it will store information about the user?
4. Can users independently delete their personal data stored on the website?
5. Does the company adhere to the principle of data minimization that meets the purpose of its processing?



RESULTS FOR APPLICATIONS

In the category of Compliance with the Ukrainian legislation on personal data, the leader, according to the study, is the drug ordering application, Tabletki.ua with 90% of the possible points. Three applications received slightly lower scores: Bolt, Liki24, and Uklon – each with 80%. In general, companies demonstrated relatively high scores in this category: nine out of ten applications crossed the threshold of at least 50% of possible points. At the same time, only one application failed to score half of the points: Busfor's score in this category amounted to 40%.



Results in Category 2
Compliance with the European standards on personal data

European standards for the protection of human rights, namely personal data, are not mandatory for companies operating in Ukraine. At the same time, the European regulation (GDPR) applies to the territory of other countries if interaction with EU citizens takes place, and Ukrainian legislation on personal data protection is on the threshold of a qualitative update and harmonization of its provisions with EU legislation.

Ukrainian companies are increasingly adapting their corporate policies to the GDPR, which is becoming the norm in the Ukrainian private sector.

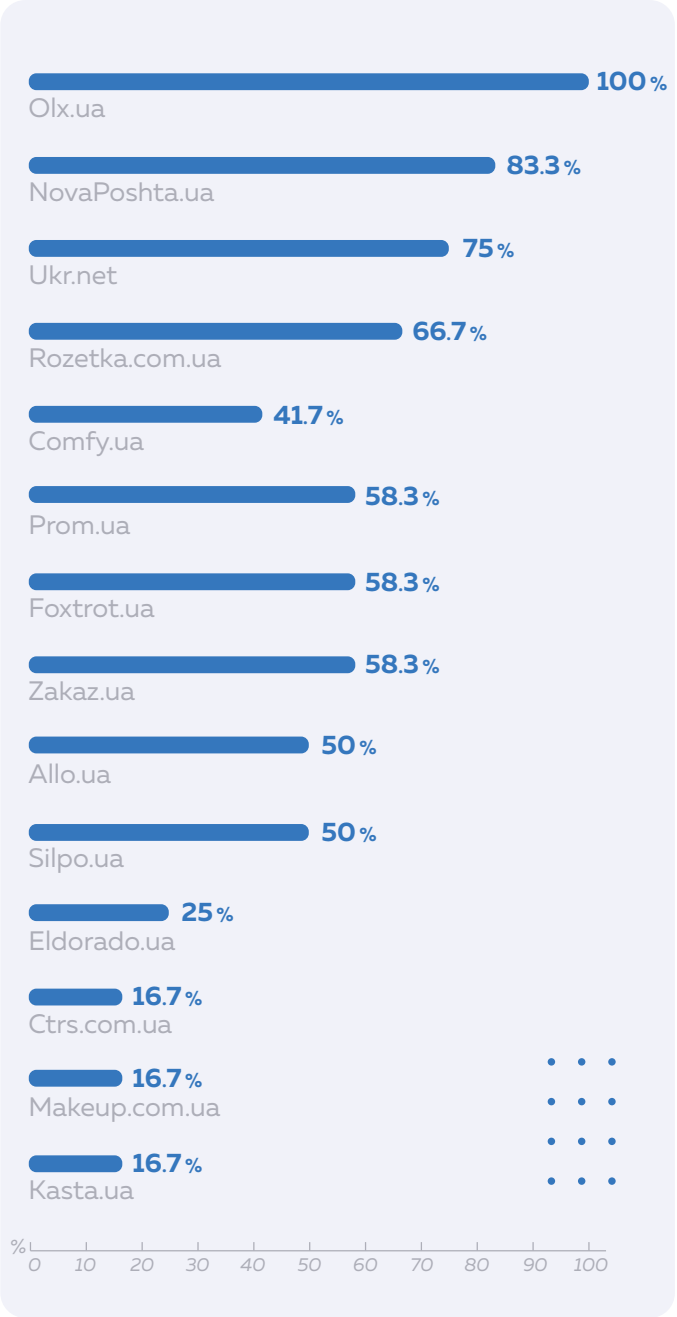
RESULTS FOR WEBSITES

Olx.ua scored 100% in this category: the company is part of a European business group, so it has implemented all provisions of the GDPR. Novaposhta.ua (83.5%), Ukr.net (75%), and Rozetka.com.ua (66.7%) also received high scores. Several other companies' websites crossed the 50% mark, including Prom.ua, Zakaz.ua, and Foxtrot.com.ua (58.3%).

The rest of the companies did not cross the 50% mark in terms of compliance with the European standards of personal data protection, and with the further adaptation of Ukrainian legislation to EU regulations, revision of the privacy policy of these companies will be on the agenda.

In Category 2, researchers evaluated companies' websites according to the following questions formulated for the study:

1. Does the website's functionality allow the user to understand clearly that he or she consents to the processing of his or her data?
2. Does the website provide information about the privacy policy in a concise, transparent, understandable and accessible form?
3. Can users familiarize themselves with previous versions of the privacy policy and changes in its updated version on the website?
4. Does the company describe the conditions for deleting a user account if the contract is terminated / the account is not used?
5. Does the company explain how it transfers user data to third parties?
6. Can the user submit a request to the company and receive a copy of their personal data?

