

Draft regulation

Period of validity

Legal basis

Gambling Act (10/2026), section 45

Amends/Repeals

-

Target groups

Licence holders

Technical Transmission of Game and Gaming Account Transaction Data under the Gambling Act

Contents

1 Säädestausta, soveltamisala ja määritelmät.....	2
1.1 Valvontaviranomaisen määräyksenantovaltuus.....	2
1.2 Lainsäädäntö.....	2
1.3 Soveltamisala.....	2
1.4 Määritelmät.....	2
2 Peli- ja pelitilitapahtumat.....	3
2.1 Pelitapahtuma- ja pelitilitapahtumatietojen allekirjoitusvaatimus.....	4
2.2 Pelitapahtumien ja pelitilitapahtumien säilytysvelvollisuus.....	4
3 Dataholvi.....	5
3.1 Dataholvin tekniset ja tietoturva-vaatimukset.....	5
3.1.1 Saatavuus ja toimintavarmuus.....	5
3.1.2 Pääsynhallinta.....	6
3.1.3 Lokitus.....	6
3.1.4 Tietojen eheys ja muuttumattomuus.....	7
3.1.5 Dokumentointi.....	7
3.1.6 Poikkeamien ilmoitusvelvollisuus.....	7
3.2 Dataholvin kansiorakenne.....	7
3.3 Tiedostojen nimeäminen.....	10
3.3.1 Versiot ja versionumeroiden käyttö.....	11
3.3.2 Pelitilitapahtumat.....	11
3.3.3 Pelitapahtumat.....	13
3.3.4 Tiedostojen uudelleenmuodostaminen.....	13

3.3.5 Tiivistetiedostot.....	14
4 Tiedonsiirto dataholvista.....	14
4.1 Yhteyksien muodostaminen.....	15
4.2 Yhteyksien ja avainten päivittäminen.....	15
4.3 Tiedonsiirron poikkeustilanteet.....	16
5 Yksinoikeustoimiluvan haltijan poikkeusmenettely.....	16
6 Voimaantulo.....	16

1 Legal framework, scope and definitions

1.1 The supervisory authority's power to issue regulations

The right of the supervisory authority to issue a binding order is based on section 45(4) of the Gambling Act (10/2026). Under the aforementioned subsection, the supervisory authority may issue further regulations on the certificate to be used to ensure that gambling transactions and player account transactions remain unchanged, the technical format for the transmission of gambling transactions and player account transactions, and the technical requirements for connecting to the interface of the supervisory authority's supervision system.

According to section 57 of the Gambling Act, the supervisory authority is the Finnish Supervisory Agency. According to section 106 of the Act, the National Police Board shall act as the competent authority referred to in section 57 until 30 June 2027.

1.2 Legislation

The following regulations are relevant to the subject matter of this order:

- Gambling Act (10/2026)
- Administrative Procedure Act (434/2003)

1.3 Scope

This provision shall apply to the holder of an exclusive licence within the meaning of the Gaming Act and to the holder of a gaming licence. The exclusive licence is governed by Section 5 of the Gambling Act and the gambling licence is governed by Section 6.

1.4 Definitions

For the purposes of this provision, the following definitions shall apply. For the purposes of this regulation:

Document: ID-26412180

Re: POL-2025-121617

- customer data means records made to a gaming account relating to the registered player's customer account, identification, and the monetary transfer and loss limits set by the player; customer data form part of gaming account transaction data and relate to customer-specific information, such as the player's gaming, loss and monetary transfer limits;
- data vault means a separate service implemented by the licence holder from which the supervisory authority retrieves game transaction data and gaming account transaction data;
- Official Control Signing Service (OCSS) means the electronic signature service used and provided by the supervisory authority;
- gambling transaction means the stake wagered by the player on the game, the outcome option chosen by the player, the choices made by the player which are relevant to the outcome of the game and the results of the markets and draws, as well as any winnings and losses recorded in the gambling system of the holder of an exclusive licence or gambling licence;
- player account transaction means account entries;
- gambling system means an online information system used by or on behalf of the gambling operator for the operation of gambling;
- gambling licence means a permit to operate gambling services within the meaning of section 6 of the Gambling Act;
- SFTP user means a user account created for the supervisory authority, which the authority uses to log in to the data vault via an SFTP connection using the SSH public key stored by the licence holder;
- transaction date means the UTC calendar day during which the game transaction or gaming account transaction was generated in the licence holder's system;
- data transfer date means the UTC calendar day on which the data are transferred to the data vault. The data shall always be submitted to the folder corresponding to the data transfer date, regardless of the original date of the transactions.
- checksum file means a file containing the SHA-256 checksum of the data being submitted, the purpose of which is to ensure the integrity of the data;
- an exclusive licence means a permit to operate gambling services within the meaning of section 5 of the Gambling Act.

