



INDEX OF PERSONAL DATA PROTECTION 2021

A study of 20 leading Ukrainian tech companies regarding their respect for the digital rights of users in the context of personal data protection



Under the general editorship of:

Vitalii Moroz

Experts:

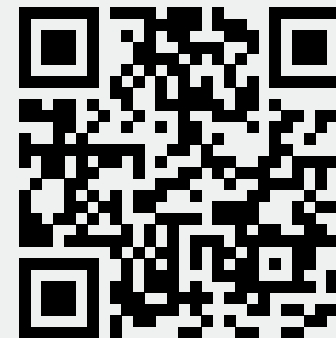
Tetiana Avdeieva
Pavlo Bielousov
Lidiia Volkova
Vitalii Moroz
Alina Pravdychenko

Project Manager:

Yuliia Babko

Design and layout:

Karina Strokan
Denys Baluba



This expert study was compiled by the NGO Internews Ukraine, with the support of the European Union and the International Renaissance Foundation within the framework «EU4USociety» initiative. Its content is the exclusive responsibility of the authors and does not necessarily reflect the views of the European Union and the International Renaissance Foundation.

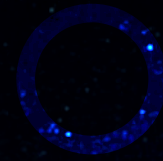
The **European Union** is made up of 28 Member States who have decided to gradually link together their know-how, resources and destinies. Together, during a period of enlargement of 50 years, they have built a zone of stability, democracy and sustainable development whilst maintaining cultural diversity, tolerance and individual freedoms. The European Union is committed to sharing its achievements and its values with countries and peoples beyond its borders.

The **International Renaissance Foundation** is one of the largest charitable foundations in Ukraine. Since 1990 we have been helping to develop an open society based on democratic values in Ukraine. During its activity, the Foundation has supported about 20 thousand projects, to which more than 60 thousand activists and organizations of Ukraine have joined. The funding amounted to over \$ 200 million. Site: www.irf.ua. Facebook: www.fb.com/irf.ukraine

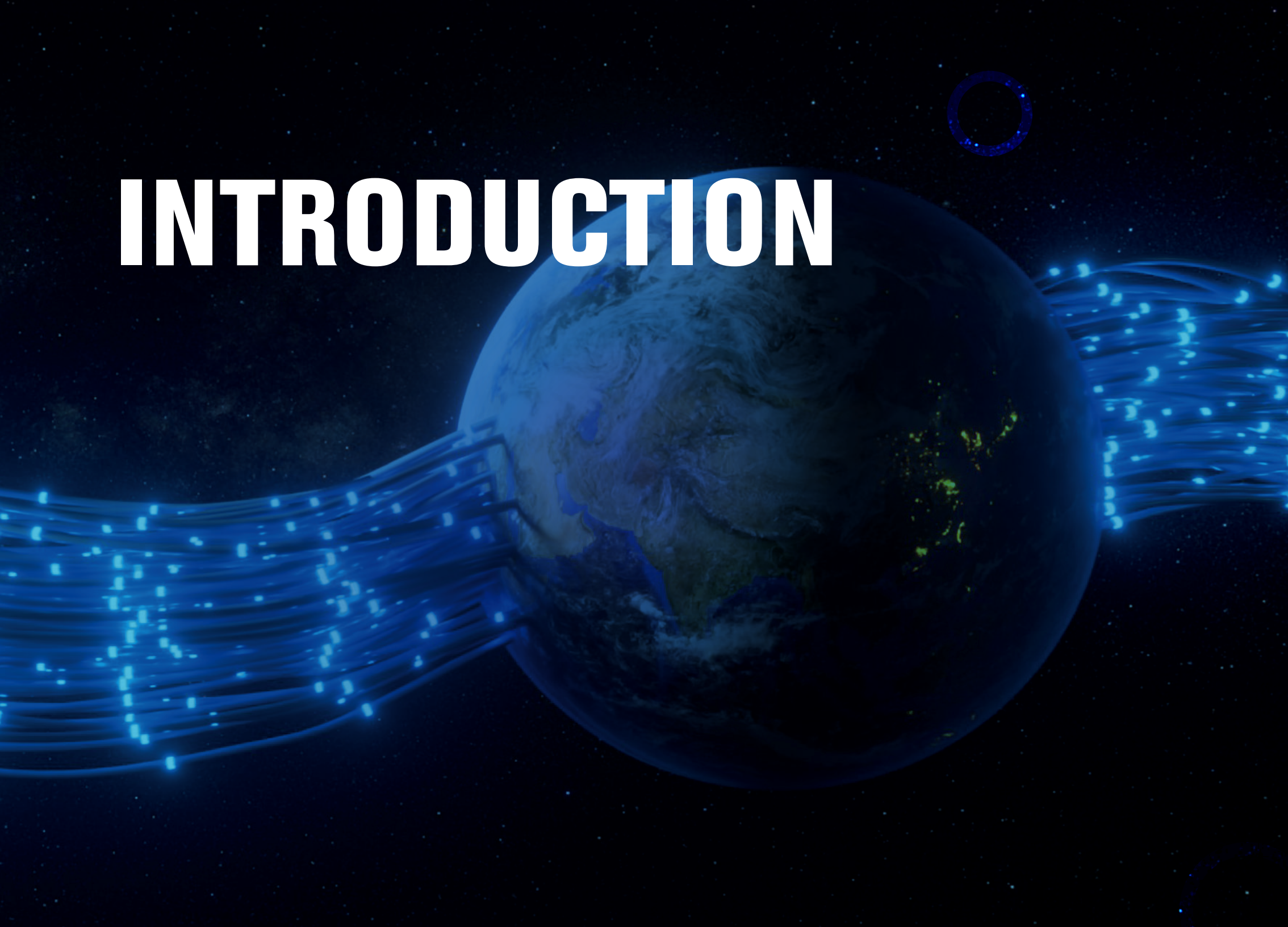
Internews Ukraine is an organization that has been operating on the media, communications, and consulting market since 1996. Website: www.internews.ua/. Facebook: www.fb.com/internewsukraine/

CONTENTS

Introduction.....	2
Summary of conclusions of the study.....	5
Overview of the study methodolog.....	9
Results of the study.....	11
Description of the study methodology.....	20
What will change for the private sector after adoption of Draft Law № 5628.....	27
Conclusions and recommendations.....	30
About the authors.....	33



INTRODUCTION



INTRODUCTION

The rapid development of digital technologies expands the field of legal relations among people in the online space, both around the world and in Ukraine. The process of establishing these relations on the Internet involves representatives of the private sector and governmental institutions. One of the trends during recent decades has been the active impacts of governments on the functioning of the online space. Oftentimes, governmental intentions to regulate relations in the online sphere provoke criticism from representatives of civil society and the private sector due to the risks for the Internet of keeping it free.

Meanwhile, another aspect of such regulation grows. Sustaining the relationships between all players in national legislation has to **guarantee implementation of the principles of protection of human rights in the online space**. This refers, among other things, to the sphere of privacy and protection of personal data: in the digital era, the scope of data and expansion of interactive tools are growing relentlessly.

Methods used for collecting and storing private information have gone through significant transformations and are different even for individual companies and organizations that accumulate and manage data from millions of users. Ukrainian users interact with the support of a considerable number of Internet technologies, and they receive online services both from the state and private sectors.

At the same time, many users give their consent to the policy of storing and managing their personal data without making an issue of it. While researching the *Index of Personal Data Protection*, the project team

raises the **question of digital rights from the perspective of an 'informed user'**. Do private companies create conditions for users' better understanding of their rights in the online space? Does the functionality of services provided by private companies include informed consent to be given by the users for processing their personal data? Does the corporate policy of private companies meet international standards for protection of human rights and Ukrainian legislation on personal data?

According to applicable Ukrainian legislation, private companies must comply with the **Law On Personal Data Protection** while interacting with users. The Law was adopted back in 2011 – at a time when attention to the online space was still not decisive, and the intensity of users' interactions was lower than it is today. At the same time, Ukraine is about to **adopt a new legislative initiative that will regulate the protection of personal data**. On June 7, 2021 draft law № 5628 on personal data protection was included in the agenda of the Verkhovna Rada of Ukraine. This draft law contains a significant number of provisions that will introduce efficient mechanisms for protection of users' personal data and harmonize national legislation with the European Union's approaches to personal data protection – these are the key conclusions of analysis of draft law № 5628 carried out by the NGO *Internews Ukraine* within the framework of the *Index of Regulation of the Online Space* presented in August 2021. Consolidated assessment based on the results of the study of draft law № 5628 totaled +0.87 on a scale from –5 to +5.

However, legislative amendments do not always guarantee changes in institutional behavior, while provisions of national legislation do not always reflect all the nuances of international human rights standards. It is precisely for this reason that the efforts aimed at raising awareness of digital human rights and expanding the range of their application are part of the projects implemented by civil society organizations in Ukraine.

The Index of Personal Data is, perhaps, the first study in Ukraine that **calls for wider discussion of policy and practice of respect for personal data of Ukrainian users by the private sector**. This study will make it possible to outline the key challenges related to protection of personal data of users, to which private companies are able to respond in the next few months. We believe that **cultivating respect for personal data at corporate policy level is a global trend among responsible business representatives. Therefore, Ukrainian private companies can join the initiative as well.**

During the first study carried out in the context of protection of users' digital rights in 2021, the **project team studied the websites of 20 large private companies in the sphere of telecommunications, provision of Internet access services, and online services in Ukraine**. The following companies/brands were included on the list:

Kyivstar JSC — [Kyivstar.ua](https://kyivstar.ua)

Lifecell LLC — [Lifecell.ua](https://lifecell.ua)

VF Ukraine PJSC, Vodafone Ukraine — [Vodafone.ua](https://vodafone.ua)

DATAGROUP PJSC — [DataGroup.ua](https://datagroup.ua)

TRIOLAN LLC — [Triolan.com](https://triolan.com)

LLC ROZETKA.UA — [Rozetka.com.ua](https://rozetka.com.ua)

UAPROM LLC — [Prom.ua](https://prom.ua)

EMARKET UKRAINE LLC / OLX Global BV — [Olx.ua](https://olx.ua)

UKRNET LLC — [Ukr.net](https://ukr.net)

NEW POST LLC — [NovaPoshta.ua](https://nova-poshta.ua)

COMFY TRADE LLC — [Comfy.ua](https://comfy.ua)

GROUP OF COMPANIES FOXTROT LLC — [Foxtrot.ua](https://foxtrot.ua)

ID ELDORADO LLC — [Eldorado.ua](https://eldorado.ua)

ZT-INVEST LLC — [Citrus.ua](https://citrus.ua)

ALLO LLC — [Allo.ua](https://allo.ua)

MAKEUP GLOBAL/MAKEUP TRADING LLC — [Makeup.com.ua](https://makeup.com.ua)

KASTA GROUP LLC — [Kasta.ua](https://kasta.ua)

SILPO-FOOD LLC — [Silpo.ua](https://silpo.ua)

ZAKAZ UKRAINE LLC — [Zakaz.ua](https://zakaz.ua)

LANET TELECOM LLC — [Lanet.ua](https://lanet.ua)



The goal of the *Index of Personal Data Protection* study is to **analyze companies' policies ensuring respect for the digital rights of users with the focus on personal data protection**. On the one hand, the study's results will help to identify which private Ukrainian companies can be included in a conventional category of '**champions of respect for the digital rights of users**'. On the other hand, the results will demonstrate which companies **should revise their corporate policies and ensure a greater focus on protecting users and their inalienable rights in the online space**.