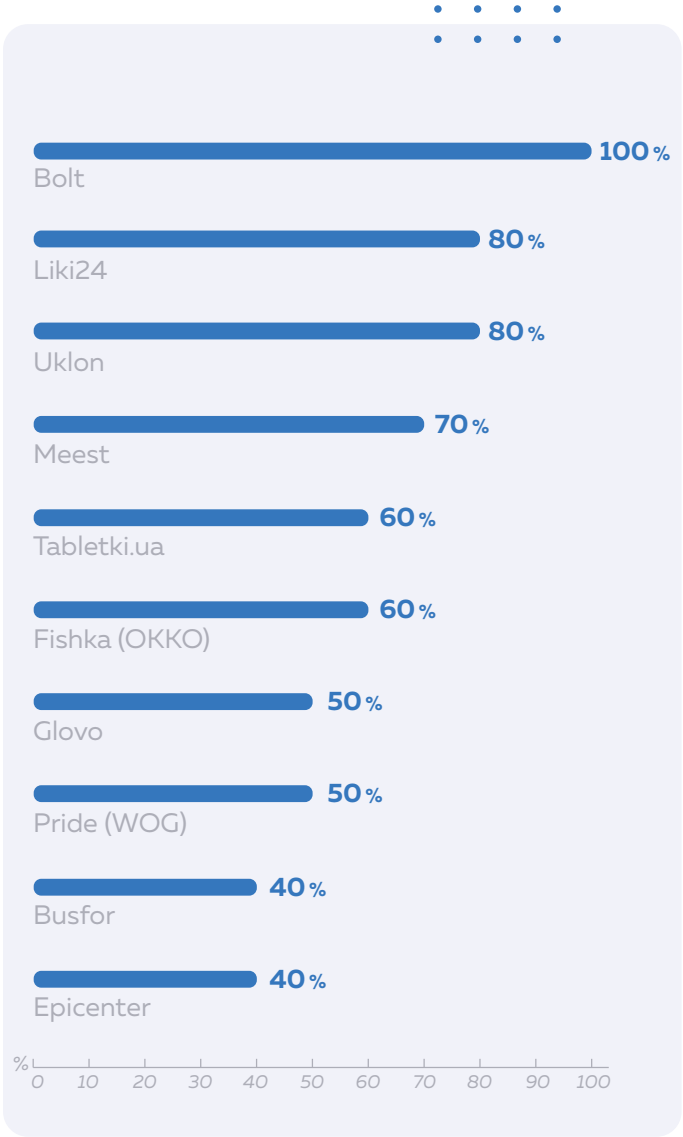


RESULTS FOR APPLICATIONS

The results application management companies demonstrated in the **Compliance with the European standards on personal data** category were quite good. All possible points in this category (100%) were awarded to the application of Bolt transportation service.

Two applications – Liki24 and Uklon – also scored high: each of them scored 80% in terms of personal data protection in the context of European regulations. Meest received 70% of the points, while Tabletki.ua and Fishka scored 60% each.

Two applications, Epicenter and Busfor, did not cross the 50% mark. Their scores amounted to 40% each.



Results in Category 3
Technological aspects of work

RESULTS FOR WEBSITES

According to the study results, safe use and interaction with corporate websites is a priority for a number of companies. On the websites of Novaposhta.ua, Ukr.net, Allo.ua (75% each), Olx.ua, Foxtrot.com.ua, and Kasta.ua (62.5% each), user interactions and personal data are mostly protected. Exactly 50% of the points in this category were scored by the following websites:

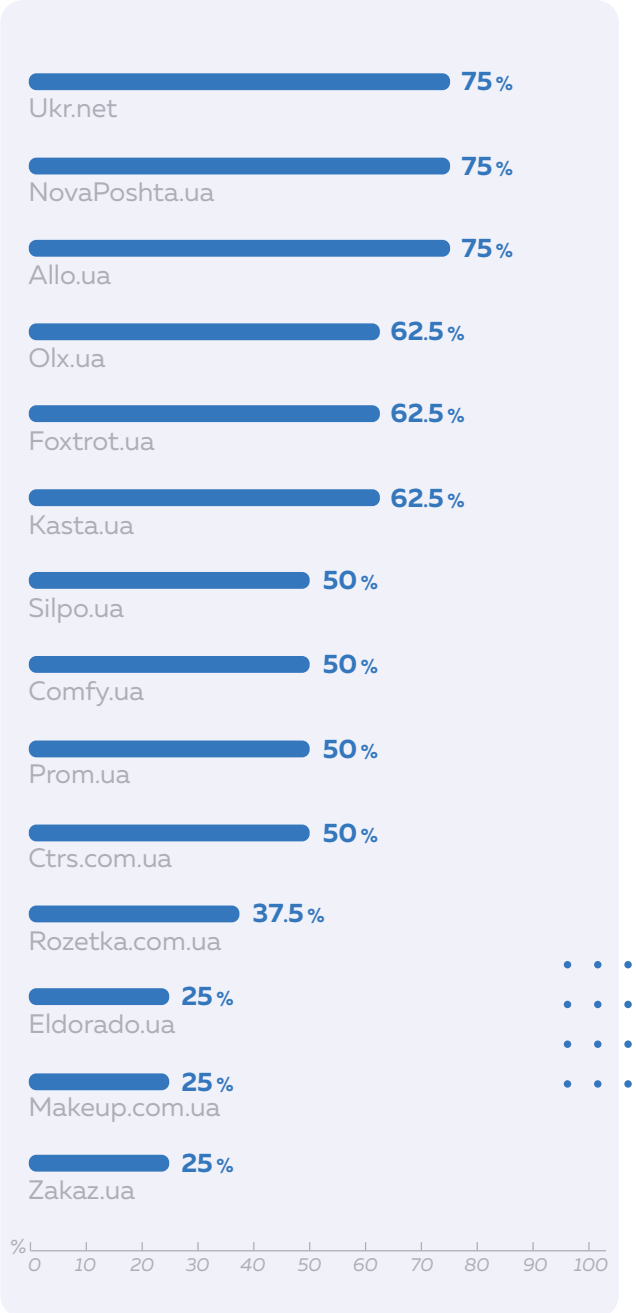
Silpo.ua	Comfy.ua
Ctrs.com.ua	Prom.ua

Traditionally, mobile operators have also received high scores in this category (we do not show specific scores for all companies working in the telecommunication sphere).

The project team advises that the rest of the companies should engage technical specialists to eliminate problems and strengthen protection against unauthorized access (for example, two-factor authentication when signing in), and inform about the safe storage of user data (servers).

In Category 3, researchers evaluated companies' websites according to the following questions formulated for the study:

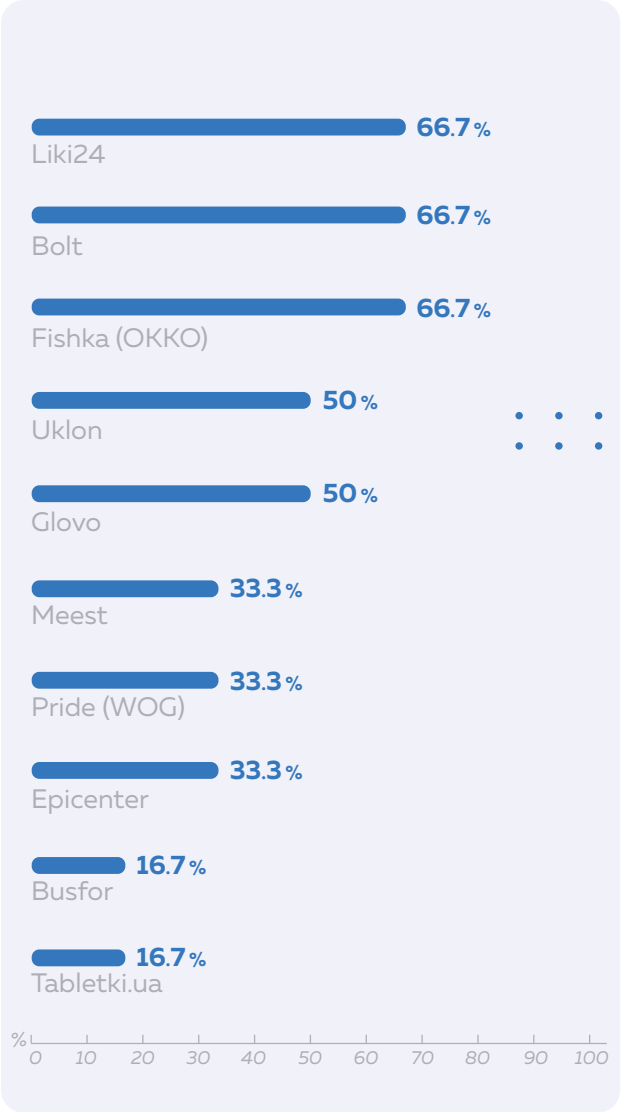
1. Does the company use the HTTPS secure connection protocol for its website?
2. Where and how does the company store user data?
3. Does the company provide users with the option of enhanced protection against unauthorized access?
4. Can users view and manage their authorizations on the website, such as when and from where they signed into the user account?



