

Personal Data Protection Board’s Decision No. 2023/1645 dated September 28, 2023, regarding “the unlawful processing of personal data by the data controller acting as the distributor and sole authorized entity of a massively multiplayer online game in Turkey”

Date of Decision : September 28, 2023

Decision No. : 2023/1645

Subject Summary : Unlawful processing of personal data by the data controller acting as the distributor and sole authorized representative of a massively multiplayer online game in Turkey

In summary, the complaint submitted to the Authority states:

- The data controller is the distributor and sole authorized entity of a massively multiplayer online game in Turkey and is the company that performs all transactions on behalf of the game for users in Turkey and generates all commercial revenue,
- The data subject applied to the data controller to exercise their rights under Article (Law) but many of their requests were left unanswered or met with misleading and incomplete information; the response provided by the data controller referenced numerous legal provisions but failed to specify which personal data was processed, for what purpose, and on what legal grounds under those provisions;
- The response provided by the data controller stating that personal data was not transferred to any location within or outside the country other than judicial and administrative authorities is entirely false, Upon reviewing the information notice labeled as the “privacy notice” on the data controller’s website, as well as the privacy policy and cookie policy published on the same website, it is readily apparent that personal data has been transferred abroad,
- The data controller uses third-party software for the purpose of “preventing fraud and deception,” this software runs every time the game is launched, scans all files and software currently on the computer, and continues to run as long as the game remains open; upon reviewing the license agreement of the company owning the software, it was determined that personal data was unlawfully obtained and transferred abroad through this software,
- The data controller’s statement that “we only identify users via IP address” is false, as it is technically impossible to determine which software is running on a person’s device using only an IP address,
- It was stated that the privacy policy on the data controller’s website does not comply with the “Communication on the Procedures and Principles to Be Followed in Fulfilling

the Duty to Inform,” and it was requested that the necessary actions be taken under the Law.

As part of the investigation initiated regarding this matter, the data controller in question was requested to submit a defense. In the response provided by the data controller, it was summarized that:

- The company’s ownership structure consists entirely of foreign shareholders, and the sector in which the company operates is based on the preparation of digital game contracts to be concluded between parties such as player-developer, player-publisher, player-player, licensor-licensee, trademark owner-trademark user, etc. and that the foreign ownership of its partners necessitates the transfer of personal data abroad due to business processes; that all servers used for gaming services are hosted in Turkey;
- The personal data processed regarding the relevant individual includes the "e-mail address, IP address," and, if the user selects a secure login method, additionally "mobile phone number," and that these personal data are processed in accordance with Law No. 5651 on the Regulation of Publications Made on the Internet and the Fight Against Crimes Committed Through Such Publications and its associated regulations, Article 419/3 of the Turkish Code of Obligations, Law No. 6563 on the Regulation of Electronic Commerce and related regulations, the Turkish Penal Code, and Law No. 6698, among others, in order to fulfill the legal obligations arising from the relevant legislation, in accordance with Article 5, Paragraph 2(c) of Article 5 of Law No. 6698 and for the purpose of safeguarding legitimate interests, provided that it does not infringe upon the fundamental rights and freedoms of the data subject, and in accordance with subparagraph (f) of paragraph 2 of Article 5 of the Law,
- Although products can be purchased within the game, credit card information is processed by the payment service provider, and neither the Company nor the user processes any credit card information, name, or surname,
- Except for the sharing of personal data with judicial authorities in accordance with Article 8(2)(a) and Article 5(2)(ç) of the Law for the purpose of fulfilling legal obligations, the personal data of users, including the supplier, is not shared with anyone,
- The data subject contacted us on May 23, 2020, and a response was provided to the data subject on June 22, 2020,
- No personal data such as “first name, last name, Turkish ID number” that would enable the matching of players with their in-game characters or in-game items is requested from any player; within the scope of the gaming service, only an “email address” is requested from the relevant individuals at ; players log in to the game using nicknames, and their email addresses do not contain their real names; this is also the general practice for online games,