When developing this study, the project team based its methodology on the methodology of **Ranking Digital Rights** – a globally recognized project developed by a U.S. non-governmental organization called *New America*. This methodology was adapted to the Ukrainian realities of the policy on protection of the digital rights of users.

SUMMARY OF CONCLUSIONS OF THE STUDY



Index of Personal Data Protection 2021*

*Out of 100%

77,50%

70,00%

70,00%

62,50%

60,00%

57,50%

57,50%

57,50%

52,50%

52,50%

Olx.ua

Ukr.net

Foxtrot.ua

Comfy.ua

Kyivstar.ua

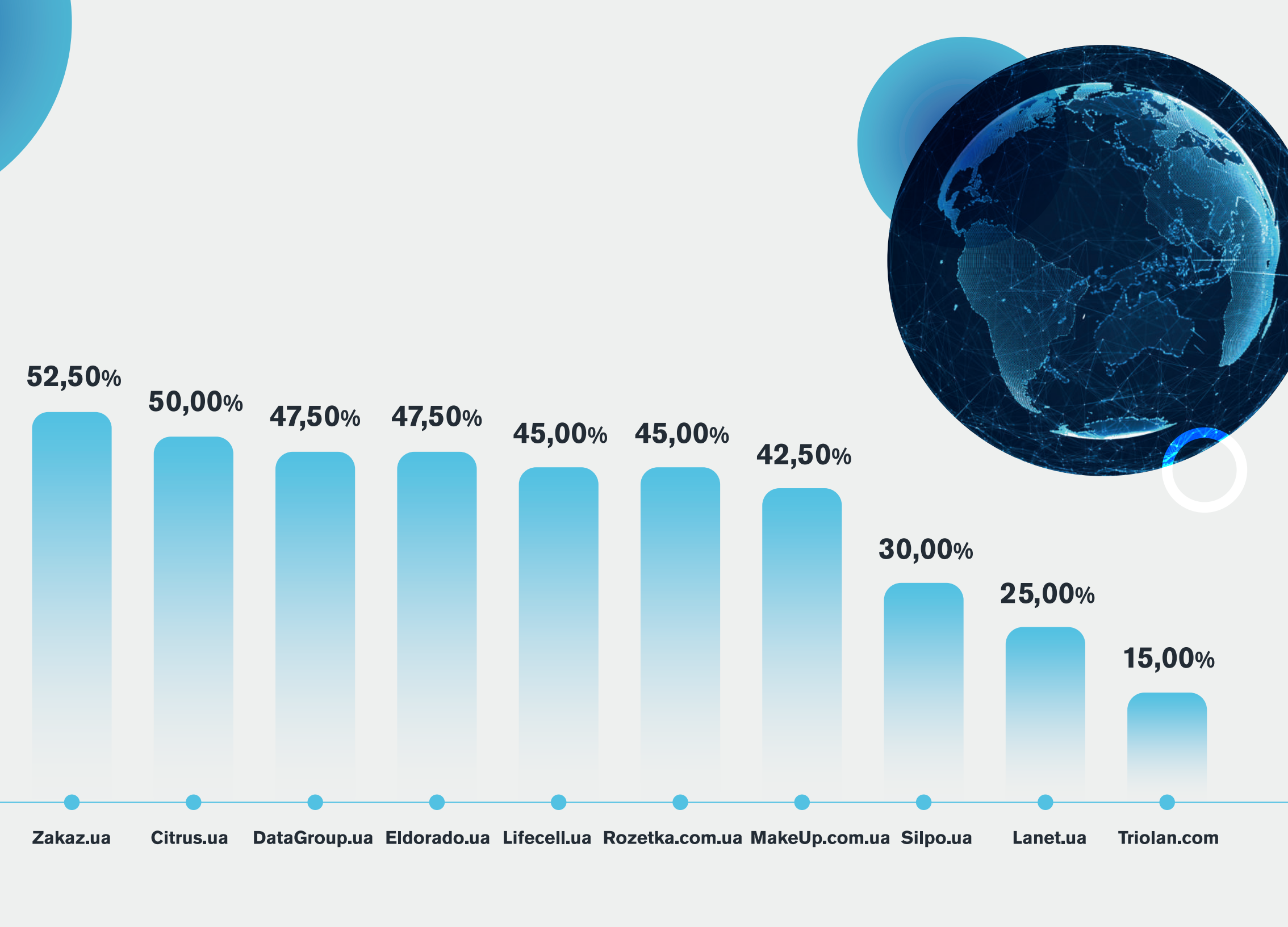
Prom.ua

Allo.ua

Kasta.ua

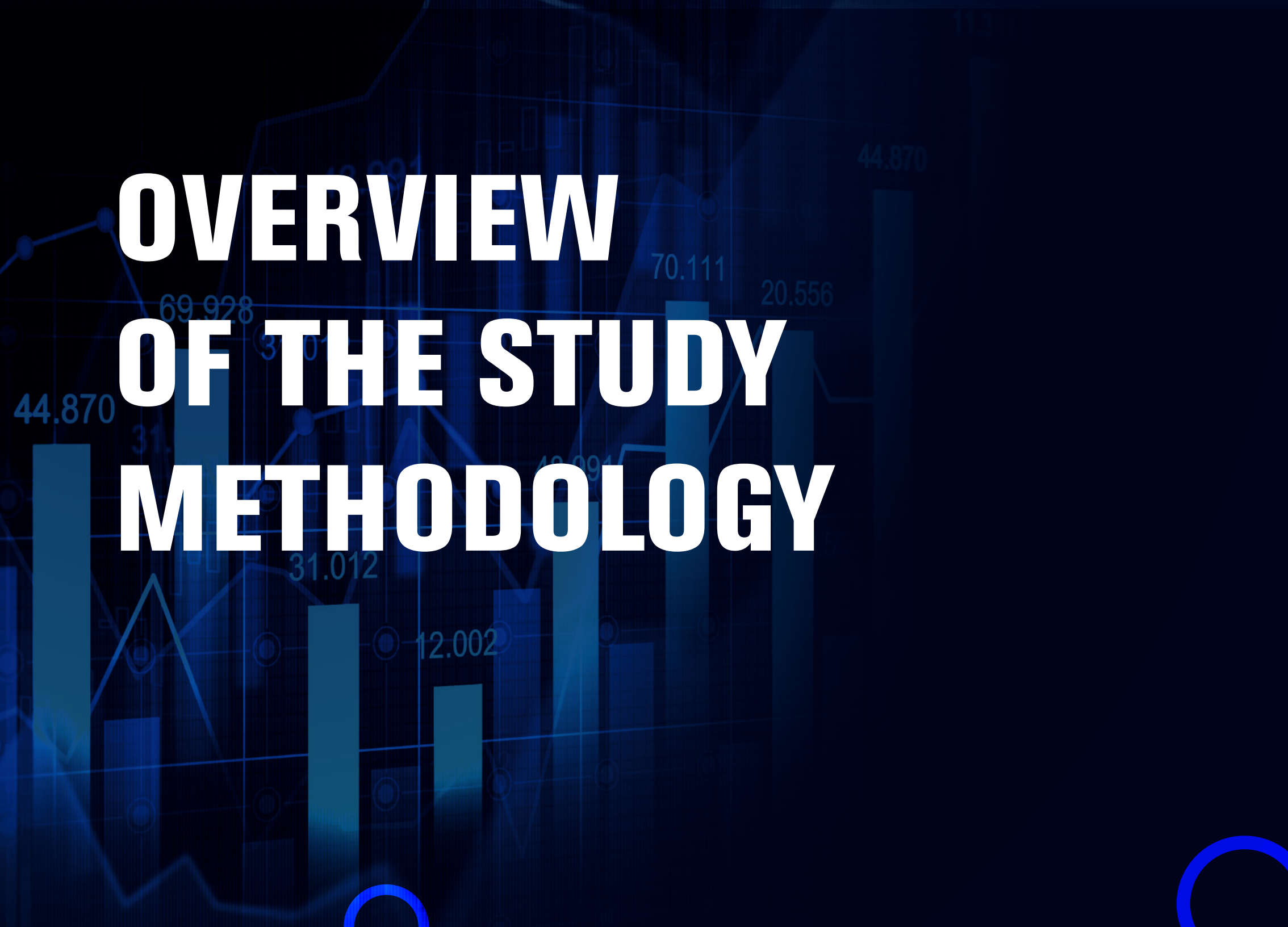
Vodafone.ua

NovaPoshta.ua



SUMMARY OF CONCLUSIONS OF THE STUDY

- The best results among the 20 companies were demonstrated by **Olx.ua, which received 77.5% as well as Ukr.net and Foxtrot.ua, both of which received 70% points out of the maximum possible 100%** reflecting the state of corporate policy on privacy and protection of users' personal data.
- At the same time, there is space for improvement even for Olx.ua, Ukr.net and Foxtrot.ua in terms of their corporate policy, in particular with regard to ensuring **adherence to the principle of minimizing the data** that they collect about users (Olx.ua), **publishing the previous versions of confidentiality policy on their websites** (Olx.ua, Ukr.net), providing a possibility for the users to **receive a copy of their personal data**, and specifying the **timelines for responding to requests from users** (Ukr.net).
- The minimum **50% of the maximum score was received by 12 out of 20 private companies with regard to the criterion of personal data protection**. The corporate policy of these companies is assessed as medium and above-medium level in the context of ensuring efficient protection of the personal data of their customers. These companies include **Kyivstar.ua, Comfy.ua, Allo.ua, Kasta.ua, Prom.ua, NovaPoshta.ua, Vodafone.ua, Zakaz.ua, Citrus.ua** as well as the above-mentioned **Olx.ua, Ukr.net and Foxtrot.ua**.
- These companies should pay more attention to **compliance with the principle of minimizing the data** they collect about users, **publishing the confidentiality policy in a simple and understandable** form on their websites, providing a clear description of the **process of data transfer to third parties**, etc.
- **8 out of 20 companies selected for the study received less than 50% of points** of the maximum score, which demonstrates a lower than medium level of personal data protection envisaged in corporate policy. These include **Eldorado.ua, DataGroup.ua, Lifecell.ua, Rozetka.com.ua, Makeup.com.ua, Silpo.ua, Lanet.ua, and Triolan.com**.
- The majority of the aforementioned companies have significant **shortcomings** in the four categories selected – **from compliance with the requirements of national legislation to user-friendly websites and inclusiveness**. The managers of these companies should consider revising the corporate policy on privacy and protection of personal data, develop and implement a plan on strengthening their confidentiality policy.
- The websites of **four companies** (Vodafone.ua, Silpo.ua, Triolan.com, Lanet.ua) **have no place to be marked by users for granting consent to the processing of their personal data**, although this is one of the requirements of the law.
- **10 companies do not inform their users about how long they will store data about users**.
- On the websites of **4 companies** (Triolan.com, Makeup.com.ua, Silpo.ua, Lanet.ua), **users have no possibility to delete their personal data**.
- **15 companies do not describe the conditions for deleting an account of the user** after termination of the contract/in the case when the account is not used.
- **10 companies do not specify where and how they store their users' data (location of servers)**.
- The results of the study for **each of 20 private companies** can be found in the questionnaire by clicking on the following link bit.ly/personaldataUA.