RESULTS FOR APPLICATIONS

In the **Technological aspects of work** category, the highest scores of companies did not exceed 2/3 of the maximum possible number of points. Three applications – Bolt, Liki24, and Fishka – each scored 66.7%, which is the highest in this category.

Uklon and Glovo received 50 per cent each, while Tabletki.ua and Busfor received the lowest scores – 16.67 per cent of possible points.



Results in Category 4
User-friendliness and inclusiveness

RESULTS FOR WEBSITES

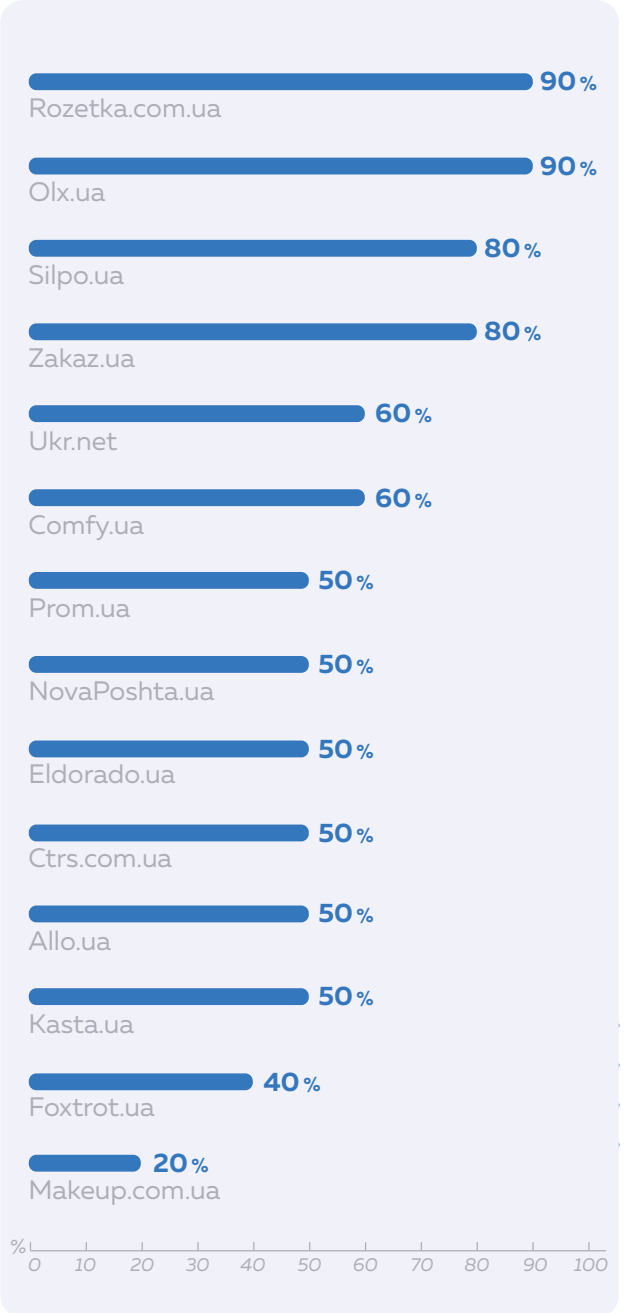
Usability allows visitors to navigate the site easily, find the information they need, and interact with it. If the site is not user-friendly, it can lead to user dissatisfaction, refusal to use the site, and reputational losses for companies. Website inclusiveness means accessibility for different categories of users, including people with disabilities, and people with different needs. When companies ensure that their websites are accessible to all users, these steps not only improve the company's reputation but also increase the website's audience.

According to the study results, Rozetka.com.ua and Olx.ua demonstrated the best performance in this category, with a score of 90%. They are followed by Silpo.ua and Zakaz.ua, which scored 80% each, while Comfy.ua received 60%.

A significant number of sites scored in the range of 40-50%, which indicates significant room for change on the part of companies to improve the usability and inclusiveness of their sites.

In Category 4, researchers evaluated companies' websites according to the following questions formulated for the study:

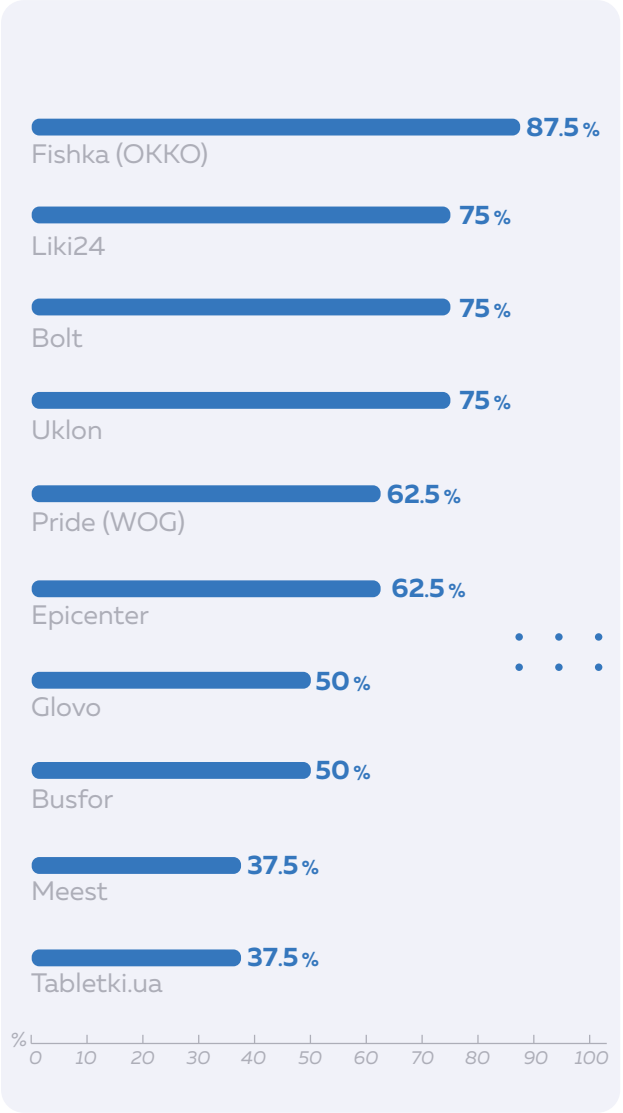
1. Can users find information on personal data protection on the website quickly and easily?
2. Can users familiarize themselves with the company's internal policies/regulations on personal data handling and protection?
3. Does the company provide information about the time limits for responding to the user's requests regarding personal data?
4. Can the users receive answers to their requests from the company through the support service using at least two means of communication (hotline, email, or chatbot)?
5. Does the company make the website useable for people with disabilities?