- The relevant individual stated that information such as game purchase records, activity logs, item records, character information, server information, etc., constitutes personal data; however, since every player can possess the aforementioned boosters or products, therefore, it is not possible for them to identify or make a specific individual identifiable; furthermore, due to the limited number of servers in the game, users can only log in via existing servers, and it is not possible to identify or make individuals identifiable through these servers,
- Special software is used to detect cheating and fraudulent activities; contrary to what the complainant stated, this software does not scan all files on a person's computer or access the camera and microphone; the software's operating principle is not to scan the computer like anti-virus programs, but rather aims to detect the code of cheating and fraud programs composed of zeros and ones; for this purpose, it scans not all files on the computer but specifically the EXE file code of cheating and fraud software defined within the software itself; furthermore, no personal data is transferred abroad in any way through the software,
- As the data controller, they exercise the utmost care regarding the protection of personal data,
- Only cookies strictly necessary for the website's operation are used; no cookies are used for marketing or similar purposes; the cookie policy appears as a "pop-up" on the screen when the website is visited,
- It has been stated that the privacy notice and privacy policy on the website were prepared prior to the Law's entry into force; therefore, a new compliance process has been initiated to update the privacy notice and privacy policy and bring them into alignment with current data processing activities.

Based on the response in question, since *"it was not possible to reach a definitive conclusion regarding whether the data controller had transferred the data subject's email address and IP address—which constitute personal data—abroad,"* an on-site inspection was conducted by visiting the data controller's office and the headquarters of another company from which it receives services. As a result of this inspection, regarding the transfer of personal data abroad by the data controller:

- The personal data of game users/members (username, email address, password, and mobile phone number if provided by the user) was not transferred abroad, and user data was not transferred to shareholders located abroad,
- The 10 physical servers purchased to provide game services to users, along with the virtual servers created in connection with these physical servers, and the 1 physical server that was leased; these are located in the data center of the company from which

services are obtained, and the physical security of the servers is ensured by the relevant company,

- No connection is established with any servers located abroad,
- Since the User Agreement and Privacy Policy were directly provided by the foreign company holding the license, no changes could be made to their content; The Personal Data Protection Policy and Registration Information Notice were prepared in parallel with these documents, and the revision process to ensure all documents on the website comply with the Law and relevant regulations is ongoing;
- Backups are taken daily and weekly; some of these backups are stored on a cloud computing platform; copies are maintained in two separate formats: the “Portal database” and the “Player database”; It was stated that personal data is stored in the “Portal database,” that the Portal database is maintained within the company as the data controller and is not accessible from outside, and that the backups transferred to the cloud computing platform do not include “Portal database” backups.

As a result of the investigation conducted regarding this matter, pursuant to the Decision No. 2023/1645 of the Personal Data Protection Board dated 09/28/2023;

- **Regarding the allegation of “unlawful processing of personal data through surveillance software”;** it was noted that in online games where the data controller acts as the distributor and sole authorized representative in Turkey, there is a high likelihood of players engaging in fraud, cheating, and selling their accounts to others. To carry out this process, players use bot software (*a software program that repeats, operates automatically, and performs predefined tasks*) without playing the game themselves. *Bots typically mimic human users’ behavior or take their place. Since they are automated, they operate much faster than human users. While they can perform useful functions such as customer service or search engine indexing, they can also be used as malicious software designed to gain full control over a computer.*) to advance the game in an automated manner, thereby enabling in-game activities such as leveling up and character development; the aforementioned bot software does not perform this process via a single IP address on the internet, and the IP address is changed during this process via a VPN (*Virtual Private Network—an internet technology enabling connection to different networks via remote access*) to change the IP address during this process; the data controller’s specialized software, however, analyzes the .exe files (*executable files—on Windows computers, the file extensions for files that allow program installation are .exe, and .exe files enable the installation and setup of various programs on Windows operating systems.*) to determine whether the player is using bot software; this software attempts only to distinguish the types of open exe files on the computer; IP changes, which are one of the indicators of fraud and cheating, are also tracked through this software; it was determined that no data transfer occurred over the internet, and that the IP address was tracked. Consequently, the data controller used the

specialized software in question at to determine whether game users were engaging in cheating or fraud; during this use, no unlawful processing of personal data was conducted by accessing personal data on the players' computers,