OVERVIEW OF THE STUDY METHODOLOGY

OVERVIEW OF THE STUDY METHODOLOGY

The purpose of the *Index of Personal Data Protection* study is to look into the corporate policy on accountability and transparency of leading companies in the private sector in Ukraine regarding their respect for digital human rights in the context of the right to privacy and culture of storing and maintaining the personal data of users.

Applied analysis and ranking is based on **work with open sources of data and official responses provided by private companies** regarding their policies on privacy and protection of personal data. The stages of field research and analysis include:

- collecting information from open sources about the corporate policies of companies, namely the **official websites of private companies**;
- wording and sending a **request for information** to private companies for clarifications on their privacy policy;
- developing a **questionnaire for evaluating the received information** that envisages classification of questions according to four research categories;
- **analyzing the data received and grading** it in accordance with the approved rating scale.

The project team focused on studying four key aspects of corporate policies of companies in the private sector:

- 1) compliance with the requirements of applicable Ukrainian legislation on personal data;
- 2) compliance with European standards on personal data;

- 3) technical aspects of the website's functioning;
- 4) user-friendly website and inclusiveness.

The study was based on documents publicly available on the official websites of companies. These documents can be accessed by any user. The researchers also studied the technical aspects of the official websites of companies.

In the first edition of the 2021 *Index of Personal Data Protection*, 20 large private companies operating in Ukraine were studied. These companies represent telecommunications, providers, and online services.

The project team developed an evaluation questionnaire to evaluate the corporate policy of the companies in accordance with the specified categories. **The questionnaire contains 20 questions.** Project experts assessed each indicator by selecting one of three possible grades:

- **0 point** means information is not available or it is not detected, which shows that the company ignores this aspect/fails to comply with the criterion of protection of digital rights;
- **0.5 point** was given when information is incomplete, which indicates partial disclosure of policy by the company in a specific aspect/partial compliance with the criterion of protection of digital rights;
- **1 point** means that information is available, comprehensive and understandable for the user/full compliance with the criterion of protection of digital rights.

Each indicator was graded by one of the experts. The received results for each indicator were then validated by the second and third expert. The results were corrected on the basis of information provided by the companies in response to an official request from the NGO *Internews Ukraine*. **The final scores (points) were compared against each other and deducted as a percentage (%) of the maximum number of points that could be scored by each company.**

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



RESULTS OF THE STUDY

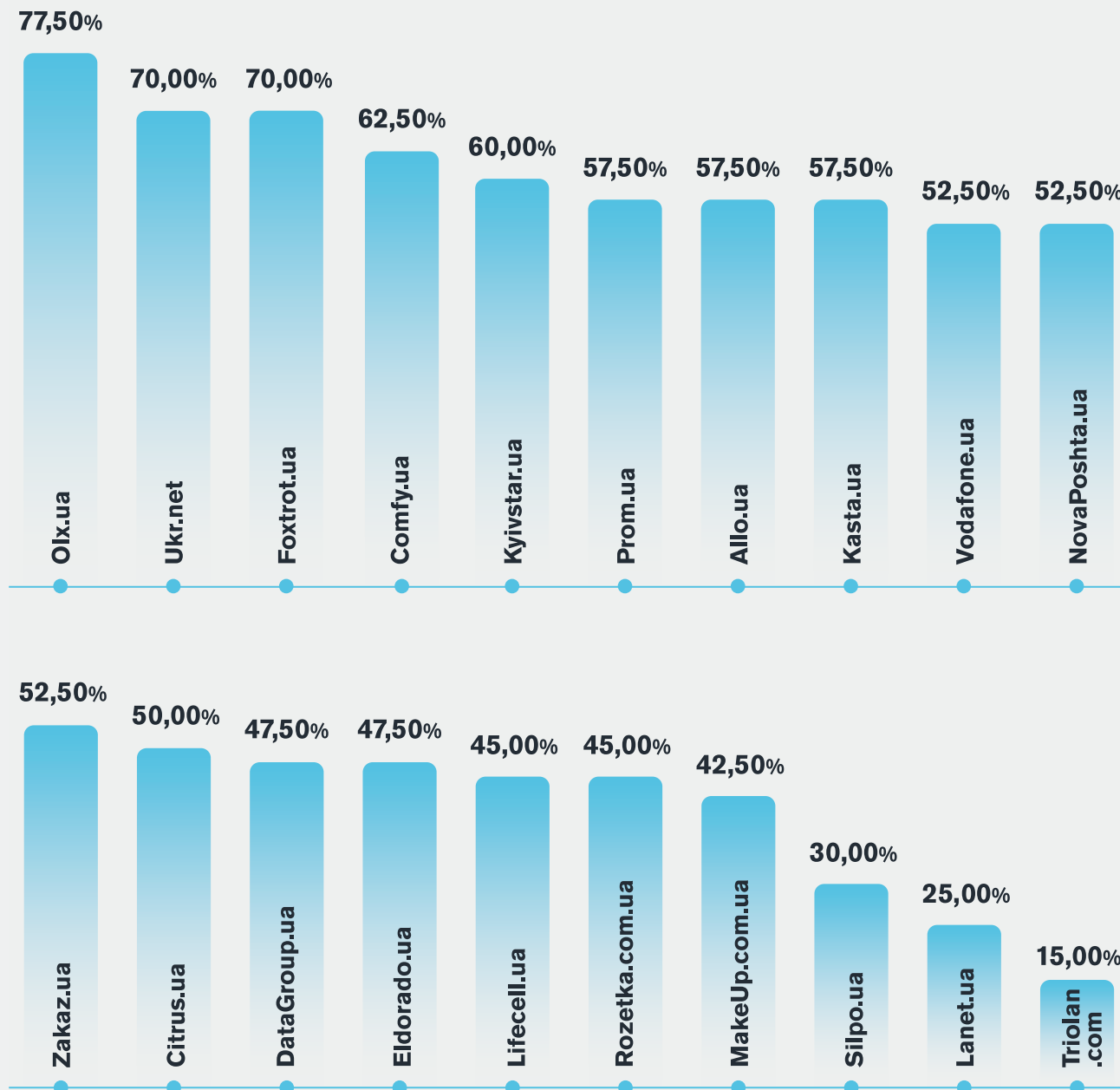


RESULTS OF THE STUDY

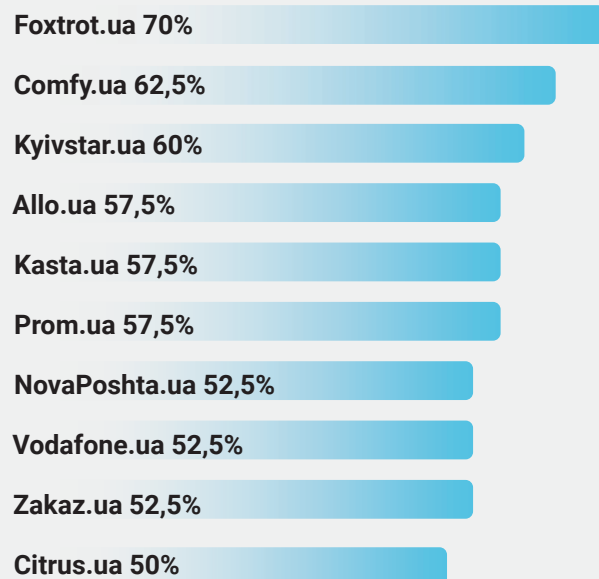
The consolidated results of the study on respect for the digital rights of users in terms of the policy on privacy and protection of personal data of private companies demonstrate that **the 'champions'** among the 20 companies selected for the study are **Olx.ua, Ukr.net and Foxtrot.ua**. They received the highest scores – **77.5%, 70% and 70% respectively**, out of a possible 100%, reflecting the state of their corporate policies on privacy and personal data protection.

For these three companies, improvements in corporate policies on privacy and personal data protection may be insignificant since the current policy design is in most aspects well thought-out and implemented. At the same time, there is room for improvement for Olx.ua in terms of adherence to the principle of minimizing the data they collect about users, and publishing the previous versions of their privacy policy on the website. For Ukr.net, informing users about the previous versions of its confidentiality policy and indicating the date of publication of the current version are also relevant. The company can specify the provisions on the possibility for users to obtain a copy of their personal data and indicate the time limits for responding to requests made by users in a clearer way.

In total, according to the study methodology, **12 out of 20 private companies comply with the criteria for personal data protection to at least 50% of the maximum score**. Consequently, the corporate policy of these companies was evaluated as medium and above medium level in the context of ensuring efficient protection of the personal data of their customers.



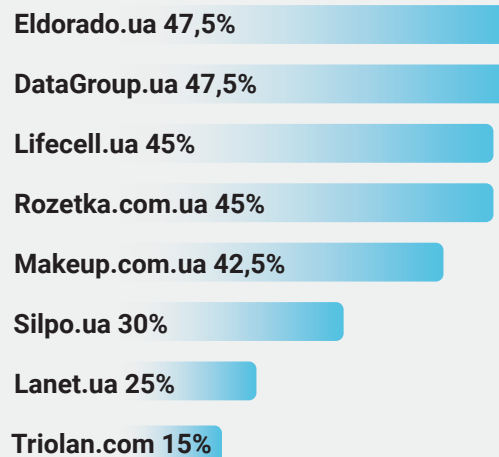
For 10 companies, the consolidated assessment varies from 50% to 70% of all possible points according to the criteria of personal data protection. They include:



Many of these companies should pay attention to the principle of minimizing the data they collect about users, publishing the confidentiality policy in a simple and understandable form on their websites. Online services that sell goods and services have to specify clearly how the data is transferred to third parties. Frequently, there is a lack of comprehensive information about secure storage of data on servers indicating the geographical location of these servers. Companies seldom inform their users whether they have developed internal policies/rules on processing and protecting personal data.