2 Gaming and player account transactions

The holder of an exclusive licence and the holder of a gambling licence shall transmit to the supervisory authority, in a format determined by the supervisory authority, the gambling transactions and player account transactions of the gambling services provided by the licence holder.

Game and gaming account transaction data shall be submitted to the supervisory authority within a reasonable period after the conclusion of the transaction. A period of no more than two weeks shall be considered a reasonable period.

For the purposes of this Regulation, a gambling game shall be deemed to have ended when its outcome has been determined or when the game has otherwise been brought to its final state in the licence holder's system. This also covers situations where the transaction is cancelled or voided. Game transaction data may also be submitted before the gambling game has ended, provided that the data have been generated in the licence holder's system.

The licence holder shall ensure that game transaction data and gaming account transaction data are made available to the supervisory authority through the data vault in accordance with this Regulation.

2.1 Signature requirement for game transaction data and gaming account transaction data

The licence holder shall ensure that all game transactions and gaming account transactions submitted to the supervisory authority are electronically signed using the OCSS signature service provided by the supervisory authority.

More detailed technical requirements concerning the creation, content and verification of signatures for game transactions and gaming account transactions are laid down in the supervisory authority's Regulation on the electronic certificate provided for in the Gambling Act.

2.2 Retention obligation for game transaction data and gaming account transaction data

The licence holder shall retain the game transaction data and gaming account transaction data relating to the gambling games it operates for at least five years. The licence holder shall ensure that gaming data stored for long-term retention remain unaltered throughout the entire retention period.

The data submitted to the data vault and the data retained for long-term storage constitute separate datasets intended for different purposes. The data vault is intended as the transmission channel for game transaction data and gaming account transaction data submitted to the supervisory authority. Long-term retention ensures that the data are preserved for the period required under section 45 of the Gambling Act.

Long-term retention may be implemented using the technical solution and storage format chosen by the licence holder. Long-term retention may consist, for example, of a data vault maintained in connection with the licence holder's gaming systems or another equivalent solution. The data vault may also be used for long-term retention, provided that the data are not stored within the folder structure intended for submitting data to the supervisory authority.

The licence holder shall, upon request, be able to restore data from long-term retention in the format required by the supervisory authority and submit them to the data vault in the folder structure intended for the supervisory authority. This obligation applies throughout the entire five-year retention period, regardless of whether the data are retained in the data vault in a separate retention structure or in another approved long-term retention solution.

If deficiencies are identified in the game transaction data or gaming account transaction data submitted by the licence holder to the data vault, the licence holder shall submit the corrected data without delay to the folder structure intended for the supervisory authority.

3 Data Vault

The data vault is a service operated by the licence holder and used to make game transaction data and gaming account transaction data available to the supervisory authority in accordance with section 45 of the Gambling Act. The technical implementation, maintenance and related solutions for the data vault are the responsibility of the licence holder. The service may be implemented either as an in-house solution or by procuring it from an external service provider. The licence holder shall be responsible for ensuring the integrity of the data submitted to the data vault, regardless of the technical implementation chosen.

The game transaction data and gaming account transaction data in the data vault intended for the supervisory authority shall be generated from the data produced by the gaming system and converted into the format specified by the supervisory authority's data model in accordance with separate technical regulations.

Only game transaction data and player account transaction data referred to in section 45 of the Gambling Act may be submitted to the directories of the data vault intended for the supervisory authority, unless the submission of other data to the directory structure has been agreed with the supervisory authority.

