



Short Public Report Recertification No. 2

1. Name and version of the IT product or IT-based service:

ADMIRAL-Card-System – Controller Service; function as provided in December 2019

2. Manufacturer or vendor of the IT product / Provider of the IT-based service:

Company Name:



ADMIRAL Casinos & Entertainment AG (ACE)

Address:

Griesfeldstraße 15, 2351 Wiener Neudorf, Austria

Contact Person:

Emil Huber

3. Time frame of evaluation:

Re-Evaluation started: 22.10.2018

Re-Evaluation ended: 18.06.2020

4. EuroPriSe Experts who evaluated the IT product or IT-based service:

Name of the Legal Expert:

Hans-Jürgen Pollirer

Address of the Legal Expert:

Fischerstiege 9, 1010 Wien, Austria

Name of the Technical Expert:

Jürgen Stöger

Address of the Technical Expert:

Fischerstiege 9, 1010 Wien, Austria

5. Certification Authority:

Name: EuroPriSe Certification Authority

Address: Joseph-Schumpeter-Allee 25

53227 Bonn

Germany

eMail: contact@european-privacy-seal.eu

6. Specification of Target of Evaluation (ToE):

- ADMIRAL-Card-System Services
 - Registration and creation of the customer (card)
 - Collection of biometric data (fingerprint)
 - Logging of times of attendance
 - Logging of stakes
 - Queries
 - Issuing and cancellation of prevention of access or prohibition of entry

- Processing of log data
- Credit screening
- PEP-Check (politically exposed person)
- High-risk-check (check of money laundering or terrorism financing)
- Interfaces of the ADMIRAL-Card-System
- Interface to the Federal Data Processing Center
- Interface/connections to the internet
- Interface to the server room of the company headquarter

The target of evaluation does not include:

- Other processes carried out by the data processing centre
- Third party networks (e.g. internet)
- ACE-Hotline
- Video surveillance of the turnstiles
- Advertising

7. General description of the IT product or IT-based service:

The ADMIRAL Casinos & Entertainment AG (ACE) - a 100% subsidiary of the NOVOMATIC AG - operates entertainment casinos in several locations in Austria. Legal basis is the Österreichisches Glücksspielgesetz (federal law) and relevant federal state laws, which require strong protective actions against compulsive gambling. ACE has therefore developed the ADMIRAL-Card-System, based on the NOVOCARD™-Ampelsystem. The ADMIRAL-Card-System is a computer-assisted system for data subjects, with procedures for access control and gaming addiction countermeasures.

Before entering an entertainment casino, each data subject has to prove its identity by submitting a photo ID. After verification of the data subject's legal age, his personal data is recorded by automatic readout of the photo ID as well as by manual input. The photo ID is scanned. In addition, an actual photo of the data subject is taken by means of a camera connected to the system. This photo is stored in the system and printed on the ADMIRAL-Card.

During registration a unique customer number is assigned to each data subject which allows explicit identification in the system. Moreover, the data subject chooses a four-digit PIN code. In the course of the registration process personal data of the data subject is collected on the basis of Article 6 (1) b, c GDPR. During the registration process or after that at any time the data subject is willing to do so, he can give his explicit consent according to Article 9 (2) a GDPR for the collection of his fingerprint. After registration the data subject receives his ADMIRAL-Card which is a combi-card with a smart-chip and a RFID-chip. Apart from the multi-digit customer number, no personal data is stored on the ADMIRAL-Card. The ADMIRAL-Card or the fingerprint enables the data subject to open the turnstile directly in front of the gaming area and to operate the gambling machine in combination with his PIN-Code. The central storage of data and the networking of all subsidiaries allow control of gambling frequency and behaviour.

The ACE warning system is based on the access control system and enables individual recording of gambling behavior (monitoring).

Due to the complete recording of the accesses to the entertainment casino as well as the exact recording of the gambling behavior directly at the gaming machine, the evaluation of the gaming intensity and frequency is possible. The data is evaluated at defined observation periods. From the first entry into the gambling area, the attendance time and frequency of participation in the game are recorded. This enables extensive monitoring measures in order to recognize potentially endangered customers at an early stage and to be able to effectively implement individually and tailor-made measures. The screening process delivers information about the dangers to financial existence and of compulsive gambling of the data subject. Additionally, the data subject has the possibility to abandon admittance permanently or for a certain period on a voluntary basis.

The data collected and processed, such as ID, photo and gambling behaviour represent the minimum of data necessary for the obligatory identification, verification and protection against compulsive gambling. Data avoidance and minimisation fully comply to general data protection principles. Regarding the transparency of the ADMIRAL-Card-System, the leaflets “Entertainment mit Verantwortung” and “Prävention ist der beste Spielerschutz” placed in the entertainment casinos give information about the

ADMIRAL-Card-System as well as advice regarding responsible gaming, self-test and contact addresses of therapeutic facilities. Because of high probability of gambling addiction, in case of an access ban – whether imposed by the system automatically or the data subject himself – the data subject is informed by an authorised and trained person in the entertainment casino.

The legal retention period is defined in accordance with section 132 Federal Fiscal Code (“Bundesabgabenordnung”) with 7 years. Under certain circumstances the retention period can be extended up to 30 years. Erasure of personal data occurs either on demand of the data subject, in accordance with the legal retention period or automatically after the end of this period, provided that the data subject has not entered an entertainment casino within the past 7 years.

