Final Decision

Case Register	734237
National file number	11.17.001.013.041
Controller	Frenwall Limited
Date	23.04.2026

Description of the Case

2.1. The data subject lodged a complaint with the Swedish Authority for Privacy Protection (DPA), and was thereafter received by the Office of the Commissioner for Personal Data Protection (Cyprus SA) on 16/12/2024. The complaint involves the Controller's failure to comply with Subject Access Requests (Article 15 of the GDPR).

2.2. The data subject exercised his right of access and requested the following information via email on 28 September and 3 October 2024:

i. All data that has been provided by the data subject, including registration information, communication history, and transaction records.
ii. All data collected about the data subject through their use of the websites and services, including gaming history, login information, and technical details.
iii. All information received from third parties regarding the data subject.
iv. Complete details on how the data subject's personal data is processed, including the purposes of processing, categories of personal data, recipients of the data, and any transfers to third countries.
v. Information regarding the duration for which the data subject's personal data will be stored.
vi. A comprehensive overview of the data subject's rights under GDPR, including the rights to rectification, erasure, and restriction of processing.
vii. The data subject requests that this information be provided in a structured, commonly used, and machine-readable format.

2.3. The controller, immediately after receiving the first email from the complainant, proceeded in a timely and appropriate manner to redirect his request to the corresponding department. The controller did not respond to the second email of the complainant and did not provide him the requested information.

Investigation by Cyprus SA

3.1. The Commissioner's office contacted the Controller, and requested their views on the matter raised by the complainant. In their reply, the Controller provided us with a comprehensive report detailing how the complainant's request was handled. According to the Controller, standard identity verification procedures were initiated in line with the General Data Protection Regulation (GDPR), particularly Article 12(6), which allows data controllers to request additional information in cases where there is reasonable doubt about the identity of the requester. The Controller stated that, for security reasons, personal data is disclosed only after verifying specific identification elements—namely, the complainant's full name, date of birth, and last payment method—and only through the email address associated with the complainant's account.

3.2. Where full verification was completed, the Controller claims that the data was provided within the regulatory 30-day time frame. Where verification was incomplete or not received, the request was not processed to avoid unauthorized disclosure. Additionally, the Controller noted limitations under Article 15(4) GDPR regarding the disclosure of certain technical and third-party data, which they state may not be shared if doing so would affect the rights or freedoms of others.

3.3. A summary of the Controller's handling of the access requests per casino platform is as follows:

3.3.1. **Winsly Casino**

The Controller contacted the complainant on 4 October 2024 to request identity verification, which the complainant provided on 5 October. The Controller confirmed on 14 October that the request would be fulfilled within the statutory period. On 31 October, they sent the complainant personal data, payment and game history, and communication records, all in password-protected documents. That same day, they also sent a separate email containing the access code, along with information on AML-related data retention obligations. On 9 November, the complainant informed them that the access code had not been received. On 10 November, Customer Support requested identity verification before resending the code, citing security requirements. The complainant initially declined but later provided the necessary details. The Controller reports that the access code was reissued on 17 November 2024.

3.3.2. **Jackpot Cow Casino**

On 30 September 2024, Customer Support contacted the complainant requesting identification details. The complainant responded on 3 October stating that sufficient information had already been provided. On 14 October, the Controller requested the final missing detail—the complainant's last payment method—for full verification. According to the Controller, no further response was received from the complainant, and therefore they could not proceed with fulfilling the access request.

3.3.3. **Mad Rush Casino**

On 4 October 2024, the Controller requested the complainant's full name, date of birth, and last payment method. A follow-up was sent on 14 October. On the same day, the complainant provided the requested information. The Controller confirmed on 21 October that the request was being processed and that the response would be provided within the required 30-day period. On 31 October, the Controller sent the complainant personal data and communication history in password-protected documents. The access code to these documents was sent in a follow-up email on the same day, along with an additional explanation about data retention obligations under anti-money laundering (AML) laws.

3.3.4. **Reko Casino**

Customer Support contacted the complainant on 30 September 2024 for identity verification. The complainant replied on 3 October, again stating that sufficient information had already been provided. On 4 October, the Controller requested the final verification detail—the complainant's last payment method—and sent a reminder on 14 October. According to the Controller, no further response was received, and the request could not be completed.

3.3.5. **Slot Owl Casino**

On 30 September 2024, the Controller requested verification details. The complainant replied on 3 October, affirming the right of access, and the Controller followed up the next day asking for the complainant's last payment method. The complainant provided the requested information on 7 October. On 27 October, the Controller sent the complainant personal data, payment and game history, and communication records in password-protected documents. A follow-up email with the access code was sent the same day. On 28 October, the complainant expressed dissatisfaction, stating that only part of the requested data had been shared. On 30 October, the Controller clarified that all available account-related data had been disclosed, and they sent another email explaining their legal obligation to retain certain data under AML regulations.

Cyprus SA assessment

4.1. Considering the above and the cooperation demonstrated by the Controller, the Cyprus SA finds that the Controller complied with its obligations under the GDPR.

4.2. The Commissioner notes that where full identity verification was completed, the Controller provided the requested information within the regulatory timeframe.

4.3. Where verification was lacking, the Controller's decision to withhold disclosure was justified to protect the rights and freedoms of data subjects and prevent unauthorized access.

4.4. In view of the above, the Commissioner considers that the investigation may be concluded as no further supervisory measures are necessary at this stage.