PROTECTION OF PRIVACY AND PERSONAL DATA

Due to the specific character of our operations and our commitment to building good relations with our customers, entities of Agora Group set great store by the protection of personal data and privacy.

In our relations with readers, users of our web services, digital subscribers and recipients of newsletters, as well as customers and business clients, we are committed to observing proper procedures and policies as well as provide education and transparent communications. In 2019 Agora continued the activities listed in Agora S.A. Responsibility Report 2018. (link)

DATA PROTECTION POLICIES AND PROCEDURES

in 2018 Agora Group adopted a new Personal Data Protection Policy, to comply with the European Parliament and Council of Europe resolution on the protection of personal information (UE) 2016/679, also referred to as GDPR or lGDPR, and the introduction of a new personal data protection act of 10 May 2018. In 2019 Agora Group reviewed our policies and protocols to verify and, if needed, make necessary updates to the regulations.

Personal Data Protection Policy In Agora is a set of rules and procedures to protect the personal data processed by the employees and collaborators of Agora as a part of their business activities.

PERSONAL DATA PROTECTION POLICY IN AGORA COMPRISES:

- **Transparency Policy (Personal Data Processing Policy)** – is a declaration signed by all employees and collaborators of Agora that ensures clients that their personal data are protected in accordance with all legal requirements. The document includes general information about the rules of processing personal information by Agora, handling of claims from the persons whose data is processed, as well as information required under Articles 13 and 14 of GDPR, concerning individuals whose personal information is processed. It is a public document available on, Agora website.

The remaining documents are available internally for employees only:

- **Personal data retention policy** – a set of rules regulating the retention of personal data stored by Agora.
- **Procedure for handling the claims and requests of data subjects** – set of procedures for handling the requests of data subjects – clients and users – exercising their legal rights in relation to the processing of their personal data. The procedure determines the terms of accepting and recognizing claims and requests, the competences of the GDPR office and business lines in the handling and responding to them.
- **Assessment of the risks and consequences of personal data processing** – the document lists measures that are necessary for properly assessing the risk and consequences of processing personal data. It also specifies the cases in which relevant further, expanded risk assessment is required.
- **Evaluation and reporting on breaches of personal data protection** – specifies what constitutes the violation of personal data managed by Agora or its subsidiaries, how and when an observed breach should be reported, as well as how it should be resolved and by whom.
- **Selection policy for personal data processing entities** – a set of provisions that oblige the company to review a supplier for compliance with personal data protection regulations. The policy is only applied to suppliers intended by Agora to have access to personal data. The review is to verify whether the supplier has technical and organizational capacity for effective protection of personal data entrusted for processing.
- **Policy of contacts with the personal data protection institution** – describes the protocol of handling cases that require contacts with the President of the Personal Data Protection Office, including controls and court-administrative procedures.

REPORTING DATA PROTECTION BREACHES

- Every employee of Agora Group is obliged to report on observed incidents of personal data breach.
- Personal data breach is any incident leading to accidental or illegal destruction, loss, modification, unauthorised publication or unauthorised access to personal data transferred, processed or otherwise handled by Agora Group.
- Personal Data Protection Officer keeps a register of breaches with all reported incidents. The company also introduced a system of monitoring and verification of cases against the markers of personal data protection breach.

COMMUNICATION AND EDUCATION OF EMPLOYEES

Since 2018 training has been provided to the employees, including instruction offered to new employees as part of Welcome to Agora orientation training, with information about the personal data protection regulations and codes observed in Agora. Employees also receive online training. We also continue to educate the employees to raise their awareness of personal data protection through repeated communications – emailing, posters and animated graphics. Additionally, Helios S.A. delivers regular training / workshops for company's departments and cinema employees.