- **Regarding the fulfillment of the duty to inform;**

- Pursuant to Article 10 of the Law titled “The Data Controller’s Obligation to Inform,” the data controller or an authorized representative is obligated to provide information to the data subjects at the time of collecting personal data regarding the identity of the data controller and, if applicable, its representative; the purpose for which the personal data will be processed; to whom and for what purpose the processed personal data may be transferred; the method and legal basis for collecting personal data; and the other rights listed in Article 11, Additionally, the “Procedures and Principles” regarding the obligation to provide information are comprehensively explained in Article 5 of the Communiqué on the Procedures and Principles to Be Followed in Fulfilling the Obligation to Provide Information,
- Upon examination of the data controller’s website, it was determined that the texts titled “Sign-Up Information Notice,” “Personal Data Protection Policy,” and “Privacy Policy” regarding personal data processing activities are present; the “Sign-Up Information Notice” and the “Personal Data Protection Policy” were prepared by the data controller, while the “Privacy Policy” was prepared by a foreign-owned company that is the data controller’s majority shareholder,
- It was observed that individuals wishing to use the online virtual game service provided by the data controller are required to create a membership account, and during the account creation process, they are asked to check a box confirming that they have read, understood, and accepted the “Registration Information Notice” and the “Privacy Policy.” Upon reviewing the “Registration Information Notice” is prepared for individuals who will create a membership account with the data controller and is generally in compliance with Article 10 of the Law and the Information Notice; however, it should not contain vague expressions such as “... may be shared,”
- Upon reviewing the text titled “Privacy Policy”; it was concluded that the text constitutes an online privacy policy provided by the company—which is the majority shareholder of the data controller—to visitors, users, and customers, and that said company acts as a separate data controller. The text generally covers: the types of information collected (processing of children’s personal data; personally identifiable information provided by data subjects; information collected through technologies, methods, and/or services) and that this information includes details such as email address, gender, phone number, home address, date of birth, and IP address; the company’s use and sharing of the

collected information (internal use for commercial purposes; use and/or sharing with third parties for commercial purposes; promotional, contest, and/or sweepstakes activities; purchase, sale, liquidation, or merger; disclosures, use, and/or sharing of information for non-business reasons) and measures to ensure the accuracy of personal information, it was determined that the aforementioned text is not in compliance with Article 10 of the Law and the Information Notice ; therefore, this text—which is presented to data subjects during the registration process and is presumed to have been accepted in the User Agreement—must be brought into compliance with the Law in a manner consistent with the other texts or removed,

- While the “Personal Data Protection Policy” text provides general information regarding personal data processing activities, when compared to the other two texts, it addresses a broader category of data subjects (job applicants, employees, shareholders/partners, supplier employees, supplier representatives, individuals receiving products or services, visitors), It outlines the purposes of the personal data processing activities conducted by the data controller, the categories of personal data, the categories of parties with whom personal data is shared, and the purposes of such sharing; however, it is not clearly understood which group of data subjects’ personal data is processed, for what purpose, and on what legal basis, nor to which third parties it is transferred, therefore, the text in question must be brought into compliance with subparagraphs (g), (ğ), and (h) of paragraph (1) of Article 5 of the Information Notice,
 - Ultimately, the presentation of three different texts creates a complex situation for data subjects; this matter was also communicated to the data controller during the on-site inspection, and the data controller stated that efforts are being made to bring these documents into compliance with the Law,
- **Regarding the transfer of personal data abroad;**
 - Article 9 of the Law regulates the “transfer of personal data abroad”; under Article 3, titled “Definitions,” paragraph (1), subparagraph (a) of the Law defines “explicit consent” is defined as “*consent that is specific to a particular matter, based on information provided, and freely given,*” and that the expression of explicit consent must allow the data subject to determine the limits, scope, and manner of processing of the data they consent to; in this context, explicit consent must include a positive declaration of intent by the consenting individual; the data controller must obtain separate explicit consent for secondary processing activities, such as data transfers abroad, following the use of the data; and the burden of proof regarding the obtaining of explicit consent rests with the data controller;

- Following an examination in the Turkish Trade Registry Gazette, it was determined that the data controller's partners are two separate foreign-owned companies; and upon reviewing the documents published on the data controller's website and the VERBIS query page regarding the cross-border transfer of personal data:
 - The “**Privacy Policy**” text prepared by one of the foreign-owned partner companies states: “...*The following privacy policy informs you about how we collect, store, retain, and use the personally identifiable information you provide to us and the non-personally identifiable information we obtain, including but not limited to all activities covered by these provisions...*” and the statement “*In connection with the paid services in our online products, we are required to establish commercial relationships with third parties. As a result of these relationships, we share all or part of our customers' personally identifiable information to successfully operate the systems for the paid services and/or products our customers request,*”
 - In the “**User Agreement**” text, it states: “...*The Company permits you to play online computer games provided you accept all terms and conditions of this agreement and comply with the Code of Conduct provided. If you accept the agreement, please click the “I accept this USER AGREEMENT” and “I accept this PRIVACY POLICY” buttons at the end of this agreement...*” is included, and on the data controller's website, to create a game account, *clicking the “Sign Up” to create a game account on the data controller's website, you must enter your “ID, email, and password” and confirm: “I hereby declare that I have read, understood, and accepted the following: Sign Up Data Protection Notice, User Agreement, Privacy Policy, and Code of Conduct. If you are 13 years old and under the legal age of majority in your country of residence, you must review this User Agreement with your family.” In the “Sign Up Information Notice” states that personal data such as “ID, email, password” obtained from data subjects by the data controller is processed under the processing conditions set forth in Article 5(2)(c) of the Law, which states, “The processing of personal data belonging to the parties to a contract is necessary provided that it is directly related to the conclusion or performance of the contract,” and and subparagraph (f), which states, “Processing is necessary for the legitimate interests of the data controller, provided that such processing does not infringe upon the fundamental rights and freedoms of the data subject”;* the personal data of users creating an account is processed for the purposes of creating a game account, enabling participation in player groups, logging into the system, and utilizing the products and services offered, and may be shared with business partners, suppliers, and, upon request and/or as