The supervisory authority shall be provided with independent access to the data vault in accordance with this Regulation, enabling it to retrieve the data required for the performance of its supervisory duties. The supervisory authority shall retrieve data from the data vault within the scope of the access rights granted to it and using the available data transfer protocols.

The licence holder shall be solely responsible for implementing the data vault in accordance with this Regulation and the technical instructions published by the supervisory authority. Following the grant of the licence, the licence holder and the supervisory authority shall carry out integration testing to verify that the supervisory authority has access to the data vault and that the data vault complies with the technical requirements laid down in this Regulation. The supervisory authority shall provide the licence holder with more detailed instructions concerning integration testing after the licence has been granted.

3.1 Technical and information security requirements for the data vault

The licence holder may implement the data vault using a technical solution of its choice, provided that the data vault complies with the technical requirements set out in chapter 3.1 and with the other requirements laid down in this Regulation.

3.1.1 Availability and Operational Reliability

Availability means the period during which the supervisory authority is able to retrieve the data stored in the data vault in accordance with this Regulation. Service downtime means the period during which the data are unavailable due to reasons attributable to the licence holder. Disruptions attributable to the supervisory authority and planned service interruptions notified in advance shall not be taken into account when assessing availability.

- The data vault shall enable the supervisory authority to retrieve the data without interruption and without undue delay.
- The availability of the data vault shall be at least 98% per month.
- The licence holder shall have procedures in place for managing service interruptions, reporting disruptions and restoring the service without delay.
- The supervisory authority's access rights shall not be blocked, restricted or slowed down without justified reason.
- All files submitted to the destination folders designated by the supervisory authority shall be retained for a minimum of 30 days and a maximum of 90 days from the date of submission. The licence holder may choose the retention period within the above-mentioned time frame. The data shall be deleted no later than 90 days after their submission. This Regulation does not affect the licence holder's obligation to retain game and player account transaction data for at least five years in a separate long-term storage solution.
- The licence holder shall ensure that the data stored in the data vault can be re-stored in the event of disruptions.

3.1.2 Access Management

- Access to the directory structure of the data vault intended for the supervisory authority shall be restricted to persons and entities that have an operational need for such access. The licence holder shall maintain an up-to-date list of users and shall provide it to the supervisory authority upon request.
- Keys and other authentication credentials provided for access to the data vault shall be handled, stored and protected in accordance with generally accepted information security standards.
- The supervisory authority shall be responsible for the proper use and management of its own authentication credentials.

Document: ID-26412180

Re: POL-2025-121617

- Network traffic to the data vault shall be restricted by means of a firewall. The firewall shall block all other network connections except those necessary for access to the data vault.
- With regard to access management, the handling, storage and protection of keys shall comply with generally accepted standards and principles.
- The licence holder shall ensure that access rights relating to keys are limited to the minimum necessary for their intended use.
- The licence holder shall ensure that all actions relating to keys are logged and monitored.

3.1.3 Logging

- Logs shall be generated for operations relating to the use of the data vault. The logs shall include, as a minimum, information on file transfers and file deletions, as well as user management events, including login and modification events.
- The logs shall not be altered or deleted and shall be retained for at least one year.
- The logs shall remain under the control of the licence holder and shall be provided to the supervisory authority upon request.

3.1.4 Data Integrity and Immutability

- The licence holder shall ensure that material stored in the directory structure of the data vault intended for the supervisory authority cannot be modified retrospectively without the modification being detectable.
- All submitted material shall remain unaltered throughout its entire lifecycle.
- Game and player account transaction data submitted to the data vault shall be signed using the OCSS service.
- To ensure the integrity of data transmission, SHA-256 hash files shall be generated for the files to be submitted in accordance with chapter 3.3.5. Once the hash file has been generated, the files shall not be modified or overwritten. If the submitted data are incorrect or incomplete, replacement game data shall be submitted in accordance with the instructions set out in this Regulation. Incorrect or incomplete files may not be deleted until at least 30 days after their submission.

3.1.5 Documentation

- The licence holder shall maintain documentation describing the architecture of the data vault, access management, logging, and procedures for managing disruption situations.
- The documentation shall be provided to the supervisory authority upon request.

