National Self Exclusion Platform (NSEP) Directive – XX/2023

A. National Self Exclusion Platform

1. Introduction

The purpose of this Directive is to describe the procedures and technical requirements which need to be implemented by Class B licensed operators in relation to the operation of the National Self Exclusion Platform (NSEP). The NSEP is a web-based service designed by the National Betting Authority (NBA) that aims to facilitate the exclusion of individuals from betting-related activity across all licensed online gambling providers operating in the Republic of Cyprus (Class B Licence holders). Central to this undertaking is the compilation and maintenance of a list of excluded players (henceforth the exclusion-list) and the provision of a REST API through which operators will be able to query this dataset and determine the exclusion status of their registered users, thus limiting their participation in betting accordingly.

2. Legal Basis

This Directive is drafted based on the provisions of regulation 23 of the Betting (Protection of Players, Minors and Pathological players) regulations of 2022 (or "Player Protection Regulations"), as amended or replaced.

The Player Protection Regulations can be found on nba.gov.cy.

3. Requirements

(1) The implementation of the procedures and technical requirements detailed in this Directive is mandatory for all Class B licensed operators.

(2) If according to the NSEP a player is excluded from a certain type of sport and/or league, then the operator must not permit the player to place a bet on said sport and/or league.

(3) If according to the NSEP a player is excluded from all types of betting, then the operator must not permit the player to place any bets or deposit money to his or her account.

(4) No message, advertisement or promotional action is sent to the player during the period of self-exclusion or after the period's completion, until the player reconnects and reoperates their account.

4. Information regarding the NSEP

(1) For the purposes of the Player Protection Regulations, the NSEP is considered part of the available self-protection measures of each Class B licensed operator. Accordingly, Class B licensed operators must include where necessary:

(i)   the relevant links and information regarding the NSEP, as well as explain the difference between the NSEP and the operator's self-exclusion system;

(ii)   instructions on how to use the NSEP.

(2) Class A and B licensed operators must provide direct access to the NSEP through a sensitive web link in the footer of every webpage of their website (www.exclusion.cy).

B. Technical Requirements

1. Introduction

This chapter details the technical requirements of the NSEP and aims to provide details on how the communication between the platform and the licensed Class B licensed operators is implemented and what specific data is exchanged in the process.

2. Workflows

A Class B operator determines the exclusion status of a user through workflows described in this section. In doing so, at least one of the following data sources needs to be queried:

1. **Live Exclusion Dataset.** This is the most recent version of the exclusion status of users registered in NSEP. It is maintained by the NBA and an operator may access it using the NSEP API described in this document.
2. **Daily Exclusion Dataset.** This is a daily snapshot that contains data pertaining to all excluded users that are registered with a particular operator. It is compiled or updated on a 24-hour cycle by querying the Live Exclusion Dataset through the NSEP API and is maintained on the operator's side. Once generated it can be directly accessed by the operator's system without requiring communication with the NSEP.
3. **Local Exclusion Dataset.** This contains exclusion data collected through self-exclusion workflows that are explicitly facilitated by an operator's platform. Both its generation and maintenance thus take place on the operator's side.

There are two distinct event-triggered workflows which require the retrieval of exclusion data from the sources listed above. A third process needs to be scheduled daily for the compilation or update of the Daily Exclusion Dataset.
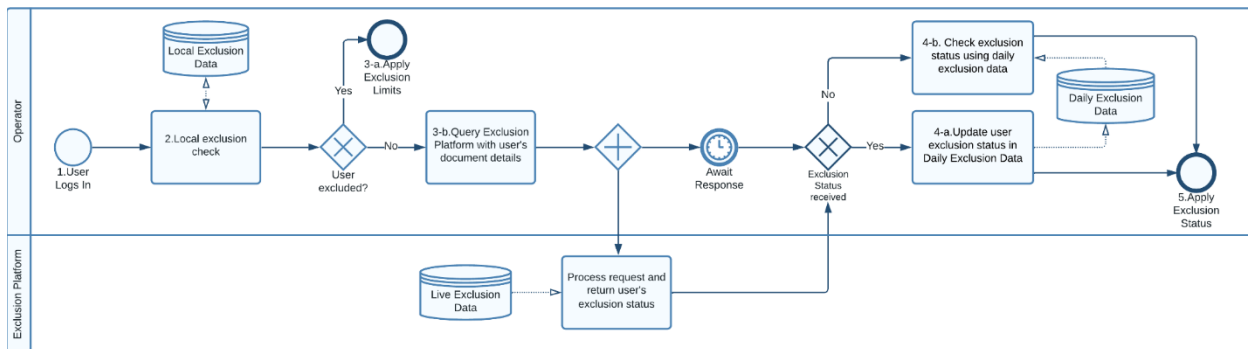
2.1 Retrieval of Exclusion Status at user login

At each and every user login, the exclusion status of a user needs to be determined and potential limits be applied to their profile before any betting activity is allowed.

