

## **Privacy policy**

Telewizja Polska S.A. (TVP) respects and observes the Users' right to privacy. Below one can find information relevant to Users on how information about the Users of the tvp.pl portal (Portal) is collected, processed and used, and how TVP cares about the protection of personal data of the Portal Users, using appropriate technological solutions.

All terms used in this document will have the meaning given to them in the Regulations for the provision of electronic services by Telewizja Polska S.A. on the tvp.pl Portal.

Version as of: January 21, 2021

### **I. Personal data protection policy**

#### **Processing of personal data of the Users of the tvp.pl Portal**

Personal data is any information relating to an identified or identifiable natural person. All personal data is collected and stored on the tvp.pl portal in accordance with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and the repeal of Directive 95/46 / EC, the General Data Protection Regulation (GDPR), the Act of July 16, 2004, Telecommunications Law and the Act of July 18, 2002, on the provision of electronic services.

Registration in the Portal is not obligatory, which means that the provision of personal data is voluntary, while providing the User's email address is necessary to register the User Account and use the Newsletter service. In order to facilitate the use of some of the services available on the Portal, the forms offered on the dedicated pages may indicate other personal data the provision of which is necessary in order to use the service offered on the Portal. For this purpose, the User agrees to the processing of personal data for the purpose of using certain services, which means that the legal basis for processing is art. 6 sec. 1 point a GDPR. The data provided is protected against access by third parties and used by TVP only for contacts with Users, necessary as part of the performance of a given service.

#### **The scope of data**

For the purposes of providing services on the Portal, Users' personal data are processed, in particular: e-mail address, name, surname, postal code, telephone number, country of origin, RTV subscriber number. In addition, on the Portal we also collect information contained in system logs (e.g. IP address) and in cookies (more on this subject in the Cookies Policy). They are used for technical purposes related to the administration of our servers. IP addresses are also used to collect general statistical demographic information about visitors to the Portal.

#### **Personal data controller**

The administrator of the personal data of the Portal Users is: Telewizja Polska Spółka Akcyjna, with its registered office in Warsaw, at ul. Woronicza 17, 00-999 Warszawa, entered into the Register of Entrepreneurs of the National Court Register under KRS number 0000100679 kept by the District Court for the capital city of Warsaw, 13th Commercial Division, tax identification number NIP 521-04-12-987, share capital fully paid up in the amount of PLN 286 596 500.00.

### **Purpose of processing personal data**

Users' personal data is collected, stored and used by TVP and TVP Trusted Partners and IAB Partners, with the consent of the persons they concern or based on the legitimate interest of the administrator, in accordance with the law and in compliance with due procedures and in a manner that guarantees their safety. TVP may use personal data only to ensure proper service to Users, for the purposes of providing Services, reporting complaints, withdrawing from the contract for the provision of Services and communicating with Users who have submitted a complaint or submitted a declaration of withdrawal from the contract for the provision of Services, and for marketing purposes, analytical and statistical purposes described in more detail in the Cookies Policy.

### **Legal basis for the processing of personal data**

The legal basis for the processing of personal data of the Portal Users is primarily the consent given by the User - art. 6 sec. 1 letter a) GDPR. The User's consent may be withdrawn at any time, which does not affect the lawfulness of the processing of personal data before its withdrawal. Personal data may also be processed to a limited extent on the basis of the legitimate interest of TVP consisting in the proper provision of the Portal service - art. 6 sec. 1 letter f) GDPR.

If the User gives his consent, personal data may be transferred to third countries for which the European Commission has not found an adequate level of protection, which in the absence of appropriate safety measures may be associated with a possible risk. The data transfer then takes place on the basis of Art. 49 sec. 1 letter a) of the GDPR - User's express consent.

Telewizja Polska always tries to secure each data transfer to third countries using the security measures indicated in the GDPR, in particular through the use of standard contractual clauses approved by the European Commission, which oblige the recipient of the data to ensure an adequate level of personal data security.

### **The period of personal data processing**

Users' personal data are processed by TVP for the period of the Portal service and / or until the voluntary consent is withdrawn by the User. These periods may be extended only if it is necessary to investigate, establish or defend against possible claims.