3.1.6 Obligation to Notify of Incidents

- The licence holder shall notify the supervisory authority without undue delay if there is reason to suspect an incident that may compromise the reliability of the data vault or the availability or immutability of the data to be provided to the supervisory authority.
- The notification shall be made in the manner separately specified by the supervisory authority. The supervisory authority may issue more detailed instructions concerning the notification procedure and the procedures to be followed in exceptional situations.

3.2 Directory Structure of the Data Vault

The licence holder shall submit game transaction data and player account transaction data to the data vault as JSON Lines (JSONL) files compressed using the gzip format. Each gzip file shall contain a single JSON Lines file.

Within the directory structure, game transaction data and player account transaction data shall be stored in separate directories. Within these directories, the structure shall be based on the date on which the files are transferred. The files shall be placed in the directory for the day on which they are transferred to the data vault, regardless of the transaction date to which the data relate.

The transaction date included in the file name shall indicate the period to which the contents of the file relate, whereas the directory structure shall indicate the date on which the file was submitted. Files may be placed in the specified directory structure only once they are ready to be retrieved. Incomplete files shall not be stored in the specified directories.

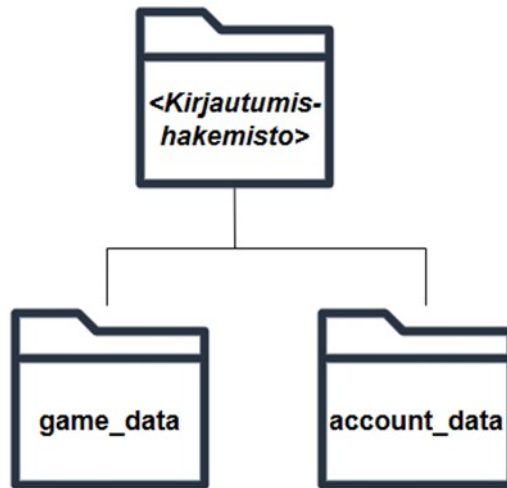
In addition, the hash files referred to in chapter 3.3.5 shall be placed in the specified directory structure. The hash file shall be generated only after the corresponding file has been transferred in its entirety. The hash file shall be placed in the same directory as the corresponding file.

The supervisory authority shall have access to the submitted data immediately after the file has been transferred to the data vault and the corresponding hash file has been created in the data vault in accordance with this Regulation.

No other files may be placed in the directories without the approval of the supervisory authority.