To that end, the user details are first checked against the Local Exclusion Data in the operator's system. If no exclusion is found, the operator performs a second check by querying the NSEP API and thus accessing the Live Exclusion Dataset.

In cases where the API is temporarily unavailable, the Daily Exclusion Dataset, which is stored on the operator's systems, is employed as a backup source.

The process is depicted below. A description of its flow is provided in Table 2.1

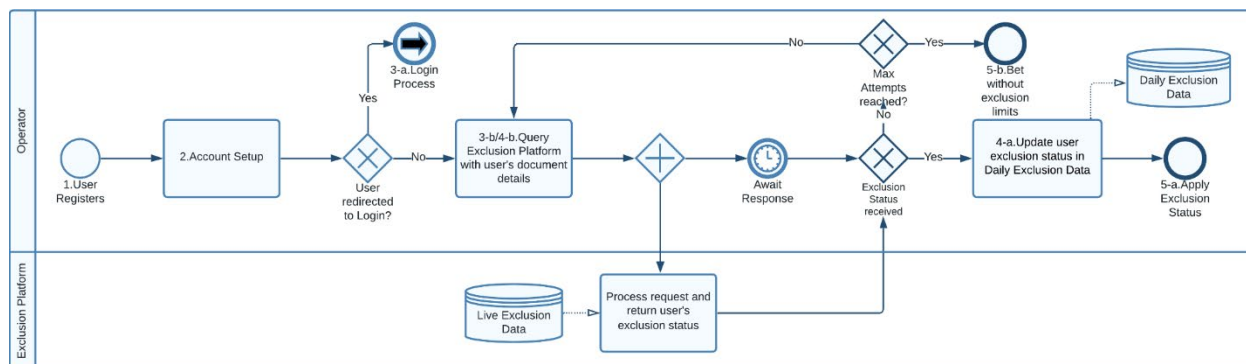| Flow Description - Process 2.1: *Exclusion Status check at User Login*	
1	The process is initiated when a user attempts to log into the operator's platform.
2	The operator checks whether the user has active exclusions in the Local Exclusion Data.
3-a	If an active exclusion exists, it is applied. The process terminates.
3-b	If no exclusion is found in the Local Exclusion Data, the operator queries the Exclusion Platform API with the required user details.
4-a	If a response is received, the operator's system updates the Daily Exclusion Data with the received user's exclusion status.
4-b	In cases where the NSEP API fails to respond to the operator's request, the user's exclusion status is retrieved from the Daily Exclusion Data.

| 5 | The exclusion status is applied. If the status translates to no exclusion, all betting activity is allowed, otherwise limits are imposed in accordance with Table 4.6 |

Table 2.1

2.2 Retrieval of Exclusion Status at user registration

Once a user registers with an operator, their Exclusion Status needs to be determined and applied to their profile by querying the NSEP API and thus accessing the Live Exclusion Dataset. Note that in systems where a newly registered user is always redirected to login, this workflow might not be necessary, provided the check will take place through process 2.1 above.

The process is depicted below. A description of its flow is provided in Table 2.2.