RESULTS FOR APPLICATIONS

Fishka received the highest number of points in the Ease of **User-friendliness and inclusiveness** category, with 87.5%. It is followed by three applications with a score of 75%, the consolidated rating leaders: Bolt, Liki24, and Uklon.

Epicenter and Pride scored high compared to the other three categories of the survey – 62.5% each. At the same time, Meest and Tabletki.ua showed the worst results in this category, with 37.5% each.



How were these results obtained?

The results of this study are based on the information collected from open data sources (official websites and Google Play applications of the companies) and official responses the companies gave to official requests. During the first stage, the project team identified the list of companies under study and monitored their official websites.

The project experts collected information on corporate policies by examining the companies' official websites. They analysed the data, assigned scores, and subsequently approved the results (questionnaire).

In order to correct the obtained results, the project team created and sent official information requests from Internews Ukraine NGO with clarifying questions about the companies' privacy and personal data protection policies. The requests were sent to the official mailing addresses of the companies and duplicated to official emails obtained from open sources.

Within 40 days after the requests were sent, the research team received about 50% of responses for the websites under study, while ten out of 20 companies provided responses as of the end of May 2023. The following companies responded: Ukrnet LLC (Ukr.net), EMARKET UKRAINE LLC (Olx.ua), UAPROM LLC (Prom.ua), Lifecell LLC (Lifecell.ua), Kyivstar PJSC (Kyivstar.ua), Citrus Group of Companies (Ctrs.com.ua), Nova Poshta LLC (Novaposhta.ua), Silpo-Food LLC (Silpo.ua), ALLO LLC (Allo.ua), and LANET TELECOM LLC (Lanet.ua). Quite a bit later, in June, COMFY TRADE LLC (Comfy.ua) responded to the request.

Regarding the applications studied, only 1 out of 10 companies responded to a clarification request from the project team – FISHKA LOYALTY LLC (Fishka).

The team did not receive a response to the request from 19 out of 30 companies within 40 days after it was sent.

The study results reflect the companies' privacy and personal data protection policies as of May–June 2023 (data analysis period).

Complete Methodology of the Study

Complete Methodology of the Study

The **Personal Data Protection Index** is a tool for studying the corporate policies of leading private sector companies in Ukraine regarding their compliance with the digital rights of users in terms of personal data protection. In 2022, the project team took into account the work of private sector companies during the war.

The project team decided not to publish the assessments of six companies representing the telecommunications industry during wartime. These are mobile operators Kyivstar, Vodafone, and lifecell, as well as Internet service providers Datagroup, Triolan, and Lanet.

This fact is explained by specific features of the legislative regulation of their activities in the context of war. Pursuant to the Law of Ukraine **On the Legal Regime of Martial Law**, the military command together with military administrations may regulate the operation of electronic communication networks and / or service providers during this period in accordance with the procedure established by the Cabinet of Ministers of Ukraine. In addition to this, in the spring of 2022, the Law of Ukraine **On Electronic Communications** was amended to require electronic communications network providers to comply with the orders of the National Centre for Operational and Technical Management of Electronic Communications Networks of Ukraine (NCU) in a state of emergency or martial law. In other words, the activities of each of these companies under martial law are partially regulated by the state authorities responsible for stability of communications during the war, so decisions on these companies' policies may be determined not only by their leadership.

At the same time, an internal assessment of these companies was conducted, and each of them received its own score within the framework of the **Personal Data Protection Index 2023** study. The study results reflect the dynamics of the protection of digital rights of users and representatives of the telecommunications industry.

In peacetime, the assessment of these companies will be made public again. You can view the results of the previous assessment of telecommunication companies in 2021 — link.

The study was carried out by **Internews Ukraine** NGO with the participation of digital experts and lawyers. The project working group included Tetiana Avdeieva, Pavlo Bielousov, Lidiia Volkova, Vitalii Moroz, and Alina Pravdychenko.

Subject matter of the study

Corporate policies of accountability and transparency of the leading private sector companies in Ukraine in terms of their compliance with the digital rights of users.

The purpose of the Personal Data Protection Index study

To study the corporate policy on ensuring accountability and transparency of the leading private sector companies in Ukraine regarding their compliance with digital human rights in terms of the right to privacy and the culture of storing and disposing of users' personal data.

Main methods of the study

The study is based on applied analysis and ranking using open data sources and official responses from companies.

Stages of the field research include:

1. collecting information on corporate policy from open sources, namely 20 official websites

and ten applications of private business companies;

2. drafting and sending an information request to 30 private business companies asking them to clarify their privacy policies;

3. development of a questionnaire for evaluating the obtained data, which envisages the classification of questions in accordance with the four categories of the study;

4. studying the obtained data and assigning scores according to the approved evaluation scale.

Assessment criteria according to methodology of the study

The project team focused its attention on studying four main aspects of the corporate policy of private sector companies.

I. COMPLIANCE WITH THE UKRAINIAN LEGISLATION ON PERSONAL DATA

The following criteria were used:

1. The company has provided an opportunity for the user to indicate their consent to personal data processing.

2. The company has ensured that the user has the right to know what information is collected about them and how it is used.

3. The company indicates how long it will store information about the user.

4. The company has provided the user an ability to delete their personal data stored on the website.

5. The company adheres to the principle of data minimization.

II. COMPLIANCE WITH THE EUROPEAN STANDARD ON PERSONAL DATA

The following criteria were used:

1. The user clearly understands that he or she consents to the processing of his or her data.

2. Information about the privacy policy is provided to the user in a concise, transparent, understandable and accessible form with clear and simple wording.

3. The company has provided an option for users to familiarize themselves with previous versions of the privacy policy and with changes in its updated version.

4. The company describes the conditions for deleting a user's account if the contract is terminated / the account is not used.

5. The company explains how it transfers the user's data to third parties.

6. The company enables its users to request a copy of their personal data.

III. TECHNOLOGICAL ASPECTS OF THE WEBSITE/APPLICATION

The following criteria were used:

1. The company envisages the use of the secure HTTPS connection protocol in the website operation.

2. The company envisages hosting servers in countries where there is no repressive legislation on the Internet and access to data is protected by law.

3. The company has provided users with an opportunity to make use of enhanced protection against unauthorized access to the user account.

4. The company has provided the user with an opportunity to view sign-in history, when and from where they signed into their account.

IV. USER-FRIENDLINESS AND INCLUSIVENESS OF THE WEBSITE / APPLICATION

The following criteria were used:

1. The user can find information on personal data protection on the website/application quickly and easily.
2. The user can familiarize themselves with the company's internal policies/regulations on personal data processing and protection.
3. The user can receive answers to their inquiries from the company through a support service.
4. The company provides information about the time limits for responding to the user's requests regarding personal data.
5. The company makes the website useable for people with disabilities.