PROTECTION OF PERSONAL DATA AGAINST CYBER THREATS

Under our information security management, Agora S.A. adopted *Strategia Bezpieczeństwa* (Security Strategy), *Polityka Bezpieczeństwa* (Security Policy) and *Polityka Bezpieczeństwa Informacji* (Information Security Policy). The role of Information Security Policy and related documents is to specify the requirements than need to be met to ensure the security of collecting, processing and transferring data in Agora S.A. and compliance of the internal data protection measures with relevant laws.
In 2018 a set of procedures was developed with regulations related to cyber threats. The procedures also refer to personal data processed in Agora's computer systems. The procedures are continuously monitored to ensure their current relevance.
With respect to web portals and its mobile applications, Agora Group introduced: *Zasady korzystania z serwisów internetowych* (Rules of Using Agora Web Services), *Polityka prywatności* (Privacy Policy) and *Polityka Prywatności w zakresie aplikacji mobilnych* (Mobile Applications Privacy Policy), as well as internal codes and regulations. In 2019 Agora Group developed a set of rules for using company devices for private purposes and private devices for work use. This is to minimize the risk of data loss or a hacking attack on the resources of Agora through increasing the employees' awareness of proper handling of the devices used for professional purposes.
For the purpose of ongoing protection of data, including personal data, Agora established *Data Protection Committee* – made up of experts in personal data protection, law, computer storage protection and communications. Moreover, to ensure compliance personal data protection regulations and internal protocols, Agora Group has established the office of *Personal Data Protection Inspector*.

PERSONAL DATA PROTECTION IN HELIOS

In 2018 also Helios SA introduced new measures to protect personal data of the clients and users of Helios.pl. Its Jak dbamy o Twoje dane (How we protect your personal information) site offers detailed information on the handling and processing of users' personal information. Additionally, the company adopted Polityka prywatności (Privacy policy) and Polityka transparentności (Transparency policy). Any social media profile managed by Helios SA has a special information clause. Additionally, Helios S.A. delivers regular training / workshops for company's departments and cinema employees.

GDPR AND GOLDENLINE PRODUCTS

Supporting clients in recruitment processes, GoldenLine observes the best personal data protection standards. To that end, a special website dedicated to protection of clients' and users' data was launched on goldenline.pl. The site offers relevant necessary information *GDPR a produkty GoldenLine - co powinieneś wiedzieć* (Compliance of GoldenLine products with GDPR – what you should know).

The firm has also adopted a new data protection policy with all necessary procedures, and updated the terms of GoldenLine.pl site, as well as implemented *Polityka prywatności* (Privacy Policy) and *Polityka przetwarzania danych osobowych - Polityka transparentności* (Personal Data Processing Policy –Transparency policy).

PROTECTION OF PERSONAL DATA IN AMS S.A.

AMS makes every effort to ensure the security of personal data it processes, including those of their employees, clients and contractors. To this end AMS adopted a number of personal data protection protocols, introduced relevant training for current employees and collaborators as well as for new employees. Every website and service managed by AMS has updated Privacy Policies and codes. To ensure personal data protection regulations and internal protocols are observed, AMS has a Personal Data Protection Inspector.

PRIVACY POLICY

To protect customers' privacy and personal data, Agora Group implemented a number of procedures ensuring the security of personal data and maintains the highest standards in our communications with clients and customers, in line with legal regulations and industry requirements.
Agora S.A. adopted *Strategia Bezpieczeństwa* (Security Strategy), *Polityka Bezpieczeństwa* (Security Policy) and *Polityka Bezpieczeństwa Informacji* (Information Security Policy).
Helios S.A. adopted *Polityka Bezpieczeństwa 2.0* (Security Policy 2.0) that covers all existing regulations: *Polityka Bezpieczeństwa* (Security Policy) and *Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych* (Instruction for Managing Computer Systems for Processing Personal Data).
Agora Group has documents that specify the principles and procedures for collecting, processing and use of information about the users of web services of each entity, brand and medium of Agora. Personal data policies and regulations, as well as rules of the use of some services or regulating e-commerce of services are available in relevant services and portals: Agora.pl, Wyborcza.pl, Gazeta.pl, Helios.pl, Ams.com.pl. The documents cover rules, scope and terms of use for the service/application by the reader/user, including complaints and claims.

COOPERATION WITH PDPO

In 2019 no breaches of personal data protection regulations were recorded in any of the entities of Agora Group, that would result in incurring financial penalties.
In 2019 two incidents were recorded, caused by internal errors, that resulted in a report sent to PDPO. In both cases necessary measures were taken instantly to minimize the risk of confidentiality breach or unauthorised access to data. Agora received three formal letters from Personal Data Protection Office urging Agora S.A. to provide explanations. Agora's timely response proved that in the relevant cases personal data was handled correctly.
In 2019 one incident was recorded in Helios S.A. resulting in a report sent PDPO. The incident was caused by an employee's error. Measures taken to minimize the risk of confidentiality breach or unauthorised access to data were approved by PDPO.