### **Users' rights related to the processing of their personal data**

The User has the right to access and correct their personal data provided to TVP as part of the User Account service (after undergoing the procedure of verifying the User's identity, consisting in entering the password), in the "MY DATA" tab. Complete deletion of the e-mail address is tantamount to deletion of the User Account, which requires selecting the "Delete Account" option in the User Account. Complete deletion of the e-mail address provided as part of the Newsletter service requires connecting to the TVP website using the internet address (the so-called "link") at the end of each message sent as part of the service.

Each User who has consented to the processing of his personal data in order to use the services available on the Portal, may contact TVP directly with a request to access his data, correct it, delete it, limit processing or object to the data being processed, and also take advantage of the possibility of data portability.

In order to exercise the rights regarding the processing of personal data, each person whose data is processed as part of the provision of services on the Portal, may contact the Data Protection Officer at the e-mail address [rodo@tvp.pl](mailto:rodo@tvp.pl), as well as by traditional mail at Telewizja Polska SA ul. J. P. Woronicza 17, 00-999 Warsaw, with a note "to the Data Protection Inspector".

The user also has the option to lodge a complaint with the supervisory authority competent for the protection of personal data.

For security purposes, if you suspect that the User Account may have been breached, e.g. by unauthorized access to the login and password used to log in to the Portal, please immediately contact the Portal's administrative staff at the e-mail address [pomoc@tvp.pl](mailto:pomoc@tvp.pl).

### **Recipients of personal data**

TVP transfers the Users' data obtained on the Portal only to Trusted TVP Partners and IAB Partners who use the data with consent and for the purposes specified by the User. Lists of TVP Trusted Partners and IAB Partners are available in Advanced Settings. The data provided to partners concerns only information obtained with the use of cookies or other similar technologies, and each User may independently decide to whom and for what purpose their data will be transferred from the Advanced Settings level.

For technical reasons, TVP may entrust the processing of users' personal data, pursuant to Art. 28 GDPR, to another entity under a contract or other legal instrument without changing the above-mentioned purposes of their processing. In such a situation, the data entrusted for processing will be processed by third parties on behalf of TVP and only for the purposes specified by TVP.

Consent to use data for some of the Trusted Partners of TVP and IAB may be related to the transfer of data to the United States or other third countries (not belonging to the European Economic Area, which includes the Member States of the European Union as well as Norway, Iceland and Liechtenstein). In connection with the above, we would like to inform you about the possible risk that may be associated with the transfer of data to third countries, consisting in the possible lack of an adequate level of protection of natural persons related to the processing of their personal data, which is guaranteed

by the provisions of the GDPR (Regulation of the European Parliament and of the Council (EU 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 / EC), due to the lack of an adequacy decision by the European Commission and the lack of adequate security.

### **The necessity to provide personal data by the User**

Providing personal data is not a statutory requirement or a condition for concluding a contract. On the other hand, the use of selected Services may require consent to the processing of personal data, e.g. when registering a User Account, as well as forms filled in by the User in order to gain access to some of the selected Services. Obtaining access to the ABO Zone requires, in particular, the User's consent for TVP to obtain information from Poczta Polska whether the User has paid for the RTV subscription. The consequence of not providing your data may therefore be the User's inability to use selected Services.

TVP processes users' data using cookies or other similar technologies, without their consent, on the basis of a legitimate interest only in situations where it is necessary for the provision and proper operation of the Portal, i.e. maintenance and technical support of the Portal, ensuring security, preventing fraud and error removal, statistical measurements necessary for the proper functioning of the Portal. More information on this subject can be found in the Cookies Policy.

### **Profiling and automated decision making**

Users' personal data processed as part of the Portal are not subject to profiling or automated decision making, except for the use of cookies and other similar technologies to display advertisements tailored to Users (creating a profile of personalized advertisements and content, selection of personalized advertisements and content). More information on the option to disable cookies in the Cookies Policy.

### **Protection of processed personal data**

The set of collected personal data is treated as a database with a high degree of security, stored on a server secured against both remote (IT) and physical access. TVP has implemented appropriate technical and organizational measures to ensure a level of security corresponding to the risk of violating the rights and freedoms of Users. In addition, all persons processing Users' personal data for the purposes of the Portal have appropriate authorizations issued by the personal data administrator in accordance with Art. 29 GDPR.

### **Transmission protection**

Data of special importance - in particular all kinds of passwords - are sent via the SSL encrypted protocol.