To evaluate the corporate policies of companies in the defined categories, the project team developed an evaluation questionnaire. It contains 20 questions for websites and 17 questions for applications, as some questions are not relevant for applications due to their technological features.

Project experts give a score to each of the items, choosing between three possible scores:

1. Score 0

Information is absent, or it is unavailable / undetectable. It indicates that the company ignores the issue / possibly does not comply with the digital rights protection criteria.

2. Score 0.5

Information is incomplete. It indicates that the company partially discloses the policy in a specific aspect / possibly partially complies with the digital rights protection criteria.

3. Score 1

Information is available, comprehensive and understandable for the user. Therefore, the company complies fully with the digital rights protection criteria.

Criteria for selecting companies for the study

In 2022, 30 companies were studied and divided into groups based on two criteria:

1. **Platform criterion.** The first group includes 20 companies whose websites are the subject of the study, and the second group includes ten companies whose applications on Google Play are the subject of the study. The division of companies is based on the specific feature of the interface, in which companies interact with the user.

2. **Company specialization criterion.** All 30 companies were divided as follows:

   2.1. Ten companies are service companies that use applications (postal services, pharmacies, transportation, delivery, ticketing, retail, and loyalty programs).

   2.2. Six companies represent mobile operators and providers and use websites.

   2.3. Fourteen provide services to users through electronic services with or without registration on the website.

Companies were grouped by taking into account the specific features of services provided to their users and the amount of personal information that companies store and manage.

The main criteria for selecting companies from the "service" group (applications):

1. Commercial activities of companies are based on the functioning of an application, through which they provide services / sell goods to users.

2. The companies' applications are some of the most popular among Ukrainian users in terms of downloads on Google Play.

The main criteria for selecting companies from the "telecom" group (websites):

1. Companies provide mobile communication/ internet access services to users.

2. Companies are market leaders and have official websites with information about their usage policies.

3. To identify users, companies collect their personal data.

The main criteria for selecting companies from the "service" group (websites):

1. The commercial activity of companies is based on the functioning of a website, through which they provide services / sell goods to users.

2. According to survey results, the companies' websites are some of the most popular among Ukrainian users.

3. Users have to register on companies' websites, transferring personal information to use the services provided by these companies, or services are provided without registration, but the transfer of personal data is envisaged.

Why did we include applications in this year's study?

1. Applications are becoming a typical way for users to interact with the private sector, as they are increasingly accessing the web from mobile devices rather than desktops: this is evidenced by numerous studies, such as the one by Kantar Cmeter for April 2022.

2. Applications usually require a lot of permissions from the user regarding their privacy, including contacts, and biometric data. This is also often associated with the provision of geolocation-based services.

3. Applications are part of the government's digitalization of society; for example, through **Diia**, a user can access administrative services. Accordingly, more and more users are getting used to the app system.

4. The project team separately identifies state/ municipal applications (Diia, Pension Fund), applications of global tech giants (Facebook, Twitter, TikTok), as well as applications the use of which is related to specific secrets protected by law: banking, medical, etc. All these applications require a separate study.

5. The ten applications analysed in the study were developed for the Android operating system and are available on Google Play, as Android devices predominate among users. The project team did not analyse the same applications that are available on the App Store and are intended for use on the iOS operating system.

How did we obtain data for the study?

The study became possible as a result of analysing the collected data set. The data was obtained from open sources (official websites and applications of companies) as well as responses from companies to official requests made by researchers. The inability to obtain official data or lack of data was taken into account when formulating the study's findings.

Two main ways of obtaining data:

1. Collecting and analysing information from open sources by monitoring official websites and applications of private sector companies.

2. Preparing and sending information requests to private business companies for clarification of their privacy policies. The requests were drafted in accordance with Ukrainian law and sent by mail. At the same time, the requests were also forwarded to the companies' official emails. The project team expected to receive responses from the companies within 40 days after the requests were sent.

How are the study results corroborated?

The project team used a double peer review approach to evaluate the results. One of the experts assigned scores, and then the second and third experts approved them. The results were adjusted based on the information received from the companies in response to official requests from **Internews Ukraine** NGO. The final scores were compared with each other and expressed as a percentage (%) of the maximum number of points that each company could receive.

What is the final product of the study?

The full text of the study, as well as summarized findings, was published as a report on the project's website uadigital.report, and it was also forwarded to each private company that was the subject of the study.

Contents of the questionnaire used for evaluating companies

The project team developed two questionnaires (for websites and applications), consisting of 20 and 17 questions, respectively, divided into four main categories. Based on the answers given to each question, the expert assigned one of three possible ratings:

1. Score 0

Information is absent, or unavailable / undetectable. It indicates that the company ignores the issue / possibly does not comply with the digital rights protection criteria.

2. Score 0.5

Information is incomplete. It indicates that the company partially discloses the policy in a specific aspect / possibly partially complies with the digital rights protection criteria.

3. Score 1

Information is available, comprehensive and understandable for the user. Therefore, the company complies fully with the digital rights protection criteria.

Compliance with the requirements of the Ukrainian legislation on personal data
(5 questions):

1. Does the website / application have a way for the user to give permission to process their personal data?
2. Does the company inform the user about what information it collects about him or her and how it is being used?
3. Does the company indicate the duration for which it will store information about the user?
4. Can users independently delete their personal data stored on the website / application?
5. Does the company adhere to the principle of data minimization that meets the purpose of its processing?

Compliance with the European standards on personal data
(6 questions for websites, 5 for applications):

1. Does the functionality of the website / application allow the user to understand clearly that he or she consents to the processing of his or her data?
2. Does the website / application provide information about the privacy policy in a concise, transparent, understandable, and accessible form?
3. Can users familiarize themselves with previous versions of the privacy policy and changes in its updated version on the website / application?
4. Does the company describe the conditions for deleting a user account if the contract is terminated / the account is not used? (Only for websites)
5. Does the company explain how it transfers user data to third parties?
6. Can the user submit a request to the company and receive a copy of their personal data?

Technological aspects of work of the website / application
(4 questions for websites, 3 for applications):

1. Does the company use the HTTPS secure connection protocol for its website? (Only for websites)
2. Where and how does the company store user data?
3. Does the company provide users with the option of enhanced protection against unauthorized access?
4. Can users view and manage their activity on the website / in the application, when and from where they signed into the user account?

User-friendliness and inclusiveness
(5 questions for websites, 4 for applications):

1. Can users find information on personal data protection on the website / in the application quickly and easily?
2. Can users familiarize themselves with the company's internal policies / regulations on personal data handling and protection?
3. Does the company provide information about the time limits for responding to the user's requests regarding personal data?
4. Can the users receive answers to their requests from the company through the support service using at least two means of communication (hotline, email, chatbot)?
5. Does the company make the website useable for people with disabilities? (Only for websites)

Explanation of the evaluation criteria

What do we mean by "compliance with the requirements of the current Ukrainian legislation on personal data"?