Document: ID-26412180

Re: POL-2025-121617

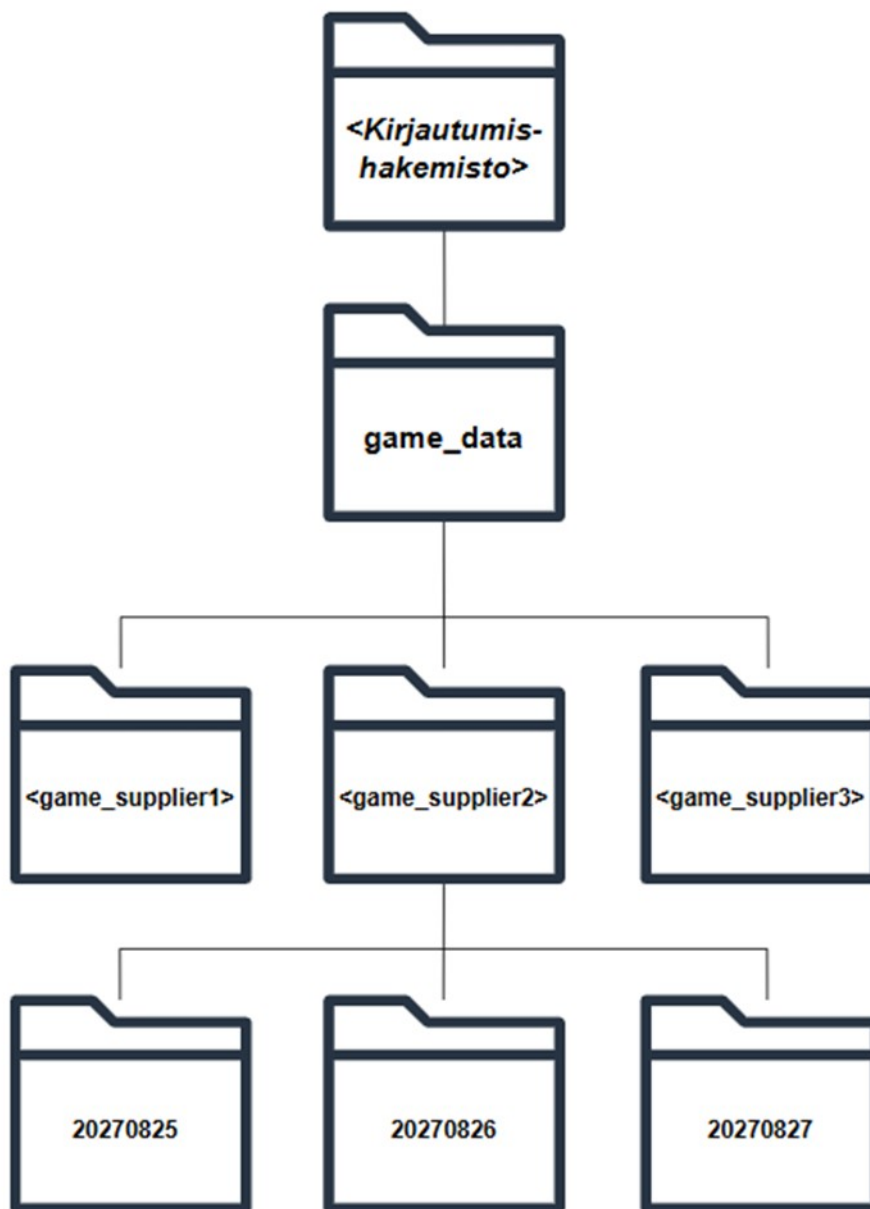


Login Directory

Game data, account data

Figure 1, Description of the service top level folder structure.

At the top level of the directory structure is the supervisory authority's login directory. This directory shall open automatically when the supervisory authority logs into the data vault using its SFTP user account. Game transaction data shall be submitted to the game_data directory in the data vault, and player account transaction data shall be submitted to the account_data directory.



Login Directory

Game data, game provider

Figure 2, Directory structure within the game_data directory of the data vault.

The game_data directory for game transaction data shall be divided into one or more subdirectories designated by the licence holder. The name of a subdirectory shall not ex-

Document: ID-26412180

Re: POL-2025-121617

ceed 40 characters and may contain only lowercase letters a–z, digits 0–9, and underscores (_). The name shall begin with a lowercase letter.

There may be one or more subdirectories. However, the licence holder may use multiple subdirectories, for example, to restrict access rights or to organise game transaction data where the game transaction data originate from a source other than the licence holder's own gaming system. The use of multiple subdirectories and the allocation of game transaction data between them shall be mandatory where more than one separate file is generated for the same game type, for example where game transaction data are produced in separate files for different gaming platforms.

Each subdirectory shall contain directories organised by the date of transfer. The transfer date shall be the date on which the relevant file was transferred to the data vault and made available to the supervisory authority. The date shall be presented in the format YYYYMMDD, for example 20271231, and shall be determined according to the UTC calendar day.