## **II. Cookies and other similar technologies policy**

### **1. Cookies**

The entity that places cookies on the Portal User's end device and obtains access to them is the Portal operator - Telewizja Polska S.A. with headquarters in Warsaw, at ul. Woronicza 17, 00-999 Warsaw (hereinafter referred to as "TVP"). The tvp.pl portal automatically collects information about the Portal Users using cookies, web beacons or other similar technologies. User data obtained in this way are used in particular to provide safe, tailored services, display personalized advertisements and analyze Internet traffic. These data are processed on the basis of the legitimate interest of the administrator or the consent of the User, which may be withdrawn at any time. The data necessary for the proper operation of the Portal are processed without the user's consent, based on the legitimate interest of TVP.

Cookie files (so-called "cookies") are IT data, in particular text files, which are stored on the Portal User's end device (e.g. computer, smartphone, tablet) and are intended for using the Portal's websites. Cookies allow the information contained in them to be read only by the server that created them, i.e. in this case TVP. Cookies posted by TVP contain the name of the website they come from, the storage time on the end device and a unique number. The user can manage the consent to the use of cookies in Advanced Settings.

### **2. The purposes for which cookies are used**

Personal data collected when the User visits individual websites on the Portal, such as IP addresses, identifiers of end devices and cookie identifiers, information about searches on individual websites of the Portal may be processed by Telewizja Polska, Trusted Partners from IAB and other Trusted Partners of TVP in the following purposes:

#### **Objective 1: Store or access information on the device**

Cookies, device identifiers or other information may be stored on the user's device or made available on it for the purposes presented to the user. Providers may store and access information such as cookies and device IDs presented to you on your device.

#### **Objective 2: Selecting primary advertisements**

Advertisements may be shown based on what you're watching, the app you are using, your approximate location or device type.

To make a basic advertisement selection, providers can:

- use real-time information about the context in which the advertisement will be displayed to display the advertisement, including information about the content and device, such as: device type and parameters, client application, URL address, IP address.
- use imprecise geolocation data of the user.
- control the frequency of advertisements displayed to the user.

- set the order in which advertisements are displayed to the user.
- prevent the advertisement from appearing in an inappropriate editorial context (dangerous for the brand).

Suppliers may not:

- Create a Personalized Advertising Profile using this information for future ad selection without a separate legal basis for creating a Personalized Advertising Profile.

Attention! Imprecise means that only an approximate location with a radius of at least 500 meters is allowed.

### **Objective 3: Creating a Personalized Advertising Profile**

A profile can be built around the user and their interests, allowing the display of personalized advertisements that are relevant to the user.

To create a personalized advertising profile, providers may:

- collect information about the user, including user activities, interests, visits to websites or applications, demographic or location data in order to create or edit a user profile to personalize advertisements.
- combine this information with other previously collected information, including from various websites and applications, to create or edit a user profile to personalize advertisements.

### **Objective 4: Selecting Personalized Advertisements**

Personalized advertisements may be displayed to the user based on their profile.

To select personalized advertisements, providers may:

- select personalized advertisements based on a user profile or other historical user data, including previous user activities, interests, website or app visits, location or demographics.

### **Goal 5: Create a personalized content profile**

A profile can be built around the user and their interests, allowing the display of personalized content that is relevant to the user.

To create a personalized content profile, providers can:

- collect information about the user, including user activities, interests, visits to websites or applications, demographic or location data to create or edit a user profile to personalize content.

## **Goal 6: Selecting personalized content**

Personalized content can be displayed to the user based on their profile.

To select personalized content, providers can:

- select personalized content based on a user profile or other historical user data, including previous user activities, interests, website or app visits, location or demographics.

## **Objective 7: Measure ad performance**

It is possible to measure the performance and effectiveness of the advertisements a user sees or reacts to.

To measure advertisement performance, advertisement providers may:

- measure if and how the advertisements were delivered to the user and what was their response.
- provide reports on advertisements, including their effectiveness and performance.
- provide reports on users who have responded to advertisements, using the data observed during the user's response to that advertisement.
- provide reports to publishers about the advertisements displayed on their surface.
- measure whether the advertisement is served in the appropriate editorial environment (brand safety).
- determine what percentage your advertisement may have been watched, as well as the duration of that viewing opportunity.