1. The user's consent is the main prerequisite for processing his or her personal data.

Of course, consent is not the only ground for processing personal data under the Law of Ukraine On Personal Data Protection; such grounds may include, in particular, the very fact of entering into and performing a transaction, to which the subject of the personal data is a party. To assess this criterion, we analyse what grounds for processing personal data the company states in its documents. If such a basis is the provision of consent, we compare the procedure for granting such permission (consent) with the requirements stipulated by law. The Law of Ukraine On Personal Data Protection (Article 2) defines consent as a voluntary expression of will by an individual (subject to the provision of respective information to him / her) granting permission to process his / her personal data in accordance with the stated purpose of their processing, expressed in writing or in a form that allows to conclude that consent has been granted. In the field of e-commerce, the consent of the personal data owner can be provided during registration in the information and telecommunication system of the e-commerce entity by marking the permission to process personal data in accordance with the formulated purpose of their processing, provided that such system does not process personal data until the consent is given. In other words, the main aspects when assessing this component are the user's active actions to provide consent, and the inability to use the service if such actions are not taken. In fact, it is the inability to receive services without pressing certain buttons / checking the appropriate boxes. If such conditions are present, the assessed entity will receive 1 point, and in case of partial compliance with these criteria – 0.5 points.

2. The main right of a personal data owner is the right to know what information is collected about them and how it is used.

At the same time, the law states explicitly that information about the personal data owner (i.e., not only the website / application that collects personal data, but also about a specific individual or legal entity), the composition and content of the collected personal data, the rights of the resource user, the purpose of collecting personal data and the persons to whom personal data is transferred must be provided when collecting personal data (Article 12 of the Law of Ukraine On Personal Data Protection). Usually, all of these issues are disclosed in the privacy policy, which is provided to the user when they are asked to grant consent for the processing of their personal data. In this case, the entity received 1 point if its website has a privacy policy that covers all of the above questions, and the user reads it before submitting their personal data; 0.5 point was awarded to entities that partially meet the listed criteria.

3. The company specifies the duration for which the data is stored.

Ukrainian legislation establishes certain requirements for the duration of processing / storage of personal data. Personal data have to be processed in a form that allows identification of the individual to whom it relates for no longer than necessary for the legitimate purposes, for which it was collected or further processed (Article 6 of the Law of Ukraine On Personal Data Protection). Expiration of the information storage duration determined by the consent of the personal data owner to the processing of such data or by law constitutes grounds for deleting the data (Article 15 of the Law of Ukraine On Personal Data Protection). Therefore, it is extremely important to indicate the duration of data storage, and this should be reflected on the company's website / application, so 1 point is awarded to companies that indicate the duration of storage of the user information directly, 0.5 points – if the duration is unclear or hidden on the website, 0 – if it is not mentioned.

4. **The Law of Ukraine On Personal Data Protection stipulates that consent to the processing of personal data can be withdrawn at any time (Article 8).**

In practice, this means that the system technically allows the deletion of personal data (there should be a corresponding button / option in the interface) / a transparent mechanism for deleting personal data should be described or at least a contact address should be provided to request the deletion of personal data. In this regard, 1 point is awarded to entities whose services contain direct and unambiguous means for deleting personal data (appropriate buttons or instructions), and 0.5 points are awarded to entities whose services allow deleting personal information upon request.

5. **The Company adheres to the legally established principle of personal data processing – the data minimization principle.**

For example, the composition and content of personal data must be appropriate, adequate and not excessive in relation to the purpose of its processing (Article 6 of the Law of Ukraine On Personal Data Protection). At the same time, the purpose of data processing should be specified in the user agreement (privacy policy) and directly related to the provision of the services offered. This means that any company should collect from users only the data necessary to provide services and not request unnecessary information. In this regard, the assessed entity received 1 point if it fully complies with the minimization principle and 0.5 points if it complies partially.

What do we mean by "compliance with the European standards on personal data"?

Ukrainian personal data protection legislation is undergoing a transformation. One of the reasons for this is the desire to comply with European standards, in particular the provisions of the General Data Protection Regulation known under the acronym GDPR, which came into force in the European Union in 2018. This regulation significantly strengthens the rights of users, primarily through the principles of simplicity and clarity. Currently, the GDPR is not mandatory in Ukraine, but given that many Ukrainian companies can provide their services to European users, and Ukraine's progress toward European integration is noticeable, the project team thought it would be appropriate to assess how user-friendly Ukrainian companies are and how they comply with the European standards.

1. One of these standards is the standard of conspicuousness of consent. According to Article 7 of the GDPR, if the data subject provides consent in the context of a written declaration that also addresses other questions, the request for consent must be presented in a clear and accessible form that is clearly distinguishable from the other questions. This means that **the user must clearly understand that he or she is consenting to the processing of their data**, and the option to provide such consent must be separated from all other possible actions (e.g., by means of a separate button, special mark, etc.). At the same time, statements such as By clicking the "Confirm Order" button, I consent to the processing of my personal data or By continuing to use the site, you consent to the processing of your personal data will not meet the standard, as they are not clearly separated from other questions or actions. Similarly, an automatically checked consent box cannot be considered compliant with the standard, as the user may uncheck it or not notice it.

2. Privacy policies of many Ukrainian websites / applications are usually written in rather dry, hard-to-understand legal language. The GDPR sets standards for notifying users about the use of their personal data. According to Article 12, information about the privacy policy, including information intended for children, must be provided to the user in a **concise, transparent, understandable and accessible form**. In fact, it means that an ordinary user, who is not a lawyer or a specialist in the personal data sphere, should be able to understand easily by whom and how the information about them will be used.

3. The company should provide an option for users to familiarize themselves with **updates (versions) of the privacy policy**. This allows the user to compare the changes that the company made to the personal data policy and, if necessary, exercise their right to withdraw consent to the processing of their data.

4. If personal data is no longer needed for the purposes, for which it was collected or processed, personal data must be erased without any unreasonable delay (Article 17 of the GDPR). Termination of the agreement or non-use of the account for a prolonged time may, in certain cases, indicate that the purpose of collecting personal data is no longer relevant, and therefore there are no grounds to process the respective data. That is why it is important whether the **company describes the conditions for deleting a user account if the contract is terminated / the account is not used**.

5. The company has the right to transfer user data to third parties, provided the user agrees. When receiving personal data, it must inform the user about the recipients or categories of recipients of personal data (Article 13 of the GDPR). In addition to this, the GDPR regulates the conditions for transferring data to a third country or an international organization in detail. Therefore, explaining the process of **transferring user data to third parties is necessary and important**.

6. The personal data owner has the right to receive copies of the processed personal data (Article 15 GDPR). Respectively, the owner is entitled not only to know about the list of such data, but also to see clearly the entire array of information being processed. Large international platforms provided this option to their users several years ago.

What do we mean by "technological aspects of the website functioning"?