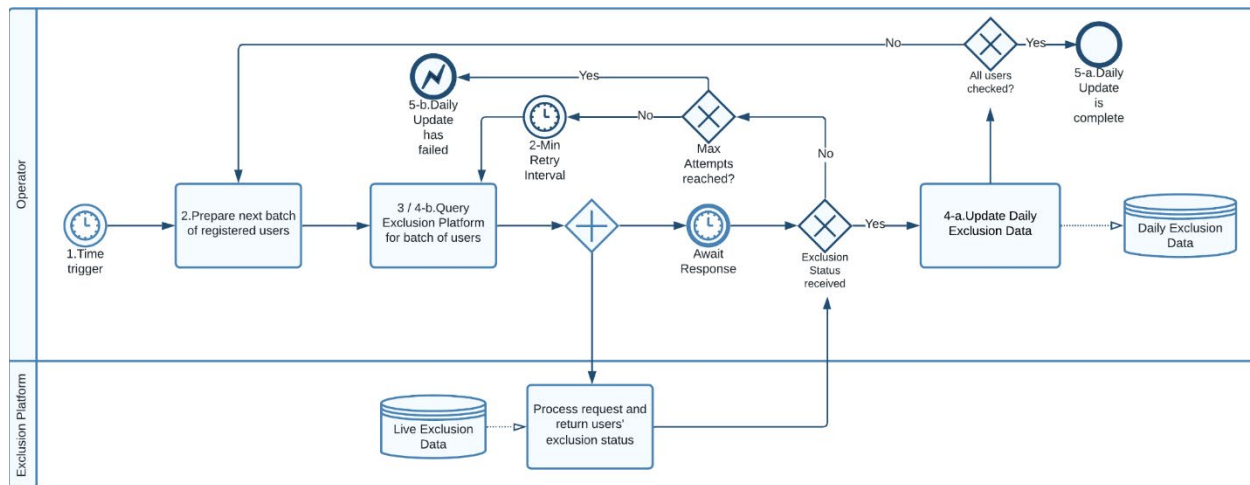| Flow Description - Process 2.2: Exclusion Status check at User Registration	
1	The process is initiated when a user registers in the operator's platform.
2	The user provides all necessary details during the account setup stage.
3-a	Once setup is completed, the user is redirected to log-in. Process 2.1 is followed.
3-b	If there is no re-direction and the user is logged into their newly set account directly, the operator's system queries the Exclusion Platform for the user's exclusion status.
4-a	If a response is received, the operator's system updates the Daily Exclusion Data with the new user's details and exclusion status.
4-b	In cases where the Exclusion Platform fails to respond to the operator's request, the operator is required to resend the query for a second attempt.
5-a	The exclusion status is applied. If the status translates to no exclusion (status "0" in accordance with Table 4.6), all betting activity is allowed, otherwise limits are imposed in accordance with Table 4.6.
5-b	After two failed attempts, the Exclusion Platform is considered to be temporarily unavailable. No exclusion limits are applied to the player. The operator is required to notify the failed communication to the NBA.

Table 2.2

2.3 Compilation / Update of the Daily Exclusion Data

On a daily basis, an operator is required to execute a check for the exclusion status of their entire set of registered users. The result of this process is the Daily Exclusion Dataset, which contains all registered users that have been found to be excluded, along with the exclusion category and expiration date. Note that players with exclusion status 0 ("No exclusions" - see Table 4.6) need not be stored in this dataset, though operators may still include them.

The Daily Exclusion Data is derived from the Live Exclusion Dataset that resides on the NSEP side. The former is compiled by dispatching sequential calls to the NSEP API, each call containing details for a number of user identification documents. The maximum number of user documents that can be included in a single query is 4000.

The process is depicted below. A description of its flow is provided in Table 2.3. Note that any steps taken beyond retrieving the information from the NSEP are indicative (step 4-a in the flow

diagram); the operator may follow that process that better suits their own configuration provided the final output is achieved.

Flow Description - Process 2.3: *Exclusion Status daily update*	
1	The process is initiated at a predetermined time on a daily basis. An exact time slot is communicated to the operator by the NBA.
2	The operator prepares the required data in batches. Specifically, a single request to the Exclusion Platform should contain no more than 4000 entries (details for 4000 identification documents).
3	A request is sent to the exclusion platform through the NSEP API.
4-a	If a response is received, the operator's system updates the Daily Exclusion Data with the new user's details and exclusion status.
4-b	In cases where the Exclusion Platform fails to respond to the operator's request, the operator is required to resend the query for a limit of five (5) attempts. Any retries should be carried out at 2-minute intervals.
5-a	All registered players have been checked against the Live Exclusion Dataset. The Daily Exclusion Dataset is now complete / updated and the process terminates.
5-b	After five (5) failed attempts, the Exclusion Platform is considered temporarily unavailable. The Daily Exclusion Dataset remains unchanged but should still be used when required as a backup source, taking into account the expiration date recorded for each exclusion. The operator is required to notify the failed communication to the NBA.

Table 2.3

2.4 Marketing material

Players that are under any category of exclusion should always be excluded from any type of marketing campaign. This includes messages, advertisements and promotions. To that end, an operator should query their Daily Exclusion Dataset and make sure that excluded users receive no advertising material.