Suppliers may not:

- Apply data from dashboard or similar audiences to metrics from advertising without a separate legal basis for using market research to generate audience insights.

## **Objective 8: Measure content performance**

It is possible to measure the performance and effectiveness of the content that a user sees or reacts to.

To measure content performance, providers can:

- measure and report on whether content was delivered to users and how they responded.
- deliver reports using directly measurable or known information about users who have responded to the content.

Suppliers may not:

- measure whether and how advertisements (including native advertisements) were delivered to the user and what was the user's response.
- apply data from dashboard or similar audiences to metrics from advertising without a separate legal basis for using market research to generate audience insights.

## **Objective 9: Use of market research to generate audience feedback**

Market research can be used to find out more about the audience who visit websites / apps and watch advertisements.

To apply market research to generate audience feedback, suppliers can:

- Provide advertisers or their representatives with aggregated reports on the audience their ads reached through panel analysis and similar analysis.
- Provide aggregated reports to publishers about the audience who reached the content or advertisements at their territory and who responded to that content or advertisements through the use of panel analysis and the like.
- Link offline data to an online user for market research purposes to generate audience insights if vendors have chosen to match and connect offline data sources.
- Combine this information with other information previously collected, including from various sites and applications.

Suppliers may not:

- measure the performance and effectiveness of advertisements that have been shown and responded to a specific user, without a separate legal basis for measuring advertising performance.
- measure what content was presented to a specific user and how they responded to it, without a separate legal basis for measuring the performance of the content.

## **Goal 10: Product development and improvement**

User data may be used to improve existing systems and software and to develop new products.

To develop new products and improve existing products, suppliers may:

- Use the information to supplement existing products with new features and develop new products.
- create new models and algorithms through machine learning.

Suppliers may not:

- carry out in this the purpose of any other data processing operations permitted for another purpose.

## **Special Purposes**

### **Special Purpose 1: Security, Fraud Prevention and Bug Fixes**

User data may be used to monitor and prevent fraud and to ensure the proper and secure operation of systems and processes.

To ensure security, fraud prevention and debugging, providers may:



- make sure that data is transferred securely.
- detect and prevent malicious, fraudulent, incorrect or illegal activities.
- ensure that systems and processes operate correctly and efficiently, including monitoring and improving the performance of systems and processes involved in permitted purposes.

Suppliers may not:

- Carry out any other processing operations for this purpose that are permitted for another purpose.

Note: Data collected and used for security, fraud prevention and debugging purposes may include automatically sent device characteristics for identification, precise geolocation data and data obtained by actively scanning device characteristics for identification without separate disclosure or consent.

## **Special Purpose 2: Technical delivery of advertisements or content**

User's device can receive and send information that allows the user to view and respond to advertisements and content.

To provide information and answer technical questions, suppliers may:

- use the user's IP address to deliver advertising over the Internet.
- respond to a user's response to an advertisement by directing the user to the landing page.
- use the user's IP address to deliver content over the Internet.
- respond to the user's reaction to content by directing the user to the landing page.
- use information about the type of device and the ability to deliver advertisements or content, for example, to deliver an advertisement file of the appropriate size or a video file.

Suppliers may not:

- carry out any other processing operations for this purpose which are permitted for another purpose.

## **Functions**

### **Function 1: Matching and connecting offline data sources**

Data from offline data sources may be combined with online user activity to fulfill one or more purposes.

Suppliers can:

- combine offline data with online data to fulfill one or more Goals or Special Purposes.

### **Function 2: Combine different devices**

The various devices may be referred to as belonging to the user or their household for one or more purposes.

Suppliers can:

- deterministically determine that at least two devices belong to the same user or household.
- probabilistically determine that at least two devices belong to the same user or household.
- actively scan device characteristics for probabilistic identification purposes, if users have allowed suppliers to actively scan device characteristics for identification (Special function 2)

### **Function 3: Receive and use automatically sent device characteristics for identification**

A User's device may differ from other devices based on information it automatically transmits, such as its IP address or browser type.

Suppliers can:

- create an identifier using data collected automatically from the device in terms of specific characteristics, eg IP address, user agent string.
- use an ID to try to re-identify the device.