Eight companies did not get 50% of all possible scores for the criteria of personal data protection according to the study methodology.

These include:



The researchers mention that the majority of these companies have significant shortcomings in all four categories – from compliance with the requirements of national legislation to user-friendly website and inclusiveness. In particular, Lifecell.ua received extremely low scores in the category of *compliance with European standards*. On the Lifecell.ua website, the user cannot understand clearly that he/she gives consent to the processing of personal data. Instead of a clear description of the confidentiality policy, the company offers general terms of using telecommunication services on 39 pages. Neither does the company indicate whether it is possible to submit a request to the company and receive a copy of one's own personal data.

In its work, a popular online shopping service called Rozetka.com.ua does not specify how long it stores data about the user. At the same time, Rozetka.com.ua tries to get as many parameters as possible from the user, including 'I have a child', although these options are not required for providing services to the user.

Managers of these companies should revise their

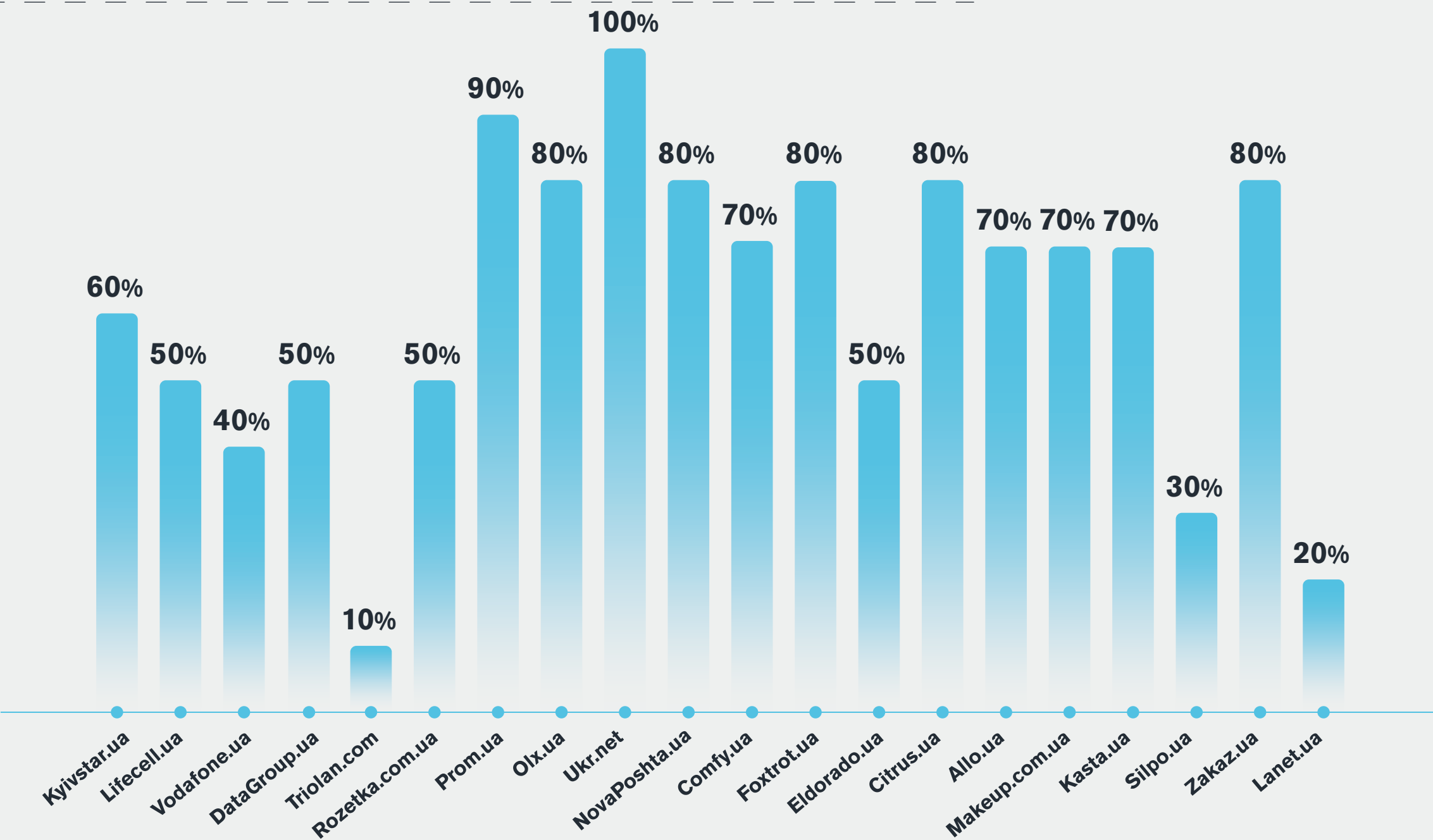
corporate policy on privacy and personal data protection, develop and implement a plan for strengthening the confidentiality policy.

Those companies that received the lowest scores should receive a specific mention. These are Triolan.com (15%), Lanet.ua (25%) and Silpo.ua (30%). Such figures demonstrate a lack of awareness on the part of these companies as to the importance of personal data protection, while their corporate policies on confidentiality and protection of personal data are least at the initial stage of implementation.

The assessment results that were submitted in the questionnaire by the researchers for each of the 20 companies can be found at bit.ly/personaldataUA.

More detailed results of the study can also be viewed with a breakdown into each of the four categories according to the study methodology (see more detailed description of the methodology on p. 21).

Category 1. Compliance with the requirements of applicable Ukrainian legislation on personal data



Results in Category № 1 Compliance with the requirements of applicable legislation

In this category, the majority of companies received higher scores compared to other categories. There is a quite logical explanation for this – each of the companies works in the legal field of Ukrainian legislation and takes into account the need to comply with the provisions of regulatory documents.

In the first category, Ukr.net received 100% of possible scores, and Prom.ua – 90%. NovaPoshta.ua, Olx.ua, Citrus.ua, and Zakaz.ua scored 80%. A slightly lower score – 70% – was received by four other services: Foxtrot.ua, Makeup.com.ua, Allo.ua and Comfy.ua.

Low scores indicating partial non-compliance with the requirements of applicable legislation by companies in the sphere of personal data protection were received by Triolan.com (10%), Lanet.ua (20%) and Silpo.ua (30%). These companies should consider carrying out a critical review of their policies on privacy and data protection and reconcile them with valid legislative requirements.

Under Category № 1, the researchers studied the companies with regard to specific research questions, including:

- Is there a mark on the website for the user to grant permission for processing his/her personal data?
- Does the company inform users about which information is collected about them, and how it is used?
- Does the company specify the period, during which it will store data about the user?

- Can users delete their personal data stored on the website at their own discretion?
- Does the company adhere to the principle of data minimization, which corresponds to the purpose of processing this data?

Results in Category № 2 Compliance with European standards

Although European standards on human rights, namely regarding personal data protection, are not mandatory for companies operating in Ukraine, the European Regulation (GDPR) applies to the territory of other countries if there is interaction with EU citizens. Many Ukrainian companies adapt their corporate policies with regard to GDPR provisions, which Ukrainian legislators looked to when developing the new draft law № 5628 on personal data protection. It is expected that members of the Verkhovna Rada of Ukraine will adopt the draft law in the fall of 2021.

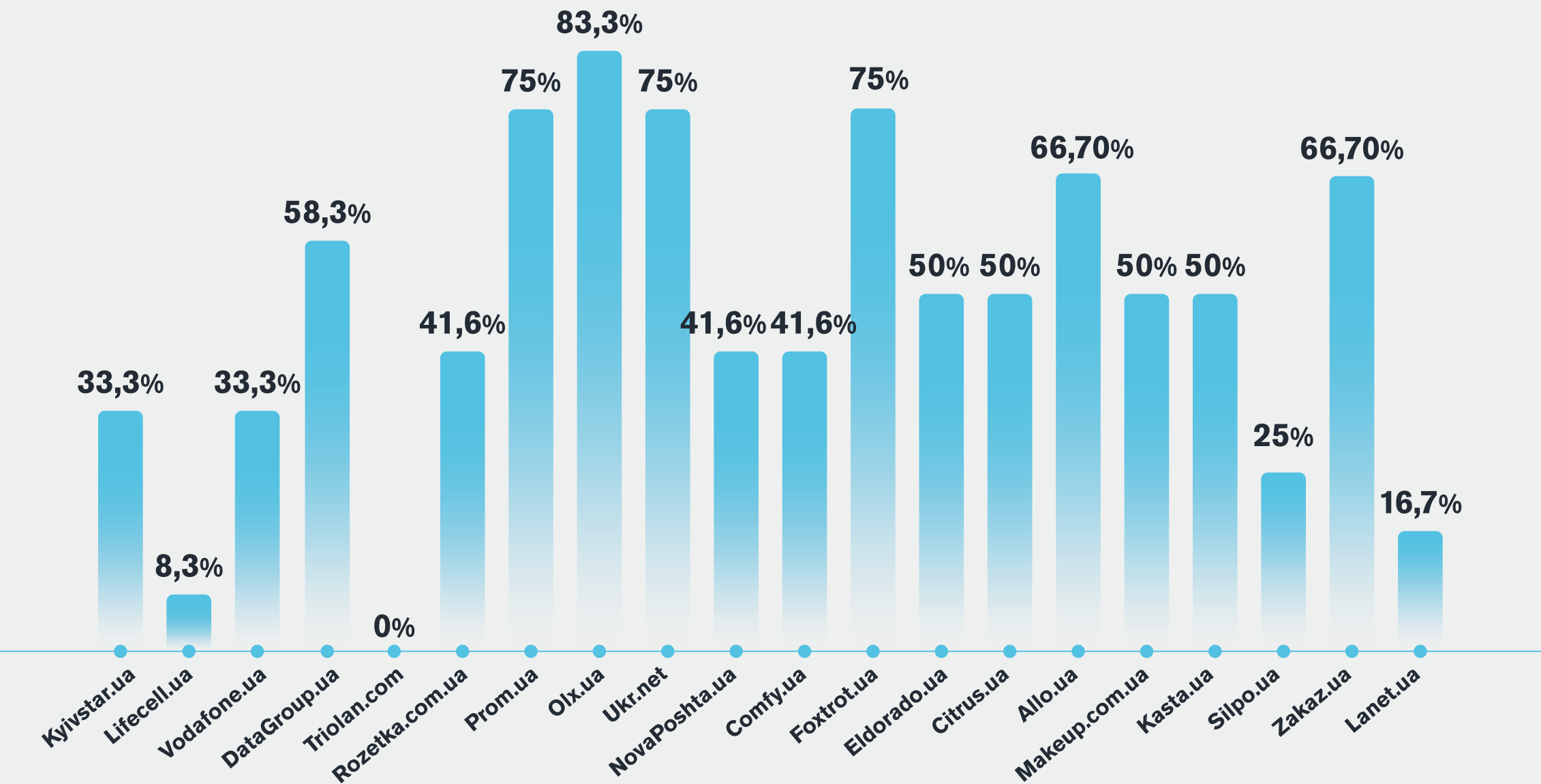
In general, the majority of the companies studied did not receive the maximum possible scores in this category, while some services got extremely low scores. The highest points were given to Ukr.net (83.5%), Olx.ua and Prom.ua (75% each).