3. Connectivity Requirements

An operator may initiate requests to the NSEP platform once the following prerequisites have been met:

3.1 Operator IP Address Whitelisting

The operator is required to provide to the NBA the IP address from which requests will be sent to the NSEP platform. Requests dispatched from a non-registered IP address will not be served.

3.2 Connectivity Credentials

The NBA will provide each operator with a unique username and password combination. Any call to the API needs to include these credentials as a header, in the manner described in Section 4.2.

4. API Specification

Licensed Operators can query the National Exclusion Platform by means of a Representational State Transfer (REST) API. A single GET method is exposed to the operators, through which they are able to query the platform on the exclusion status of one or multiple players.

4.1 API Methods and Endpoints

Method	Endpoint URL
GET	https://www.exclusion.cy/api/bookmakers/playerStatus

Table 4.1

4.2 Request Structure

4.2.1 Headers

A request requires to have the following headers in order to be successfully authenticated and processed:

Authorization

For a request to be successfully authenticated and authorized, the username and password strings need to be concatenated with a colon placed exactly between them and no spaces, resulting in a string of the form **<username>:<password>**. This string is then encoded in Base64 and prefixed with **Basic<space>** before being used as the value of the Authorization header.

Transaction-Id

The Transaction-Id key takes a value that is generated by the operator's system and is used as an identifier for the transaction. Provided the request is successfully processed (response status 200 - see Table 4.7), the same Transaction-Id is included in the Header of the response, in order to match it to its initiating request without ambiguity. This field can take any arbitrary sequence of ASCII characters as its value. It is the responsibility of the bookmaker to ensure proper usage, e.g., by avoiding the use of the same values for transactions that are not separated by a significant time interval.

KEY	VALUE	COMMENT	EXAMPLE
Authorization	**Basic <username>:<password>**	The **<username>:<password>** combination needs to be encoded in base64.	For username *test* and password *123456* the expected value is **Basic dGVzdDoxMjM0NTY=**
Transaction-Id	Any sequence of ASCII characters.	This field is utilized as means of matching client requests to API responses. Its method of generation and level of complexity is thus arbitrary and is the responsibility of the operator.	**3fa85f64-5717-4562-b3fc-2c963f66afa6**

Table 4.2

4.2.2 Request Body

The body of the request contains the necessary data fields for one or more players that the operator wishes to look up in terms of their exclusion status. The data structure follows the JavaScript Object Notation (JSON).

An example is shown below:

```json
{
    "listOfPlayers": {
        "player": [
                {
                        "idDocType": "1",
                        "idDoc": "0904",
                        "issueCountryCode": "FRA"
                },
                {
                        "idDocType": "1",
                        "idDoc": "0905",
                        "issueCountryCode": "AUS"
                },
                {
                        "idDocType": "1",
                        "idDoc": "0902",
                        "issueCountryCode": "GRC"
                }

            ]

        }
}
```

A detailed description of the fields that are required for each player is provided in the table that follows:

KEY	VALUE	COMMENT	EXAMPLE
idDocType	Identification document type: 0 for passport 1 for Civil ID	The bookmaker can send details of a player's passport or civil id, depending on which of the two they have on record.	For a player's Civil Id, the expected value would be **"1"**
idDoc	Number of Identification Document (this can be alphanumeric)	Passport Number or Civil ID, in the exact form this is printed on the document (e.g., including any leading or trailing zeroes)	For a Civil ID issued by the Republic of Cyprus this is the number found under the "ID Card Number" field, e.g., **"0000823721"**
issueCountryCode	The ISO 3166 **Alpha-3 Code** of the Country by which the document was issued	A full list of codes can be found here.	The code for Cyprus would be **"CYP"**

Table 4.3

Note: A request may contain more than one entry for the same player in cases where the operator keeps more than one of that player's documents on record (e.g., passport and civil id).

4.3 Response Structure

4.3.1 Response Headers

A successful API response will contain the following header:

Transaction-Id

The Transaction-Id key takes the value that was included in the header of the request under the same key ("Transaction-Id") to allow the matching of the two by the client that initiated the request. The Exclusion Platform does not change this identifier in any way, it is sent back in the exact same form it was received.