User interaction with companies' websites / applications implies that the user should be protected from possible harmful influences and information leaks. Modern standards for protecting websites / applications and their servers are becoming mandatory, and they should be reflected both in the architecture of the technical component of companies' operations and in the functioning of the websites / applications themselves. Furthermore, websites / applications should provide technical protection capabilities at the user level.

Thus, the basic criteria for the technical component include the ability to visit websites that operate **on the basis of the HTTPS secure connection protocol** using a TLS certificate. **The company's servers should be located in countries** where there is no repressive legislation on the Internet and access to data is protected by law, which minimizes the risks of unauthorized access to information on these servers and, accordingly, to users' personal data.

At the level of user control over their data, responsible companies **provide a possibility for users to view their browsing history**, see when and from where they accessed their accounts. The company should be able to **ensure enhanced protection** (e.g., two-factor authentication (2FA), authorization via SMS or IP address) when logging into a personal account to protect the user from unauthorized access to the account.

What do we mean by "user-friendliness and inclusiveness"?

User-friendliness of a website / application means that its usability responds to the user's need to find information quickly and easily, with links to it displayed on the first page of the first screen of the website / application and visible against the background of other content on the website / application. Companies can emphasize the protection of personal data in the following ways:

1. Publish **reference information** on personal data protection on the website / application.
2. Develop and implement the **company's internal policy / regulations on personal data processing** and protection.
3. Provide information about the **timeframe for the examination of requests** related to personal data.
4. Provide a possibility for users to **contact the company through a support service** in several convenient ways, such as through a hotline, email, or chatbot.

The use of services, and, accordingly, of the website / application, involves taking into account the interests of people with disabilities. In order to comply with the principle of inclusiveness in the organization of the company's work, it is necessary to **provide services to people with disabilities (for example, people with visual or hearing impairments) in a convenient and accessible form**. In particular, companies should envisage a possibility to contact an operator or chatbot in a voice format, to have a separate version of the website or application for people with disabilities if the company's services cannot be provided without the said version. Companies should also place a disclaimer about such a version so that users know about the possibility of using additional (special) functionality. When formulating its policy, the company should avoid any discriminatory provisions against persons with disabilities and promote inclusiveness in every way possible.

Conclusions and Recommendations

Conclusions and Recommendations

In 2023, the team of the **Personal Data Protection Index** project presented the results of one more study of corporate personal data protection policies of 30 private companies that use digital technologies to interact with their customers and operate in Ukraine. This time, the list of 20 companies, whose websites the project team studied for the first time in 2021, has been expanded to include ten companies that have their customers use mobile applications to interact and receive services.

The study was carried out in the context of Russian aggression against Ukraine, which impacted its implementation. Due to martial law, the project team decided not to publish the ratings of six companies representing the telecommunications industry. These are mobile operators Kyivstar, Vodafone, and lifecell, as well as Internet service providers Datagroup, Triolan, and Lanet.

Under martial law, the activities of each of these companies are partially regulated by the state authorities responsible for stability of communications during the war, so decisions on these companies' policies may be determined not only by their leadership.

Another reason for our decision is based on the fact that we believe it is inappropriate and potentially harmful to publicize and discuss the details of shortcomings and gaps in data protection on the part of companies that belong to a critical area during the war.

During the war, a significant number of private companies in Ukraine did not shut down their operations and continue to provide services to their customers, adapting to the conditions of martial law. Companies also participate in charitable projects, initiating fundraising campaigns and expanding their services to temporarily displaced persons and refugees who were forced to leave the territory of Ukraine due to the security situation. The project team is aware that updating corporate policies, particularly in terms of personal data protection, is not a priority for companies in times of war. At the same time, the project team has noticed that a number of companies have improved their policies since 2021 (when the results of the first study were announced).

In the 'websites' category, Olx.ua and Ukr.net demonstrated the best results among the 20 companies studied, with 80% and 75% of the points respectively, which reflect the status of the corporate policy on privacy and protection of users' personal data. In the previous study conducted in 2021, these companies were also among the leaders, having scored 77.5% and 70%, respectively.

At the same time, it is still important for Olx.ua to ensure adherence to the principle of minimizing the data that the company collects about users, to provide them with the opportunity to view and manage authorizations on the site, and to indicate clearly how long it stores user data (currently it is stated: "For as long as necessary", which is not optimal in terms of ensuring respect for the users' digital rights.

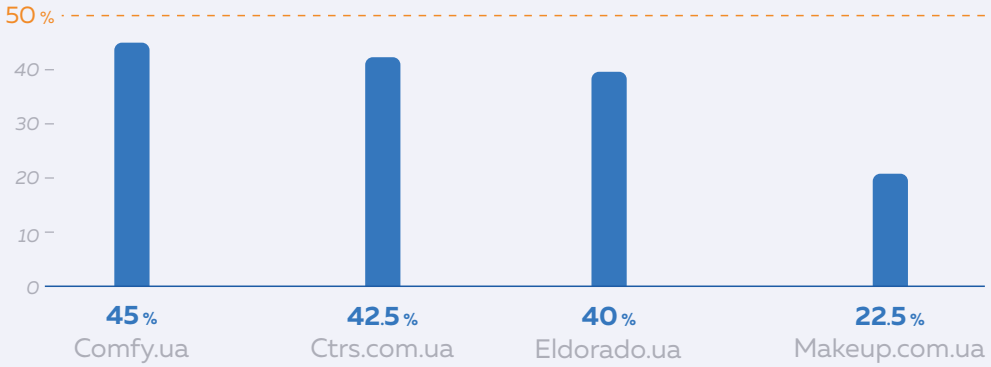
There is also room for Ukr.net to improve its policies, including providing users with the possibility to read previous versions of privacy policies on the site, explaining the data storage security in more detail, and indicating the geographical location of its servers (EU countries or Ukraine).

Ten out of 20 private companies in the websites category received at least 50% of the maximum number of points for the personal data protection criteria. There are two fewer companies in this list than in the previous 2021 survey. The project team assessed the corporate policies of these companies as average and above average in terms of ensuring the effective protection of their customers' personal data. These are Allo.ua, Prom.ua, Foxtrot.com.ua, Silpo.ua, Novaposhta.ua, Rozetka.com.ua, Kasta.ua, and Zakaz.ua, as well as the above-mentioned Olx.ua and Ukr.net.

Personal Data Protection Index 2023
Results for the sites

Ten out of 20 private companies received less than 50% of the maximum points for the personal data protection criteria. Compared to the 2021 study, there has been a regression, as previously only eight out of 20 private companies received scores below 50% of the maximum possible points. This indicates the possibility of significant gaps in personal data protection, as reflected in the companies' current corporate policies.

When assessing these ten out of 20 private companies, the researchers identified shortcomings in all four categories of the study: compliance with the national legislation, compliance with the European standards, to a lesser extent, technological aspects of website functioning, as well as website usability and inclusiveness.



The results of the study for the six telecommunications companies, as described in the Complete Methodology of the Study section, are not published due to martial law, but each of these companies will be informed of their assessment results.