Extremely low points were given to Lifecell.ua (8.3%), Lanet.ua (16.7%), and Silpo.ua (25%). The provider Triolan did not receive any points in this category (0%).

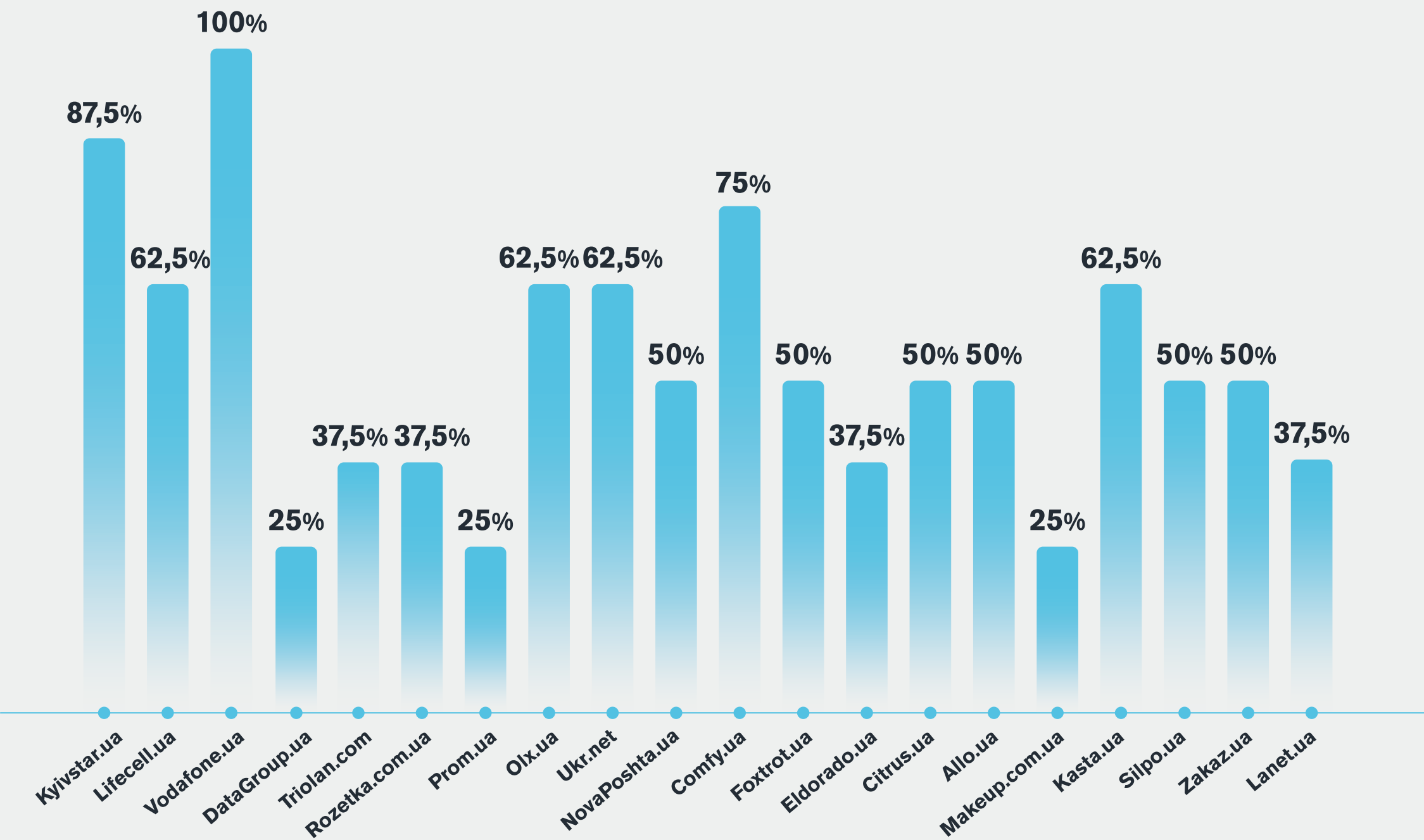
Under Category № 2, the researchers assessed the companies with regard to specified research questions, including:

- Does the functionality of the website make it clear to the user that he/she gives consent to the processing of his/her personal data?
- Is information about the privacy policy provided on the website concise, transparent, clear, and easy to understand?
- Can the users find previous versions of the confidentiality policy on the website together with amendments to the updated version of the confidentiality policy?
- Does the company describe the terms of deleting the user's account after termination of the contract/when the account is not used?
- Does the company explain how the user's data is transferred to third parties?
- Can the user submit a request to the company and receive a copy of his/her personal data?

Category 2. Compliance with European standards on personal data



Category 3. Technical aspects of the website's functioning



Results in Category № 3 Technical aspects of the website's

Based on the results of the study, corporate policy on safe use of the website is a priority for such companies as Vodafone.ua (100%), Kyivstar.ua (87.5%) and Comfy.ua (75%) – users' interactions and their personal data are, in the main, protected.

The worst scores were received by DataGroup.ua, Makeup.com.ua and Prom.ua –25% each, and this requires companies to enlist technical specialists for eliminating the problems related to the lack of enhanced protection from unauthorized access (such as two-factor authentication during login) and informing about the safe storage of user data (servers).

Under Category № 3, the researchers studied the companies with regard to specified research questions, including:

- Does the company use the secure https connection protocol for the website?
- Where and how does the company store user data?
- Is the option of enhanced protection against unauthorized access available to users?
- Can users view and manage authorizations on the website, when and from where the user's account was accessed?

Results in Category № 4 User-friendly website and inclusiveness

Ease of use and inclusiveness characterize the design thinking of companies that offer their websites to users for interaction.

According to the research results, the best indicators were demonstrated by Olx.ua, which scored 80%. Four companies – Kyivstar.ua, Lifecell.ua, Comfy.ua, and Foxtrot.ua – received 70% each.

The lowest score was received by the food delivery service Zakaz.ua (10%). It is followed by three companies that scored 20% – Makeup.com.ua, Citrus.ua and Triolan.com.

Under Category № 4, the researchers studied the companies with regard to specified research questions, including:

- Can the users find information on the website quickly and easily about personal data protection?
- Can the user review the company's internal policy/rules regarding the handling of their personal data and its protection?
- Does the company provide information about the time limits for responding to requests by users regarding personal data?
- Can the user get answers to his/her requests from the company through the help desk using at least two means of communication (hotline, email, chatbot)?
- Does the company provide possibilities for people with disabilities to use the website?

How were these results obtained?

The results of this study were obtained on the basis of collecting information from open data sources (official websites of the companies) and the company's official responses to formal requests. During the first stage, the project team identified the list of companies to be studied and monitored the official websites of

companies.

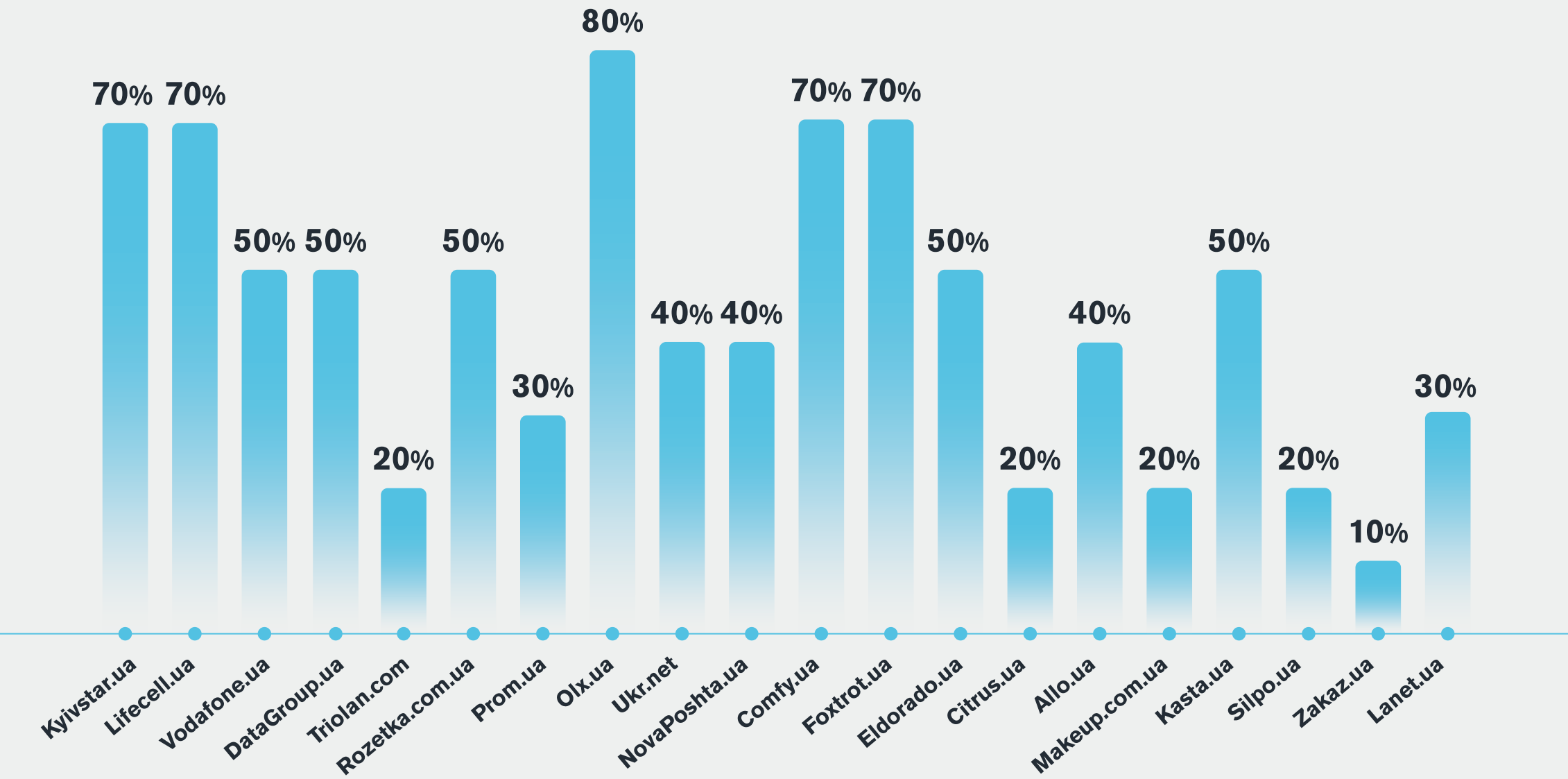
The project's experts collected information about corporate policies after studying the official websites of companies. Then they analyzed the data obtained, graded it (gave it scores) and, finally, validated the results received (questionnaire).