KEY	VALUE	COMMENT	EXAMPLE
Transaction-Id	Any sequence of ASCII characters.	This field is utilized for the sole purpose of matching client requests to API responses. It is generated by the betting platform of the bookmaker and is included in the initial request (see 4.2.1). The NSEP Platform returns it in the response without applying any changes.	**3fa85f64-5717-4562-b3fc-2c963f66afa6**

Table 4.4

4.3.2 Response Body

Provided the sender's request has been successfully processed, the API returns with a status code 200 (a list of all possible statuses is provided in Table 4.7 and the body of the response contains data in the form of a JavaScript Object Notation (JSON) object, detailing exclusion details for each of the players the bookmaker inquired about. An example is shown below:

```json
{
    "listOfPlayersResponse": {
        "player": [
            {
                "id": "AA6C3E5188B71DEB577C4AE5EC750933C6FDF788",
                "exclusions": [
                    {
                        "exclusionCategory": "1",
                        "exclusionEndDate": "2023-04-17T00:00:00"
                    },
                    {
                        "exclusionCategory": "2",
                        "exclusionEndDate": "2024-04-17T00:00:00"
                    },
                    {
                        "exclusionCategory": "3",
                        "exclusionEndDate": "2025-04-17T00:00:00"
                    },
                    {
                        "exclusionCategory": "4",
                        "exclusionEndDate": "2026-04-17T00:00:00"
                    }
                ],
                "idDoc": "0904"
            },
            {
                "id": "FA27ACF4DE1286A052DCD055C6AD6FE5AB89455C",
                "exclusions": [],
                "idDoc": "0905"
            },
            {
                "id": "403C5AEB260387D0817C21D4297156C1FCD4C068",
                "exclusions": [
                    {
                        "exclusionCategory": "1",
                        "exclusionEndDate": "2023-04-17T00:00:00"
                    }
                ],
                "idDoc": "0902"
            }
        ]
    }
}
```

A detailed description of the player fields that are included in the body of a successful response for each player included in the original request is provided in the table that follows:

KEY	VALUE	COMMENT	EXAMPLE
id	A unique identifier for this player.	This is generated through the SHA-1 hashing algorithm and takes as input a concatenation of idDoc, issueCountryCode, idDocType and the string "NBA" (in this order) submitted for this player through the bookmaker's request.	For a player with input parameters idDoc:0000823721 issueCountryCode: CYP idDocType: 1 the id value is calculated using SHA-1("0000823721CYP1NBA") which results in **"70255EECD65E4D611C7375A2CBDBE4928F31AF7D"**
idDoc	Number of Identification Document	This corresponds to the idDoc field submitted for this player through the bookmaker's request.	**"0000823721"**
exclusions	List of the player's exclusions	In cases where there are no exclusions, this list will be empty	[]
For each exclusion in exclusions			
exclusion Category	A numerical value denoting the category of the exclusion.	Examples of exclusion categories are provided in Table 4.6 (the list is dynamic and will be updated accordingly from time to time).	If a player is excluded from sports betting the expected value is **"1"**
exclusion EndDate	Datetime string in the form of YYYY-MM-DDThh:mm:ss	The date at which the exclusion expires. Depending on the exclusion status, this field may not be applicable, in which case it is omitted.	**"2023-04-17T00:00:00"**

Table 4.5

Examples of Exclusion Categories

exclusionCategory Value	Exclusion Scope
1	All Sports Betting.
2	Men's Cypriot Football League Division A.
3	All Cypriot Sports Betting.
4	Cyprus Athletics.

Table 4.6

4.4 Response Status Codes

For requests that comply with the structure outlined in section 4.2, the API returns a response with Status 200, which contains all elements described in section 4.3. In cases where the request sent is erroneous in one or more ways, the response carries a different status code and contains informative feedback for debugging purposes.

A full list of the possible response status codes and their meaning is provided in Table 4.7 below.

Error in Request	Response Status	Error Feedback (Body)
No errors, the request complies with Section 4.2.	200 OK	No error feedback. The body contains information on player exclusions as described in Section 4.3.2.
One or more of the players included in the request is missing one or more input fields (idDocType, idDoc, issueCountryCode)	400 Bad Request	The body contains the JSON entries (players) that are missing one or more input fields, together with the message: "*One or more search terms is missing for one or more players. Check the mandatory terms (idDocType, idDoc, issueCountryCode) and send the request again*"
Missing key(s) or unexpected format in request body	400 Bad Request	"*Missing key(s) or unexpected format in request body*"

The Id-Transaction header is missing.	400 Bad Request	"*Missing header Transaction-Id*"
Authorization header is either missing or contains the wrong value.	401 Unauthorized	"*Unauthorized user, check header user credentials.*"
The user credentials refer to an inactive user. User activation / deactivation is managed by the NBA.	403 Forbidden	"*Given user with credentials is inactive.*"

Table 4.7