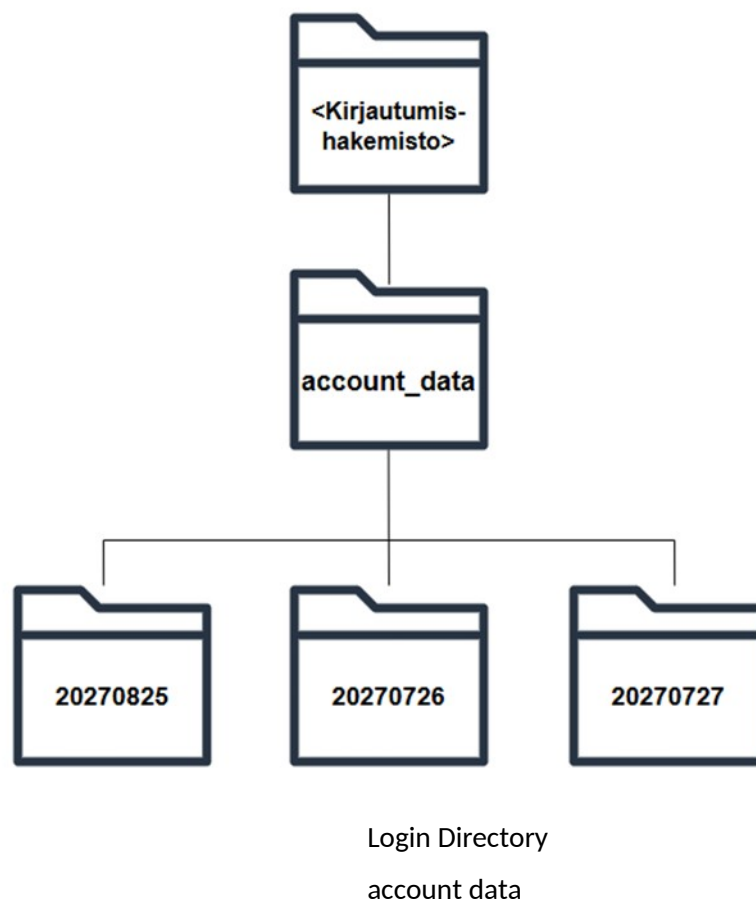


Figure 3, Directory structure within the account_data directory of the data vault.

The account_data directory shall be divided directly into subdirectories named according to the data transfer date. As with game transaction data, player account transaction data shall always be stored in the directory corresponding to the date on which the data are transferred. For example, data transferred on 1 July 2027 shall be stored in the 20270701 directory.

3.3 File Naming

The licence holder shall submit to the data vault the game transaction data and player account transaction data required by the supervisory authority in accordance with the separate regulations governing the technical format for submitting such data. The regulations governing the technical submission format specify the data to be recorded for each game transaction and player account transaction, the structure of the data and the permitted values.

Files containing game transaction data and player account transaction data shall be named in accordance with the requirements laid down in this Regulation. The file naming convention shall depend on the data being submitted and the purpose for which the file is submitted.

3.3.1 Versions and the Use of Version Numbers

A version shall contain one UTC calendar day (transaction date) of data of a particular type. The data types are defined in Sections 3.3.2 and 3.3.3 of this Regulation. A UTC calendar day begins at 00:00:00 UTC and ends at 00:00:00 UTC on the following day. It is permissible for the final transactions of a UTC calendar day to be included in the file for the following calendar day.

A version shall not be supplemented or modified in part. As a general rule, one version shall be submitted for each transaction date. The creation of more than one version shall constitute an exceptional situation. In such exceptional situations, where an error or omission is identified in the submitted data, a new version shall be submitted that replaces the previous version in its entirety. The new version shall contain all data included in the previous version together with any missing, corrected or amended data. Missing, corrected or amended data shall be appended to the end of the new version in such a way that the transaction sequence of the original version and the associated OCSS signatures are preserved as far as possible. The new version may be submitted after the original submission date once the error has been identified.

3.3.2 Player account transaction data

Player account transaction data are divided into three file types:

- player_profiles: Player profile data.
- player_rewards: Bonus and other similar player reward data.

- player_transactions: Financial transactions relating to the player account.

1) player_profiles

Files containing player_profiles data shall be named as follows:

- player_profiles-<transaction_date>-v<version_number>.jsonl.gz

where:

- <transaction_date>: The date on which the player's information was changed or recorded in the licence holder's gaming system. It is permissible for the final transactions of a UTC calendar day to be included in the file for the following calendar day. Transactions shall never be omitted in their entirety. The date shall be in the format YYYYMMDD, for example 20271231, and shall be determined according to the UTC calendar day.
- <version number>: The version number of the file for the same day, which shall normally be 1. If, in an exceptional situation, multiple versions of the file are submitted to the data vault in the same directory, version numbers 1 to n shall indicate the version concerned. The most recent version shall replace all preceding versions in their entirety.