In order to adjust received results, the project team prepared and sent official requests for information from the NGO *Internews Ukraine* to the companies with clarifying questions about their policies on privacy and personal data protection. The requests were sent to the official mailing addresses of companies and forwarded to the company's official e-mail addresses, as taken from open sources.

Within 40 days of these requests being sent, the team of researchers received approximately 30% of responses – only 8 out of 20 companies had provided answers as of the end of June 2021. Responses were provided by the following companies: Olx.ua (EMARKET UKRAINE LLC), Prom.ua (UAPROM LLC), Vodafone.ua (VF UKRAINE PJSC), Kyivstar.ua (Kyivstar JSC), NovaPoshta.ua (New Post LLC), Silpo.ua (SILPO-FOOD LLC), Comfy.ua (COMFY TRADE LLC) and Lifecell.ua (Lifecell LLC). The remaining 12 companies probably did not answer the requests since the project team did not receive their responses within 40 days of the date when the requests were sent out.

The study results reflect the policies of companies on privacy and personal data protection as of July 2021 – the data analysis period.

Category 4. User-friendly website and inclusiveness



The background features a close-up of a hand reaching out, with a blue tint. Overlaid on the hand are various digital and technical icons: a bar chart in the upper left, a circular progress indicator in the upper right, a loading bar with the word 'LOADING' in the lower right, and several small person icons connected by lines, suggesting a network or data flow. The overall aesthetic is futuristic and technological.

DESCRIPTION OF THE STUDY METHODOLOGY

DESCRIPTION OF THE STUDY METHODOLOGY

The *Index of Personal Data Protection* is a tool for looking into the corporate policy of leading companies working in the private sector in Ukraine with regard to their respect for the digital rights of users in terms of personal data protection. The study was carried out by NGO *Internews Ukraine* and involved experts on digital technologies and lawyers. Tetiana Avdeieva, Pavlo Bielousov, Lidiia Volkova, Vitalii Moroz, and Alina Pravdychenko were members of the project's working group.

Subject matter of the study

Corporate policy on the accountability and transparency of leading companies operating in the private sector in Ukraine with regard to their respect for the digital rights of users.

Objective of the study

To examine the corporate policy on accountability and transparency of leading companies of the private sector in Ukraine with regard to their respect for digital human rights in terms of the right to privacy and culture of storing the personal data of users and its disposal.

Key methods of the study

The study is based on applied analysis and ranking resulting from work with open sources of data and official responses provided by the companies. The stages of field research and analysis were:

- collecting information about the companies' corporate policies from open sources, namely the official websites of private business companies;

- preparing and sending a request for information to private business companies for clarifications on their privacy policy;
- developing a questionnaire for evaluating the received information, which envisages classification of questions according to four research categories;
- analyzing the received data and grading it in accordance with the approved rating scale.

Evaluation criteria according to the methodology of the study

The project team focused on studying four key aspects of corporate policies of private sector companies:

1. Compliance with the requirements of applicable Ukrainian legislation on personal data. It was assessed on the basis of the following criteria:

- the company provided a possibility for the user to put a mark for granting consent for processing of their personal data;
- the company provided a possibility for a user to know what information is collected about him/her, and how it is used;
- the company specified the period, during which information about the user is stored;
- the company provided a possibility through the website for the user to delete the stored data about him/her;

- the company observes the data minimization principle.

2. Compliance with European standards on personal data. It was assessed based on the following criteria:

- the user understands clearly that he/she grants consent for the processing of personal data;
- information about the confidentiality policy has to be presented to the user in a concise, transparent, understandable and easily accessible form using clear and simple language;
- the company includes an option for the user to read the previous versions of the confidentiality policy and amendments to the updated version of the confidentiality policy;
- the company describes the terms of deleting the user's account after termination of the contract/when the account is not used;
- the company provides an explanation on how the user's data is transferred to third parties;
- the company provides a possibility for users to submit requests for receiving a copy of their personal data.

3. Technical aspect of the website's functioning. It was assessed based on the following criteria:

- the company envisaged the use of the secure https connection protocol in the website's functioning;
- the company provided server hosting in countries without repressive legislation on the Internet, where access to data is protected by law;
- the company provided a possibility for a user to have enhanced protection from unauthorized access to the user's virtual cabinet;
- the company provided a possibility for a user to view the history of their visits, when and from where the user's cabinet was accessed.

4. User-friendly website and inclusiveness. It was assessed based on the following criteria:

- the user can find information about personal data protection on the website in a fast and convenient way;
- the user can review the company's internal policy/rules regarding the handling of their personal data and its protection;
- the user can receive a response from the company to their requests submitted through the help desk;
- the company provides information about the time limits for responding to requests related to personal data from users;
- the company provides possibilities to people with disabilities to use its website.

In order to assess the corporate policies of companies with regard to the specified criteria, the project team developed an evaluation questionnaire. The questionnaire consists of 20 questions. The project

experts graded each point by selecting one of three possible scores:

- **0 point** means information is not available or it is not available/not detected, which demonstrates that the company ignores this aspect/fails to comply with the criterion for protection of digital rights;
- **0.5 point** was given when information is incomplete, which indicates partial disclosure of policy by the company in a specific aspect/partial compliance with the criterion of protection of digital rights
- **1 point** means that information is available, comprehensive and understandable for the user/full compliance with the criterion on protection of digital rights.

Criteria used to select companies for the study

In total, during the first stage of the project carried out in 2021, we selected 20 companies for the study, which were divided into two groups: the first group included six companies represented by mobile operators and providers. The second group are 14 companies that provide services to their users with the help of electronic services with or without registration on their websites. Such division of companies is explained by the specific nature of provision of services to users and the amount of personal information collected and disposed of by these companies.

Key criteria for selecting companies in the first group (telecom):

- companies provide services to users related to mobile communication/access to the Internet;
- companies are market leaders and have official websites with information on their usage policies;

- companies collect personal data for identifying the users.

Key criteria for selecting companies in the second group (service companies):

- the basis of commercial activities of companies is formed by the functioning of the website, through which services are provided/goods are sold to users;
- companies' websites are the most popular among Ukrainian users based on the results of research, in particular and in accordance with the results of the Kantar CMeter study as of February 2021;
- users have to be registered on companies' websites by sharing their personal data in order to be able to use services provided by the company, or services are provided without registration but the sharing of personal data is nevertheless required.

Where does the data for the study come from?

The study becomes possible by analyzing the huge mass of data collected. The data was received from open sources (official websites of the companies) and in the form of responses by companies to official requests made by the researchers. Failure to receive official data or the absence of data was taken into consideration in the process of preparation of the study's conclusions.

There were two key ways to receive data:

- 1) collecting and analyzing information from open sources through monitoring of official websites of the companies operating in the private sector;
- 2) preparing and sending a request for information to private business companies asking for clarifications

as to their policies in the privacy sphere. The requests were prepared in accordance with the requirements of Ukrainian legislation and sent out by mail. Copies of the same requests were also sent to the official e-mail addresses of companies. The project team waited for responses from the companies for 40 days from the time the request was sent.

How did the study team work?

The study team's members consisted of six specialists in digital technologies and lawyers. The project team was responsible for adaptation of the study methodology, implementation of the filed stage, analysis of the results based on received data, and presentation of the project's outcomes.

The project team was formed within the framework of the project *Transparent Reporting in the Telecommunications Sphere: Protecting Ukrainian Users' Privacy* implemented by the NGO *Internews Ukraine* with support from the International Renaissance Foundation and the European Union under the joint initiative EU4USociety.

How were the study results validated?

The project team used a double expert method (peer review) of assessment of the received results. One of the experts scored (graded) the answers, and then the second and third experts validated the results. The results were then corrected with regard to information received from the companies in response to the official request submitted by the NGO *Internews Ukraine*. The final scores (points) were compared and the percentage (%) of the maximum score received by each company was calculated.

What does the final product of the study look like?

The complete text of the study, together with the summarized conclusions published in the form of a report on a dedicated website of the project, are publicly available online, and they were also forwarded to each of the private companies studied.

Questions included in the questionnaire for evaluating the companies

The project team developed a questionnaire consisting of 20 questions that were divided into four key categories. Based on the results of responses to each question, the experts selected one of three possible scores:

- **0 point** means information is not available or it is not available/not detected, which demonstrates that the company ignores this aspect/fails to comply with the criterion of protection of digital rights;
- **0.5 point** was given when the information is incomplete, which indicates partial disclosure of policy by the company in a specific aspect/partial compliance with the criterion on protection of digital rights;
- **1 point** means that information is available, comprehensive and understandable for the user/full compliance with the criterion on protection of digital rights.

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

1. Is there a mark on the website for the user to grant permission for the processing of his/her personal data?

2. Does the company inform the user about which information is collected about him/her, and how it is used?
3. Does the company specify the period, during which it will store data about the user?
4. Can the users delete their personal data stored on the website at their own discretion?
5. Does the company adhere to the principle of data minimization, which corresponds to the purpose of processing this data?

Compliance with European standards on personal data (6 questions):

1. Does the functionality of the website make it clear to the user that he/she gives consent to the processing of his/her personal data?
2. Is information about the privacy policy provided on the website in a concise, transparent, clear, and easy to understand way?
3. Can users find previous versions of the confidentiality policy on the website together with amendments to the updated version of the confidentiality policy?
4. Does the company describe the terms of deleting the user's account after termination of the contract/when the account is not used?
5. Does the company explain how the user's data is transferred to third parties?
6. Can the user submit a request to the company and receive a copy of his/her personal data?