This year, the project team also studied ten applications of private companies. They generally demonstrated better results in terms of personal data protection than websites, as 8 out of 10 applications received at least 50% of all possible points under the personal data protection criteria in accordance with the study methodology.

The greatest progress in assessments compared to the 2021 study can be seen among the following three private companies:

+ 32,5 %

Silpo.ua

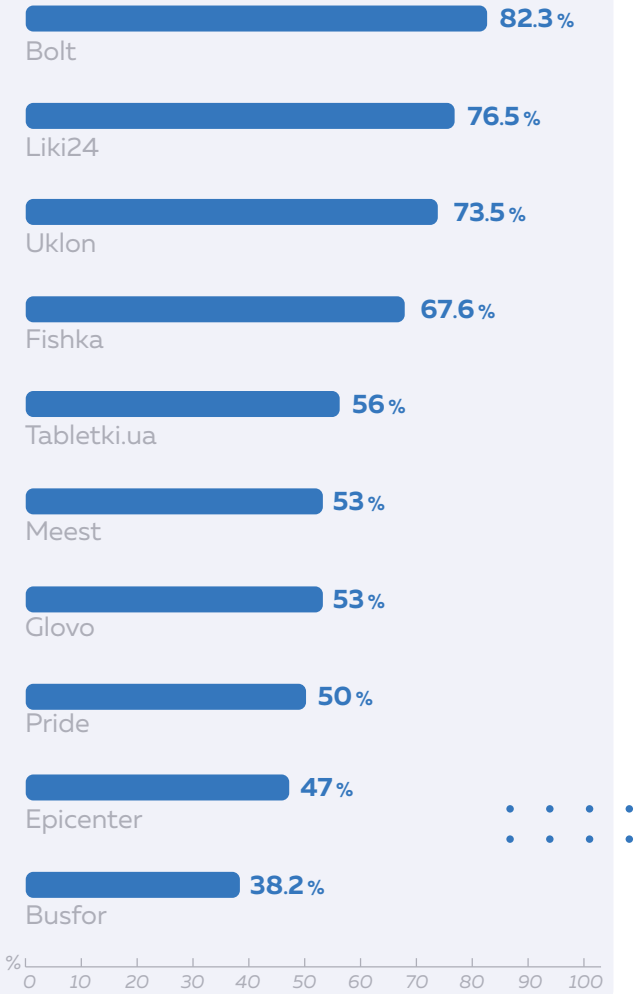
+ 22,5 %

Rozetka.com.ua

+ 15 %

Novaposhta.ua

Personal Data Protection Index 2023
Results for the applications



The highest scores were received by Bolt (82.3%), Liki24 (76.5%), and Uklon (73.5%). They were followed by Fishka (67.76%) and Tabletki.ua (56 %). At the same time, Bolt received 100% of the points in the compliance with European standards on personal data category, presumably because the company is an EU resident: its headquarters is located in Estonia. Liki24 and Uklon received 80% in the same category. At the same time, Liki24, Bolt, and Uklon scored high 80% in the compliance with Ukrainian legislation on personal data category, while Tabletki.ua is the leader in this category with 90%.

Epicenter (47%) and Busfor (38.2%) received the lowest scores among applications. Each of the companies represented by these applications had low scores, which affected the overall score, in two categories, compliance with European standards on personal data and technological aspects of the application. These results indicate significant room for improvement in the respective companies' policies and technological improvements in their applications.

We recommend that companies whose websites and applications have been evaluated within the framework of the Personal Data Protection Index 2023 should pay attention to the main aspects of their privacy policies to improve the following:

1. Adhere to the principle of data minimization – collect only the data about users that is necessary to provide their services.

2. Clearly and exhaustively specify what and how personal data is transferred to third parties.

3. Simplify the privacy policy by presenting it in a simple language accessible to the average user, devoid of legalese and overloaded semantic constructions.

4. Clearly indicate the duration, for which the company will retain user data. Some companies should reconsider the principle of 'keeping the data for life', which contradicts the principles of respecting users' digital rights.

5. Provide an option for users to view previous versions of the privacy policy to understand what innovations the company offers.

6. Explain to users the security of data storage and indicate the geographical location of the servers, which means not disclosing the specific location of the servers, but stating that the data is stored in the EU, Ukraine or other democratic countries.

As in the previous study, we suggest that all companies selected for the study should carefully review the results of the **Personal Data Protection Index 2023**, consult with the project team on the results obtained for each of the 30 companies, and make changes to their corporate privacy and personal data protection policies, involving lawyers in implementation of a plan to strengthen their privacy policies.

Detailed results of the study for the websites of 20 private companies can be found in the questionnaire, and for the applications of ten private companies – follow the link.

Authors of the Study

Tetiana AVDEIEVA

Tetiana is a lawyer at Digital Security Laboratory, a member of the Independent Media Council, and an expert of the Expert Committee on Artificial Intelligence Development under the Ministry of Digital Transformation of Ukraine. She graduated from the National University of Kyiv-Mohyla Academy with a degree in human rights. Tetiana is a co-organizer and judge of the international media law competition Price Media Law Moot Court Competition. Her professional interests include human rights, public international law and international humanitarian law, legal regulation of innovative technologies and the Internet.

Pavlo BIELOUSOV

Pavlo is a digital security expert at Internews Ukraine NGO, a consultant at DSS380 Digital Security School and Nadiyno.org Digital Security Hotline. He conducts digital security audits and training sessions for journalists, civil society activists, and government officials, covering topics such as protecting accounts from external threats, confiscation, loss of information, and setting up confidential communication in the online space.

Lidiia VOLKOVA

Lidiia is a lawyer specializing in human rights, international humanitarian, criminal, and media law. She has worked for various national and international organizations, including Internews Ukraine NGO and Global Rights Compliance. Lidiia received her law degree at the National University of Kyiv-Mohyla Academy.

The opinions expressed in this report are those of the author and do not necessarily reflect the views of the organizations for which she works

Vitalii MOROZ

Vitalii is a digital technology consultant at eQualitie Canadian technology organization, where he is responsible for the projects on the development of decentralized Internet in Ukraine. In recent years, he implemented projects related to advocacy for digital rights, Internet freedom, and the introduction of artificial intelligence technologies. Formerly: Manager of new media programs at Internews Ukraine. Vitalii graduated from the National University of Kyiv-Mohyla Academy and Emerson College in Boston as a Fulbright Scholar. He has delivered more than 500 training sessions and speeches on digital innovations, media literacy, and digital security. Vitalii is the author of various studies on technology.

Alina PRAVDYCHENKO

Alina is a lawyer specializing in media law and personal data protection, and an author of numerous publications on the subject. She is a graduate of the Annenberg-Oxford Media Policy Summer Institute and a member of the Committee on Media and Advertising Law of the Ukrainian National Advertising Association. Alina received her law degree at Donetsk National University.

ABA AMERICAN BAR ASSOCIATION
Rule of Law Initiative

INTERNEWS UKRAINE

internet freedom