Example:

- player_profiles-20271230-v1.jsonl.gz

2) player_rewards

Files containing player rewards, such as bonuses, shall be named as follows:

- player_profiles-<event date>-v<version number>.jsonl.gz

where:

- <transaction_date>: The date on which the player account transactions contained in the file were generated in the licence holder's gaming system. It is permissible for the final transactions of a UTC calendar day to be included in the file for the following calendar day. Transactions shall never be omitted in their entirety. The date shall be in the format YYYYMMDD, for example 20271231, and shall be determined according to the UTC calendar day.
- <version number>: The version number of the file for the same day, which shall normally be 1. If, in an exceptional situation, multiple versions of the file are submitted to the data vault in the same directory, version numbers 1 to n shall indicate the version concerned. The most recent version shall replace all preceding versions in their entirety.

Example:

- player_rewards-20271230-v1.jsonl.gz

3) player_transactions

Files containing player account financial transactions shall be named as follows:

- player_transactions-<event date>-v<version number>.jsonl.gz

where:

- <transaction_date>: The date on which the player account transactions contained in the file were generated in the licence holder's gaming system. It is permissible for the final transactions of a UTC calendar day to be included in the file for the following calendar day. Transactions shall never be omitted in their entirety. The date shall be in the format YYYYMMDD, for example 20271231, and shall be determined according to the UTC calendar day.
- <version number>: The version number of the file for the same day, which shall normally be 1. If, in an exceptional situation, multiple versions of the file are submitted to the data vault in the same directory, version numbers 1 to n shall indicate the version concerned. The most recent version shall replace all preceding versions in their entirety.

Example:

- player_transactions-20271228-v1.jsonl.gz

3.3.3 Game transaction data

Game transaction data shall be divided into separate files according to game type:

- webcasino: online casino games (electronic gaming machines, table games, live casino and e-bingo)
- poker: online poker (cash games and poker tournaments)
- fixed_odds_betting: fixed-odds betting and virtual betting
- pool_betting: pool betting
- lottery: lottery games operated by the holder of the exclusive licence
- scratchcards: physical scratch cards
- electronic_scratchcards: electronic scratch cards
- slot_machines: gaming machines operated by the holder of the exclusive licence
- casino_games: other games offered by the holder of the exclusive licence at casinos and gaming venues.

Game transaction data files shall be named as follows:

- <game_type>-<event date>-v<version number>.jsonl.gz

where:

- `<game_type>`: The game type, such as webcasino, poker, fixed_odds_betting or pool_betting.
- `<transaction_date>`: The date on which the game transactions contained in the file were generated in the licence holder's gaming system. It is permissible for the final transactions of a UTC calendar day to be included in the file for the following calendar day. Transactions shall never be omitted in their entirety. The date shall be in the format YYYYMMDD, for example 20271231, and shall be determined according to the UTC calendar day.
- `<version number>`: The version number of the file for the same day, which shall normally be 1. If, in an exceptional situation, multiple versions of the file are submitted to the data vault in the same directory, version numbers 1 to n shall indicate the version concerned. The most recent version shall replace all preceding versions in their entirety.

Example:

- fixed_odds_betting-20271231-v1.jsonl.gz

3.3.4 Regeneration of Files

The supervisory authority may, by means of a separate written request, require the licence holder to regenerate and submit game transaction data or player account transaction data from long-term storage to the directory structure of the data vault intended for the supervisory authority.

The regenerated data shall be submitted in the format specified by the supervisory authority and to the same directory structure as other data of the same type. The same file formats, compression methods and hash files shall be used for regenerated data as for other data submitted in accordance with this Regulation.

The regenerated data shall be signed with a single OCSS signature covering the entire file. The regenerated data need not be bit-for-bit identical to the original files.

Regenerated files shall be distinguished from other files in the directory by their file names. The element "by_request" shall be added to the file name of files regenerated at the request of the supervisory authority. In the file name, "by_request" shall be inserted between the transaction date and the version number.

Examples:

- fixed_odds_betting-20271228-by_request-v1.jsonl.gz
- player_transactions -20271228-by_request-v1.jsonl.gz
- player_rewards -20271230-by_request-v1.jsonl.gz

3.3.5 Hash Files

Once a file to be submitted has been transferred in its entirety to the directory structure of the data vault intended for use by the supervisory authority and is ready to be retrieved, a hash file containing the file's SHA-256 hash in hexadecimal format shall be placed in the same directory. The hash file shall serve as an indication to the supervisory authority that the file is ready to be retrieved.