Technical aspects of the website's functioning (4 questions):

1. Does the company use the secure https connection protocol for the website?
2. Where and how does the company store the user's data?
3. Is the option of enhanced protection against unauthorized access available to users?
4. Can users view and manage authorizations on the website, when and from where the user's account was accessed?

User-friendly website and inclusiveness (5 questions):

1. Can users find information quickly and easily on the website about personal data protection?
2. Can the user review the company's internal policy/rules regarding the handling of their personal data and its protection?
3. Does the company provide information about the time limits for responding to requests from users regarding personal data?
4. Can the user get answers to his/her requests from the company through the help desk using at least two means of communication (hotline, email, chatbot)?
5. Does the company provide possibilities for people with disabilities to use the website?

Explanation of Evaluation Criteria

What do we understand by 'adherence to the requirements of applicable legislation of Ukraine on personal data'?

1. **Availability of the user's consent** is the vital precondition for processing his/her personal data. The *Law On Personal Data Protection* (Article 2) defines consent as a voluntary expression of will by an individual (provided such person was duly informed) to grant consent for processing their personal data in accordance with the specified purpose of such processing, stated in written form or in a form that makes it possible to make a conclusion on granting of the consent. In the e-commerce sphere, the consent from the subject of personal data can be granted during registration in the information and telecommunication system of the e-commerce actor through a mark **on granting consent** for personal data processing in accordance with the specified purpose of such processing, **provided that the respective system does not process personal data until the respective field has been marked**. In other words, the key aspect during evaluation of this component is, in our opinion, the active actions of the user for granting consent, and the impossibility to use the service without such actions. In fact, the issue here is about it being impossible to receive services without pressing certain buttons/making respective marks. Under such evaluation conditions, the entity receives 1 point, and for partial compliance of these criteria – 0.5 points.
2. The key right of the subject of personal data is the right to **know, which information is collected about him/her, and how it is used**. At the same time, the

law clearly stipulates that information about the holder of personal data (i.e. not only about the site that collected personal data, but about a specific individual or legal entity), about the composition and contents of the personal data collected, the rights of a user of the resource, the purpose of collection of personal data and the individuals to which personal data is transferred, has to be provided at the moment when personal data is collected (Article 12 of the Law of Ukraine *On Personal Data Protection*). All the aforementioned issues are usually specified in the confidentiality policy that is provided to a user for information together with a possibility to grant consent for personal data processing. In view of this, the evaluated entity receives 1 point if it has the confidentiality policy on its website with all the described aspects and provided that the user reads this policy before providing his/her personal data. If the entities meet these criteria in part, they receive 0.5 point.

3. **The company has to specify the period of data storage**. Ukrainian legislation sets out special requirements for the timelines for processing/storing personal data. Personal data is processed in a form that allows identification of an individual, to which they refer, for **no longer than it is necessary for legitimate purposes, for which it was collected or further processed** (Article 6 of the Law of Ukraine *On Personal Data Protection*). Termination of the period for storing the data specified in the consent of the personal data subject for processing such data or in the law constitutes grounds for deleting the data (Article 12). Therefore, it is extremely important to specify the period of data storage, and it should be mentioned on the company's website. Accordingly, 1 point is received by the companies

that directly specify the period of storing data about the user, 0.5 – if the period is not specified clearly or hidden on the website, and, 0 – if it is not mentioned.

4. The Law *On Personal Data Protection* clearly stipulates **that consent for personal data processing can be withdrawn at any time** (Article 8). In practice, this means that technically the system provides a possibility to delete personal data (there should be the respective button/option on the interface)/a description of a transparent mechanism for deleting personal data or at least a contact address, to which a request for deleting personal data can be sent. This being said, 1 point is given to those subjects whose services contain direct and unambiguous possibilities for deleting personal data (respective buttons or instructions), and 0.5 point is given to the entities whose services provide a possibility to delete data upon request.
5. The company complies with the **principle of minimizing the data**, whereby the composition and contents of collected personal data should be relevant, adequate, and not excessive with regard to the specified purpose of their processing. One of the legislatively established principles for personal data processing is its minimization. For instance, **the structure and contents of personal data should be relevant, adequate and not excessive with regard to the specified 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 mentioned in the user agreement (confidentiality policy) and related directly to the provision of the services offered. This means that any company has to collect only that data from users which is necessary for the

provision of services, without asking for excessive information. In view of this, the evaluated entity receives 1 point in the case of complete compliance with the minimization principle, and 0.5 point in the case of partial compliance.

What is understood here when we talk about 'compliance with European standards on personal data'?

Ukrainian legislation on personal data protection is currently undergoing transformation. One of the reasons for this is an aspiration to meet European standards, more specifically the GDPR – General Data Protection Regulation, which came in force in the European Union in 2018. This Regulation strengthens the rights of users to a large extent, first of all through the principles of simplicity and understandability. As of today, the GDPR is not mandatory for application on the territory of Ukraine, but since many Ukrainian companies can provide services to European users, as well as noticeable steps by Ukraine on the way to European users, as well as in view of Ukraine's significant steps toward European integration, it would be quite reasonable to assess the extent to which Ukrainian companies are user-friendly and compliant with European standards.

1. One such standard is the **clear consent standard**. According to Article 7 of the GDPR, if the state subject's consent is given in the context of a written declaration that also concerns other matters, the request for consent shall be presented in a manner, which is clearly distinguishable from other matters, in an intelligible and easily accessible form. This means that the **user must understand clearly that he/she agrees to the processing of their personal data**, and the option for granting

such consent must be separated from all other possible actions (for example, with the help of a separate button, making a special mark, etc.). At the same time, statements like "By ticking the 'Confirm order' button I consent to the processing of my personal data" or "By continuing to use this website, you consent to the processing of your personal data" do not comply with this standard since they are not clearly separated from other matters or actions. Similarly, the automatically marked space on granting consent does not comply with the standard because the user can remove it, and it can go unnoticed by the user.

2. **Confidentiality policies** of many Ukrainian websites **are usually written in legal parlance that is difficult to understand**. However, the GDPR sets standards for informing users about the use of their personal data. According to Article 12, information on the privacy policy has to be provided to the user in a **concise, transparent, understandable and easily accessible form**, in particular information that is purpose-written for a child. In other words, the point is that an average user who is not a lawyer or a specialist in the sphere of personal data protection should be able to easily understand who will use the data about him/her and how.
3. The company should provide an option for users to review the **updated (versions of) privacy policy**. This allows the user to compare changes that the company introduced to the personal data policy and, if necessary, to exercise his/her right to withdraw consent to its processing.
4. If the need for personal data no longer exists in terms of the purposes, for which it was collected or otherwise processed, the **personal data must**

be deleted without any unjustified delays (Article 17 GDPR). Termination of the contract or non-use of the account for a long time may, in some cases, indicate that the purpose of collecting personal data is no longer relevant, and hence the grounds for processing such data are also absent. That is why it is important as to **whether the company described the terms of deleting the user's account after termination of the contract/when the account is not used**.

5. The company has the right to **transfer the user's data to third parties subject to the user's consent**. When the personal data is received, the user has to be informed about the recipients or categories of recipients of personal data (Article 13 GDPR). Furthermore, the GDPR regulates in detail the conditions for transferring the data to a third country or an international organization. Therefore, **explaining the process of transferring the user's data to third parties** is considered to be quite important.
6. **The subject of personal data has the right to receive copies of the processed personal data** (Article 15 GDPR). Accordingly, the subject is able not only to know about the list of such data, but also clearly see the entire array of data that is processed. Large international platforms provided such an option to their users several years ago.

What do we understand by 'technical aspects of the website's functioning'?

Users' interaction with the websites of companies envisages **protection of the user from possible harmful influences and information leakage**. Contemporary standards of protection of websites and their services

become a necessity, and they have to be reflected both in the architecture of the technical component of a company's work and in the work of the websites. Furthermore, the websites should provide technical protection features at the user level.

Therefore, the basic criteria of the technical component include the possibility to visit websites that **function on the basis of the secure https connection protocol** using a TLS-certificate. **The company's servers should be located in countries** without repressive legislation on the Internet, where access to data is protected by law to minimize the risks of unauthorized access to information on these services and, accordingly, to the personal data of users.

At the level of users' control over their data, responsible companies **provide a possibility to users to view the history of visits** and see when and where they accessed their account. To protect the user from unauthorized access to their account, the company has to **provide enhanced protection** (for example, the two-factor authentication option (2FA), authorization via sms or authorization by IP-address) when logging in to a personal account.

What do we understand by 'user-friendly website and inclusiveness'?

The user-friendliness, or usability, of the website responds to the **user's need to find necessary information quickly and easily**, so the links to such information should be available on the first page of the website and visible against the background of other content on the website. Companies can give emphasis to personal data protection in the following ways:

- publishing **reference information** about personal data protection on the website;

- developing and implementing the company's **internal policy/rules on handling personal data** and its protection;
- providing information about the **time limits for examination of requests** related to personal data;
- providing a possibility for users to **contact the company through a help desk** in several ways that are convenient for the user, such as hotline, email or chatbot. Using the services and, accordingly, the website requires taking into account the interests of people with disabilities. In order to ensure compliance with the principle of inclusiveness in the organization of the company's activities, **services should be provided to people with disabilities (such as people with visual or hearing impairments) in a convenient and accessible form**. More specifically, companies should provide a possibility to contact the operator or chatbot in a voice format, have a separate version of the website or application for people with disabilities if the company's services cannot be provided without such a version.

The companies should also place a disclaimer on the availability of such versions so that the users know about the possibility of using additional (special) functionality. Any discriminatory provisions against people with disabilities should be avoided in the formulation of the company's policy, and inclusiveness should be promoted in every possible way.

WHAT WILL CHANGE FOR THE PRIVATE SECTOR AFTER ADOPTION OF DRAFT LAW № 5628

WHAT WILL CHANGE FOR THE PRIVATE SECTOR AFTER ADOPTION OF DRAFT LAW № 5628

On June 7, 2021 draft law № 5628 on personal data protection was registered in the Ukrainian Parliament. Representatives of civil society organizations, international partners, as well as representatives of the private sector started to talk about the need to adopt it. What should the private sector expect if this draft law is adopted?

First of all, all **standards for personal data protection will be reconciled** with the requirements of the EU General Data Protection Regulation (known as the GDPR). In practice, this means that EU-registered companies and Ukrainian services will have to comply with the same requirements. At the same time, those consumers who have to provide their personal data to receive a service will have more guarantees and protection against abuse. In particular, the draft law details the procedure for obtaining consent, and establishes a mechanism for protection against automatic decision-making. This will impose an additional obligation on companies regarding the functioning of websites. For instance, so-called cookie banners will have to be organized properly, and the fields for granting consent will no longer be marked in advance, so the person will have to do this on their own (in accordance with the case law of the EU Court of Justice on *Verbraucherzentrale Bundesverband eV v Planet49 GmbH*).