Suppliers may not:

- create an identifier using the data collected by actively scanning the device to obtain specific characteristics, such as installed fonts or screen resolutions, without the user's separate consent to actively scan the device characteristics for identification.
- use such an ID to re-identify the device.

## **Special functions**

### **Special Feature 1: Use of accurate geolocation data**

Users' precise geolocation data may be used for one or more purposes. This means that the user's location can be accurate down to several meters.

Suppliers can:

- collect and handle accurate geolocation data for one or more purposes.

Note: Accurate geolocation means there is no limit to the accuracy of your location; can be accurate up to several meters.

### **Special Function 2: Active scanning of the device characteristics for identification purposes**

A user's device can be identified by a scan of a unique combination of device features.

Suppliers can:

- create an identifier using data collected by actively scanning the device to obtain specific characteristics, such as installed fonts or screen resolutions.
- use such an ID to re-identify the device.

### **3. Types of Cookies**

Due to the purpose of cookies, the Portal uses the following types:

- necessary cookies, enabling the use of services available on the Portal, e.g. authentication cookies used for services that require authentication on the portal;
- cookies used to ensure security, e.g. used to detect fraud in the field of authentication on the Portal;
- performance cookies, enabling the collection of information on the use of the Portal's websites;
- functional cookies, enabling "remembering" the settings selected by the User and personalizing the User's interface, e.g. in terms of the selected language or region from which the User comes, font size, website appearance, etc .;
- statistical data for counting statistics on websites;
- advertising cookies, enabling the delivery of advertising content to Users more tailored to their interests.

The Portal User may consent to the storage of cookies from the Portal on their end device using the settings of the software installed on the device he / she uses, e.g. laptop, tablet, smartphone.

Some web browsers allow cookies to be stored on the device used by the User by default. You can change cookie settings at any time. These settings can be changed in particular in such a way as to block the automatic handling of cookies in the web browser settings or to inform about their every posting in the Portal User's device.

It is worth remembering that restrictions on the use of cookies may affect some of the functionalities available on the Portal's websites.

Each User has the option of changing the browser settings so that cookies are not saved on the User's end device. This functionality is available in the software (web browser) settings.

Below are the addresses of websites describing disabling or changing the settings for example web browsers:

- Mozilla Firefox
- Safari
- Internet Explorer
- Google Chrome
- Opera

### **4. Partners**

The Portal may contain redirects to websites owned and operated by external entities (such as: Facebook, YouTube, Instagram, LinkedIn, Twitter, Snapchat, TikTok, Wykop, Redit or Telegram). Third party websites have their own privacy policies and they likely use cookies, so be sure to read these policies. TVP is not responsible for the content of cookies sent by other websites to which links are placed on the websites of the websites on the Portal.

Some information from cookies placed on the Portal User's end device is made available to Trusted Partners cooperating with TVP, e.g. in the field of advertising services offered on the Portal's pages. The purposes of sharing this information with them are indicated in point 2 of this policy.

Below are the lists of Trusted Partners:

- Trusted TVP Partners
- Trusted Partners from IAB

Consent to the use of data for some IAB Trusted Partners and TVP Trusted Partners may be related to the transfer of data to the United States or other third countries (not belonging to the European Economic Area, which includes the Member States of the European Union as well as Norway, Iceland and Liechtenstein). In connection with the above, we would like to inform you about the possible risk that may be associated with the transfer of data to third countries, consisting in the possible lack of an adequate level of protection of natural persons related to the processing of their personal data, which is guaranteed by the provisions of the GDPR (Regulation of the European Parliament and of the Council (EU 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 / EC), due to the lack of an adequacy decision by the European Commission and the lack of adequate security.

The personal data of the Portal User may be processed by TVP both on the basis of the user's consent as well as on the basis of the legitimate interest of TVP, i.e. without the need to obtain the consent of the Portal User. TVP processes user data on the basis of a legitimate interest only in situations where it is necessary for the provision and proper operation of the Portal, i.e. maintenance and technical support of the Portal, ensuring security, preventing fraud and removing errors, statistical measurements necessary for the proper functioning of the Portal.

The TVP and IAB Trusted Partners may also process the User's data on the basis of the User's voluntary consent or the legitimate interest of the administrator. The User may at any time withdraw his consent or object to the processing of his data using Advanced Settings, which will result in the cessation of the User's data processing.