The name of the hash file shall otherwise correspond to the name of the transferred file, with the extension ".sha256" appended. The hash file enables the supervisory authority to verify that the file has been transferred completely and without modification.

The contents of the hash file shall consist solely of the file hash. The hash shall be represented as a 64-character hexadecimal string in lowercase, without spaces or any other characters. A single line feed character (LF, U+000A) may be appended after the hash.

Example of a hash file name:

- webcasino-20271230-v1.jsonl.gz.sha256

Example of the contents:

- e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855

4 Retrieval of data from the data vault

The supervisory authority shall check daily whether files are available for retrieval in the directories of the data vault. If interruptions occur during data transfer or files are not submitted on a daily basis, the files shall be retrieved in the order of their transfer dates. The supervisory authority shall maintain, in its own system, a record of the files that have been retrieved.

4.1 Establishment of connections

The licence holder shall provide the supervisory authority with independent access to the data vault via an SFTP (SSH File Transfer Protocol) connection. The solution shall support SFTP version 3. The connection shall be unidirectional, with the supervisory authority retrieving the submitted files from the data vault. The licence holder shall prevent unauthorised access to the data vault.

The licence holder shall open and communicate the static connection details required to access the data vault (for example, a DNS name or IP address), open the required ports, and configure the service so that the supervisory authority can establish an SFTP connection and retrieve data as required.

The supervisory authority shall generate an Ed25519 SSH key pair, and the public key shall be stored on the licence holder's service. The licence holder shall create a user ac-

count for the supervisory authority and shall disable password-based authentication for SFTP connections.

The supervisory authority shall issue separate instructions containing more detailed information on establishing, testing and maintaining connections.

The data vault shall be configured so that, when the supervisory authority logs in, the default directory is the login directory shown in Figure 1 of Section 3.2.

In exceptional situations, the licence holder and the supervisory authority may also agree on other methods of data transfer.

4.2 Updating Connections and Keys

The licence holder and the supervisory authority shall coordinate the resolution of issues relating to cryptographic keys so as to ensure that the supervisory authority always has the keys required for the performance of its supervisory duties. The licence holder shall ensure that the public key of the valid SSH key pair provided by the supervisory authority is stored in the data vault. SSH keys shall be replaced where necessary at the initiative of the supervisory authority.

If the licence holder detects any issues relating to SSH keys or the establishment of connections, it shall notify the supervisory authority without delay.

If the supervisory authority detects any issues relating to SSH keys, it shall notify the licence holder.

The licence holder shall not unilaterally modify the supervisory authority's network connections to the data vault or the configuration settings relating to the supervisory authority's access to the data vault. Any such changes shall be notified to the supervisory authority in advance.

4.3 Exceptional situations affecting data transfer

If the licence holder detects a technical problem that prevents the submission of the required data, it shall notify the supervisory authority without delay. The licence holder shall investigate the cause of the technical problem and, upon request, report its findings to the supervisory authority. If the licence holder's investigation gives reason to suspect that the problem is related to the supervisory authority's system, the supervisory authority shall participate in determining the cause of the technical problem.

5 Derogation for the holder of the exclusive licence

In place of the arrangements set out in this Regulation, the holder of the exclusive licence may, with the approval of the supervisory authority, continue to use existing integrations for the submission of game transaction data and player account transaction data relating to lotteries, betting games, gaming machines and casino games as referred

Document: ID-26412180

Re: POL-2025-121617

to in section 5 of the Gambling Act. Alternatively, the holder of the exclusive licence may submit the data through the data vault in accordance with this Regulation. Where the holder of the exclusive licence replaces the existing data transfer method with the data submission method provided for in this Regulation, it shall notify the supervisory authority of the change and coordinate the transition with the supervisory authority.

Regardless of the data transfer method used, the holder of the exclusive licence shall comply with the obligations laid down in section 45(1) and (2) of the Gambling Act concerning the retention of, and submission to the supervisory authority of, game transaction data and player account transaction data. In addition, where necessary, the holder of the exclusive licence shall be able to restore the abovementioned data to the supervisory authority, upon separate request, in accordance with section 2.2 of this Regulation.

6 Entry into force

This regulation enters into force on 1 July 2027.

The National Police Board
Gambling Administration
Riihimäki
Telephone , poliisi.fi