Second, companies will have a wide range of **responsibilities to verify compliance of personal data processing procedures with international standards**

in the human rights sphere (in accordance with the case law of the ECtHR regarding protection of privacy on *M.L. and W.W. v Germany*). This will have to be done in cases of systematic and large-scale analysis of the personal aspects of lives of individuals (in the form of automatic processing, including profiling), processing of sensitive data or monitoring of public places or sources. In addition to this, the controller will have to appoint a person responsible for personal data protection with guarantees of the impossibility of his/her dismissal for providing assessment of the level of data protection. In this way, the companies will have to at least create a separate staff unit that will take care of personal data protection.

Third, innovations in the draft law also include **development of codes of conduct on personal data protection**, which will consist of a set of rules, standards and procedures for industries, sectors or specific organizations. Such codes can be common for several entities or individuals for each organization. In fact, this is a manifestation of self-regulatory and co-regulatory mechanisms, and it will contribute to better introduction of the standards: business representatives will have a better understanding of how their product or service functions, and thus will be able to organize the data protection procedure in the best way without compromising the quality of services.

The draft law also proposes regulations for **protection of personal data in the labor sphere that will limit**

the possibility of employers interfering excessively in employees' privacy. Among the important aspects, one should mention the prohibition to use sensitive personal data for purposes other than assessment of the person's professional competencies. A separate provision also regulates the possibility to use the data for internal investigation. In particular, it is specified that if such an investigation yields negative results, the employer must delete the data, which is completely in line with the case law of the ECtHR on *López Ribalda and Others v Spain*. The data must be stored until expiry of the period of limitation.

Furthermore, the draft law obliges the data controller, including business representatives – to **inform the subject of personal data in the event of leakage.** The document proposes three exceptions here: the controller took sufficient technical and organizational safeguards; the controller took measures to prevent risks for the subject's rights; such notification creates an excessive burden for the controller. Although these exceptions are quite controversial in view of their all-embracing nature, introduction of the general rule will, nonetheless, impose new obligations for the controller of personal data.

An important aspect for the controllers is also the **time limits for examining requests submitted by citizens.** Pursuant to Article 27 of the draft law, the subject can submit a request to the controller demanding implementation of his/her rights envisaged by law. At the same time, the controller has to make a decision

immediately, but no longer than within one month from the date of receiving the request. If the issue relates to **sensitive data, the controller has to examine it within 10 days**. Respective requests may relate to both withdrawal of consent to data processing, and implementation of the right to be forgotten. Therefore, companies will have sufficient time for examination of a complaint or a demand from their customers or service users.

For controllers that were established or operate abroad, the draft law envisages introduction of an obligation **to appoint their representative in Ukraine** if the company uses the personal data of Ukrainian users. Conditions for implementation of this requirement include systematic processing of personal data by companies, as well as the presence of one of the following factors:

- 1) the controller processes the personal data of Ukrainian citizens;
- 2) personal data processing is related to offering works, services or good to persons in Ukraine;
- 3) personal data processing is related to monitoring the behavior of subjects on the territory of Ukraine.

In addition to this, the draft law proposes a **significant increase in sanctions both for individuals and for legal entities that violate the legislation** on personal data protection. In the event of violation, companies will have to pay a fine of **up to 150 million hryvnias**. By comparison: the highest fine envisaged in the GDPR totals 20 million Euros (more than 640 million hryvnias).

Thus, private companies can expect a significant number of procedural novelties, as well as a

potential change of internal standards and partial reorganization in the way they handle the personal data of the users of their services.

CONCLUSIONS AND RECOMMENDATIONS

CONCLUSIONS AND RECOMMENDATIONS

The results of the first *Index of Personal Data* study give grounds for **moderate optimism regarding the state of the corporate culture of privacy and protection of personal data in large tech companies in Ukraine** as of July 2021. Less than half of the 20 companies (more specifically, eight) that were selected for the study demonstrated consolidated **results below 50% of the maximum possible score**.

At the same time, in view of the growing role of tech companies under the conditions of rapid development of digital space, **the need to protect the personal data of users is growing**. Today, it is **big data** that constitutes **the most valuable asset in the world**, where the leaders in the private sector are those who are able to accumulate and analyze large masses of data with the help of artificial intelligence and machine learning. Among Ukrainian tech companies, **there are already some leaders whose role and influence** on forming legal relations and introducing 'rules of the game' in the online space will grow constantly in the future. We suggest that all companies that were selected for this study **should read the results of the Index of Personal Data Protection carefully, discuss the suggested amendments with the project team, and update their corporate policies on confidentiality and protection of personal data**.

- The best results among the 20 companies **were demonstrated by Olx.ua, Ukr.net and Foxtrot.ua, which received 77.5%, 70% and 70% points, respectively**, out of the maximum possible 100% as a reflection of the state of their corporate policies on

privacy and protection of the personal data of users.

- However, even for Olx.ua, Ukr.net and Foxtrot.ua **there is space for improvement in terms of their corporate policies**, particularly with regard to **adherence to the principle of minimizing the amount of user data** that is collected (Olx.ua), publishing the previous versions of the confidentiality policy on their websites (Olx.ua, Ukr.net), providing a possibility for users **to receive a copy of their personal data**, and indicating the **time limits for responding** to requests by users (Ukr.net).
- **At least 50%** of the maximum possible score was received by **12 out of 20 private companies** under the criterion of personal data protection. **The corporate policies of these companies are evaluated at the medium and above medium level** in the context of ensuring efficient protection of the personal data of their users. These companies are **Kyivstar.ua, Comfy.ua, Allo.ua, Kasta.ua, Prom.ua, NovaPoshta.ua, Vodafone.ua, Zakaz.ua and Citrus.ua** as well as the above-mentioned **Olx.ua, Ukr.net and Foxtrot.ua**.
- The aforementioned companies should pay attention to adherence to **the principle of minimizing the data** they collect about users, **publishing their confidentiality policy in a simple and understandable form** on their websites, providing a clear description in the policy of the **method of data transfer to third parties**, etc.
- 8 out of the 20 companies selected for the study scored under 50% of the maximum possible points under the criteria of personal data protection. These

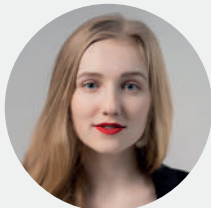
include **Eldorado.ua, DataGroup.ua, Lifecell.ua, Rozetka.com.ua, Makeup.com.ua, Silpo.ua, Lanet.ua and Triolan.com**.

- The majority of these companies have significant **shortcomings in all four categories – from compliance with the requirements of national legislation to a user-friendly website and inclusiveness**. Managers of these companies should consider revising their corporate policy on privacy and personal data protection, develop and implement a plan on strengthening the confidentiality policy.
- Websites of **four companies** (Vodafone.ua, Silpo.ua, Triolan.com, and Lanet.ua) **have no place to be marked by users for the granting of consent to the processing of personal data**, although this is one of the requirements of the law.
- **10 companies** do not inform their users **about how long they will store information about users**.
- On the websites of **4 companies** (Triolan.com, Makeup.com.ua, Silpo.ua, and Lanet.ua), users **have no possibility to delete their personal data**.
- **15 companies** **do not describe the conditions for deleting an account** of the user after termination of the contract/in the event when the account is not used.
- **10 companies** do not specify **where and how they store the data of users** (location of servers).
- If we group the companies according to the principles

of provision of services, then among the three key operators, **Kyivstar.ua and Vodafone.ua received 60% and 52.5% of the maximum score, respectively**, under the criterion of implementation of the corporate policy on privacy and personal data protection. At the same time, **Lifecell.ua received 45%** of the maximum score (see details below).

- Under the categories *Technical aspects of the website's functioning, User-friendly website and inclusiveness*, Lifecell.ua received rather high scores – 62.5% and 70%. At the same time, the company should pay attention to the following aspects of its confidentiality policy: places should be added on the Lifecell.ua website to be marked by the user for granting permission for his/her personal data to be processed, and a confidentiality policy should be developed and published on the website in addition to the available 39-page long terms and the procedure for providing telecommunication services. The user should also be provided with the possibility to receive a copy of his/her personal data by submitting a request to the company.
- **Among the group of providers** that were selected for the study, **all companies were ranked below average** under the criterion of implementation of corporate policy on privacy and personal data protection – **DataGroup.ua (47.5%), Lanet.ua (25%) and Triolan.com (15%)**. The two latter companies should make efforts to improve their confidentiality policies with the help of lawyers, and to then implement them.
- The results of the study for **each of the 20 private companies** can be found in the questionnaire by clicking on the following link bit.ly/personaldataUA.

AUTHORS OF THE STUDY



Tetiana Avdeieva

A lawyer on media law and manager of a project on artificial intelligence at the Center for Democracy and the Rule of Law (CEDEM), and a lawyer of the Independent Media Council. A graduate of the National University of Kyiv Mohyla Academy, majored in human rights. Co-organizer and referee of international legal contests on media law, Price Media Law Moot Court Competition. Tetiana's professional interests include human rights, international public law and international humanitarian law, legal regulation of innovative technologies and the Internet.



Alina Pravdychenko

A lawyer specializing in media law and personal data protection, and author of numerous publications on this topic. She is a graduate of the Annenberg-Oxford Media Policy Summer Institute, a member of the Committee on Media and Advertising Law of the Ukrainian National Bar Association. Alina majored in law at Donetsk National University.



Vitalii Moroz

A consultant on digital technologies helping organizations and media outlets implement strategies and innovative approaches in the digital space. In recent years, Vitalii worked as Head of new media programs at the NGO *Internews Ukraine*, where he was responsible for development of educational and advocacy projects, including free Internet advocacy projects in Ukraine, and the Digital Security School 380. Vitalii received his MA at the National University of Kyiv Mohyla Academy and Emerson College in Boston as a student of the Fulbright Program. He has delivered more than 500 training sessions, speeches on digital innovations, media literacy, and digital security. Vitalii is also the author of research papers on technologies.



Pavlo Bielousov

Expert on digital security of the NGO Internews-Ukraine, consultant of the Digital Security School DSS380, expert of the TrollessUA project. Pavlo delivers training sessions on digital security for journalists covering the topics of protection of accounts from external threats, confiscation, data loss, setting up confidential communication on social networks, search and identification of so-called FB-trolls.



Lidiia Volkova

A lawyer specializing in human rights, international humanitarian, criminal and media law. Lidiia has experience of working with various national and international organizations, including the NGO Internews Ukraine, Global Rights Compliance, etc. She received a legal education at the National University of Kyiv Mohyla Academy.