The user, in relation to cookies, also has the option of removing them by sending such a request to the address [rodo@tvp.pl](mailto:rodo@tvp.pl) along with additional information identifying him, i.e. with a number identifying cookies from the TVP domain left in the User's end device.

The use of data for both advertising and analytical purposes can be managed by the User using Advanced Settings.

### **III. Trusted partners**

Third party websites have their own privacy policies and likely use cookies, so be sure to read these policies.

TVP is not responsible for the content of cookies sent by other websites to which links are placed on the websites of the websites on the Portal.

Some information from cookies placed on the Portal User's end device may also be made available to advertisers and partners cooperating with the Portal operator. You can see the list of advertisers below.

Adform A/S  
Adprime sp. z o.o.  
Agata S.A.  
All4Affiliate sp. z o.o.  
Amnet Polska sp. z o.o.  
Animex Foods sp. z o.o. sp.k.  
Animex-Animpol SF sp. z o.o. sp.k.  
Appnexus Inc.  
Arena Media Communications sp. z o.o.

Benhauer sp. z.o.o.  
Blueway Com sp. z o.o. sp.k.  
Brand Connection sp. z o.o.  
Carat Polska sp. z o.o.  
Clickad Interactive Sp. z o.o.  
Clickonometrics

Dentsu Aegis Network Polska sp. z o.o.

Edge NPD Sp. z o. o.

Effective Media sp. z o.o.

Facebook Ireland Ltd.  
Five Media sp. zo.o. sp.k.  
Fullsix Media sp. z o.o.

Gemius S.A.  
Gemius S.A.  
Google Ireland Ltd  
Google Ireland Ltd  
GroupM sp. z o.o.  
GroupM sp. z o.o.

Grupa OLX sp. z o.o.  
Grupa Pracuj sp. z o.o.  
Grupa RMF sp. z o.o. sp.k.  
Havas Media sp. z o.o.

Infinity Media sp. z o.o.  
Initiative Media Warszawa sp. z o.o.  
Iprospect Polska sp. z o.o.  
IQ Media sp. z o.o.  
Isobar Polska Sp.z o.o.

K2 Precise S.A.

Lidl sp. z o.o. sp.k.  
Loyalty Point sp. z o.o.

Media Concept sp. z o.o. sp.k.  
Media Data Mind sp. z o.o.  
Media Direction sp. z o.o.  
Media Group sp. z o.o.  
Media On sp. z o.o. sp. k.  
Media People sp. z o.o. sp. k.  
Media Republic sp. z o.o.  
Mediacom-Warszawa sp. z o.o.  
Mediaplus Warsaw sp. z o.o.  
Mets sp. z o.o.  
Mindshare Polska sp. z o.o.

Nielsen Holdings Plc

Octopus Activation sp. z o.o.  
Octopus Media sp. z o.o.  
OMD sp. z o.o.  
Omnicom Media Group sp. z o. o.  
Oracle Corporation  
One House

PHD Media Direction sp. z o.o.  
PKO Bank Polski  
PKP Intercity S.A.  
Procter&Gamble DS Polska sp. z o.o.  
Przedsiębiorstwo Prywatne IMPEX P.Grabowski, M.Szpakowski s.c.  
Pure Play sp. z o.o. sp.k.

Rainbow Tours S.A.  
Reprise Media sp. z o.o.  
RTB House S.A.

SalesTube sp. z o.o.  
Scoop sp. z o. o.

SDE Group sp. z o.o.  
SIA "Setupad"  
Smart AdServer SAS  
SMG Poland sp. z o.o.  
Socialformance sp. z o.o.  
SOCIALYSE sp. z o.o.  
Starcom sp. z o.o.  
STS S.A.  
Synerise SA

The & Partnership Limited sp. z o.o.  
The Media Insight Polska sp. z o.o.  
Trade Desk Inc.

U2 Media sp. z o.o.  
United Experts sp. z o.o. sp.k.  
Universal McCann sp. z o.o.

Value Media sp. z o.o.  
Vizeum Polska sp. z o.o.

Wavemaker sp. z o.o.  
Wawel S.A.  
Waytograd Sp. z o.o.

Yield Riser sp. z o.o.  
YieldBird sp. z o.o.  
Zenith Poland sp. z o.o.