required by law, with authorized public institutions and organizations, judicial authorities, courts, and notaries in accordance with Articles 8 and 9 of the Law,

- In the text titled “Personal Data Protection Policy,” the category of data subjects includes job applicants, employees, shareholders/partners, supplier employees, supplier representatives, individuals receiving products or services, and visitors; the categories of parties with whom personal data is shared include suppliers, , authorized public institutions and organizations, and shareholders; The “person receiving products or services” category mentioned in the aforementioned document refers to individuals who create a membership account to utilize the online virtual computer game service provided by the data controller via its website and to purchase game products upon request, by accepting the Registration Information Notice, User Agreement, and Privacy Policy published on the data controller’s website,
 - Upon reviewing the information registered by the data controller in VERBIS, it is observed that the group of data subjects includes job applicants, employees, shareholders/partners, potential product or service purchasers, interns, supplier employees, supplier representatives, and individuals who purchase products or services; while the categories of data transferred abroad include identification, contact (address number, email address, mailing address, KEP address, phone number) and transaction security (IP address information, website login/logout information, password and PIN information),
 - Additionally, since *“it could not be definitively determined whether the data controller had transferred the email address and IP address—which constitute personal data of the relevant individual—abroad,”* an on-site inspection was conducted by visiting the data controller’s office and the headquarters of another company from which it receives services; it was determined that the data controller had purchased 11 game servers to be kept within the country, and a contract had been entered into with a company for services related to security, hosting, etc., services, and that screenshots regarding the backup of the databases provided by the data controller were reviewed, revealing that information related to online virtual games (such as game levels and in-game items) was backed up on a cloud computing platform, while it was determined that the personal data of players/members was not backed up; in this context, it was concluded that the data controller maintains the game servers within the country and that the personal data of the relevant individuals who are game users/members is not transferred abroad,
- **Regarding the legality of personal data processing activities conducted via cookies;**

- The “Guidelines on Cookie Practices” published by our Institution outlines the matters that data controllers must consider when processing personal data through the use of cookies; in this context, in summary: when processing personal data via cookies, “*Criterion A: The cookie must be used solely for the purpose of providing communication via an electronic communications network*” and “*Criterion B: The use of cookies must be strictly necessary for the provision of information society services explicitly requested by the subscriber or user to receive the service.*” Furthermore, for personal data processing activities based on the condition of explicit consent, such consent must be based on the user’s active action (*for example, using the “opt-in” method for cookie preferences presented to the user at*). when obtaining explicit consent regarding cookies, a cookie management panel (*such as a pop-up or banner*) should appear upon entering the website, and the “accept,” “Reject,” and “Preferences” buttons displayed in equal prominence (in terms of color, size, and font), and that the privacy notice should clearly include information regarding the cookie’s name, purpose of use, duration of use, and whether it is a first-party or third-party cookie,
- In the data subject’s complaint, it is stated that the data controller’s cookie policy published on its website includes the phrase “*The user’s visit to this Site constitutes consent to the use of cookies under this policy,*” despite the absence of explicit consent, and that some companies located abroad allegedly process personal data using third-party cookies and transfer it abroad,
- The data controller’s website uses essential cookies, functional cookies, analytics/performance cookies, and targeting/advertising cookies; under the cookie-related pop-up explanation, *two options are presented: “use only essential cookies” and “allow all cookies,”* and that by presenting the “allow all cookies” option for personal data processing activities involving cookies other than necessary cookies, the data controller has opted for a blanket consent approach without offering individuals the opportunity to choose, yet since explicit consent must be obtained for each cookie type requiring it, “opt-in” method, the data controller’s consent text undermines the elements that consent must be “specific to a particular matter” and “given freely,” and a lawful personal data processing activity under Article 5 of the Law has not been carried out,
- On the other hand, the cookie table included in the “Cookie Statement” and “Cookie Policy” published on the data controller’s website indicates that various cookies provided by third-party cookie providers are used under the “necessary cookies” category, however, as also noted in the Guidelines on Cookie Practices, in cases where third-party cookies are placed on a website, both the website owner and the third party are obligated to ensure users are clearly informed about cookies and to obtain their consent, Considering that, in cases where websites

operating in Turkey carry out data transfer activities abroad through cookies used via companies based abroad, such data transfer activities must be conducted in accordance with the conditions set forth in Article 9 of the Law; the data was transferred abroad without obtaining the explicit consent of the data subjects and in violation of Article 9 of the Law,

- Regarding the fulfillment of the **obligation to provide information concerning the processing of personal data through cookies**, it was determined that the “Cookie Policy” and “Cookie Statement” texts on the website contain differing information regarding cookies in the tables at ; therefore, based on the assessment that these tables must be updated and made consistent;
- The pop-up notification regarding cookies published on the data controller’s website presents two options: “Use only necessary cookies” and “Allow all cookies.” By offering the “Allow all cookies” option, the data controller obtains collective explicit consent for every cookie type outside the “necessary cookies” category, thereby failing to provide data subjects with the opportunity to make a choice, In the cookie table included in the Cookie Statement and Cookie Policy texts, it is stated that various cookies provided by third-party cookie providers are used under the “necessary cookies” category; the third-party cookie provider is a company based abroad, Since the elements of “being specific to a particular matter” and “being given freely” – which are essential components of explicit consent – were not met in the personal data processing activity conducted on the website by the data controller based on the condition of explicit consent via cookies, the explicit consent is deemed invalid, and a lawful personal data processing activity under Article 5 of the Law has not been carried out; on the other hand, it was concluded that the personal data processing activity, which involved the transfer of personal data abroad through the use of third-party cookies—whose providers are companies established abroad and fall under the category of essential cookies—is unlawful because it does not comply with the conditions for data transfer abroad specified in Article 9 of the Law; and, and
- The Cookie Policy and Cookie Statement texts must be made consistent and compatible with one another, taking into account the Guidelines on Cookie Practices, and brought into compliance with Article 10 of the Law and the Communiqué on the Procedures and Principles to Be Followed in Fulfilling the Duty of Information, Instructing the data controller to include a provision in the aforementioned texts regarding the transfer of personal data abroad via cookies and to notify the Board thereof,
- Instructing the data controller to implement the necessary arrangements on the website to obtain separate explicit consent from the relevant individuals for the transfer of personal data abroad via cookies and to notify the Board,
- Instructing the data controller to ensure that the texts titled “Privacy Policy,” “Registration Information Notice,” and “Personal Data Protection Policy” published on

the website to be consistent and in harmony with one another and with the information processed in VERBIS, in accordance with Article 10 of the Law and the Communiqué on the Procedures and Principles to Be Followed in the Fulfilment of the Information Obligation, and to instruct the data controller to notify the Board,

- Considering that, in the online gaming service provided on the data controller's website, players'/members' personal data is not transferred abroad via the game servers since the servers are hosted domestically (); the "Privacy Policy," "User Agreement," "Registration Information Notice," and "Personal Data Protection Policy," as well as the relevant sections of the VERBIS registration pertaining to the transfer of personal data abroad, and to instruct the data controller to notify the Board thereof,
- The data controller has purchased 11 game servers to be kept within the country; a Service Agreement has been entered into with a company for security, hosting, and other related services for the servers, and a monthly service fee is paid; the numbers of the game servers belonging to the data controller located in the company's server room match the numbers of the servers specified in the annex to the Service Agreement; Considering that the data controller has backed up information related to online virtual games (such as game levels, in-game items, etc.) on a cloud computing system, and that it was determined through an on-site inspection that the personal data of players/members was not backed up; it has been concluded that the data controller maintains the game servers within the country and that the personal data of the relevant individual, who is a game user/member, has not been transferred abroad; therefore, no action will be taken against the data controller under the Law regarding this matter;
- Considering that the software used by the data controller and subject to the complaint, which was in use while the relevant individual was playing the aforementioned online game, is a program designed to identify whether the game user is using software for cheating or fraud by distinguishing the types of files with the "exe." extension; it has been concluded that no unlawful personal data processing activities were carried out by accessing the personal data on the computer of the game user/member, and it has been decided that no action will be taken against the data controller under the Law regarding this matter.