Hardware and software for authenticating the data subject’s access to the gaming area has been delivered and developed by a third party provider who is also responsible for maintenance. The software necessary for the analysis of days and durations of attendance as well as gambling behaviour was also developed by a third party provider who is also responsible for maintenance. The ADMIRAL-Card-System is processed in the ACE-owned data processing service center. The Backup-Servicecenter is located in the data processing center of the HTM GmbH, which is also a 100% subsidiary of the Novomatic AG. Regarding the automatic imposition of an access ban, the transparency of this automatic transition is secured by the leaflet-information as well as by a briefing given by the location manager.

8. Transnational issues:

The ADMIRAL-Card-System is an IT-based Service offered by ACE in Austria only. Transmission of personal data to a processor situated in a “third country” takes places on the basis of the EU Standard Protection Clauses.

9. Tools used by the manufacturer of the IT product / provider of the IT-based service:

- Windows/Linux
- Apache/PHP
- Oracle DBMS

- Firebird DBMS
10. Edition of EuroPriSe Criteria used for the evaluation:
January 2017
11. Modifications / Amendments of the IT product or IT-based service since the last (re)certification
- The idea of the planned use of the Responsible Gaming Analyzer (RGA) will not be pursued due to problems in the software development process. With regard to Hardware and Software components the ADMIRAL-Card-System has been further enhanced by a Fingerprint System for the purpose of access control. The customer is able to agree to the usage of his biometric data (fingerprint) on his explicit consent.
12. Changes in the legal and/or technical situation
- A change of the legal regulation has taken insofar place as the retention period in section 5 Österreichisches Glücksspielgesetz (federal law) has been removed.
- Appropriate regulations in the federal laws are inconsistent, some of them have followed the regulation in the federal law, some of them contain a retention period of 5 years at the minimum.
13. Re-Evaluation methods:
- Analysis of ToE
 - Analysis of the Austrian federal gambling law and the relevant state laws
 - Analysis of the lawfulness of processing according to Article 6 and 9 GDPR
 - Verification of all relevant internal directives for the fulfilment of the rights of the data subject according to chapter III GDPR
 - Verification of correctness of retention periods
 - Verification of all contracts concluded with processors
 - Request and study of documents, guidelines, procedural instructions, configuration files, logging files of ADMIRAL-Card-System
 - Interviews and e-mail correspondence with responsible employees of ACE and developers at Octavian.SPb.
 - Inspection of the ACE headquarter in Wiener Neudorf
 - data center

- IT department including storage room
- Inspection of HTM data center in Gumpoldskirchen
- Inspection of A1 data center in Vienna, Antonigasse
- Assessment and demonstration of the ADMIRAL-Card-System (at the headquarters)
- Inspection of ADMIRAL branches in Wiener Neudorf (Lower Austria) and Hartberg (Styria)
- reliability check of the biometric subsystem (at the headquarters)
- Performing a penetration test on systems of the ADMIRAL-Card-System

14. Re-Evaluation results:

Considering the fundamental aspects of processing, it can be stated that the ADMIRAL-Card-System represents a system for preventing gaming addiction in full compliance with data protection regulations and in consideration of findings of addiction research.

Evaluation of the criteria concerning processed personal data has shown that all processed data are precisely specified and that data processing happens only on the basis of the GDPR. ACE complies fully with its information duty; effective processes have been implemented to honour the relevant rights of the data subject according to chapter III GDPR.

In the fundamental technical construction of the ADMIRAL-Card-System, data avoidance and minimization was given particular attention. Only data needed for data subject identification and gambling behaviour as well as for a possible ban on admittance is collected and processed.

Regarding transparency and product description, it is ascertained that on his first visit to an entertainment casino, the data subject is accurately informed about the fact that the ADMIRAL-Card-System is an electronic system, combining the obligation of registration with control of access and observation. In addition, two flyers placed in the entertainment casinos in eleven languages offer detailed information.

Legal basis for the processing of personal data is the Österreichisches Glücksspielgesetz entered into force on January 1st 2011, as well as the relevant federal state laws.

Regarding the depth of intervention with respect to the fundamental right of data protection, it should be noted that the legal requirements concerning identity verification, gaming frequency verification as well as an immediate imposition of prohibition of entry can only be fulfilled by automatic data processing, centralised data storage and merging all locations in a network.

The processing of biometric data (fingerprint) is based on the explicit consent of the Data Subject.

Regarding the special requirements to the various phases of processing, it should be noted that especially internal data disclosure is secured by an effective authorization system.

ACE has implemented state-of-the-art technical measures regarding the prevention of data loss and unauthorized access to data, programs and devices of the ADMIRAL-Card-System.

These measures comprise

- redundancy of servers and data centers for operation of the ADMIRAL-Card-System;
- implementation of physical access control to data centers, servers and media of ACE;
- implementation of logical access control on operating system, database and application level;
- efficient change and patch management processes that keep devices of the ADMIRAL-Card-System up-to-date;
- efficient capacity management and monitoring processes as well as redundancy measures that guarantee performance and availability of the ADMIRAL-Card-System;
- implementation of a backup and recovery concept that guarantees quick recovery of data in emergency cases.

Regarding network security, ACE has implemented the following measures against external attacks and intrusion:

- redundant, powerful firewalls;
- state-of-the-art VPN encryption for securing communication between headquarter, entertainment casinos and branch offices;
- network segmentation by using VLAN technology for devices of the ADMIRAL-CARD-System.

ACE has implemented a certified information security management system according to the international standard ISO/IEC 27001. An information security policy that describes the aims of and responsibilities for information security has been developed.

Furthermore, ACE has also defined and implemented security processes (e.g. security incident management as well as test and release management) that point out the importance of data security regarding the ADMIRAL-Card-System.

Erasure of data after the cessation of the requirements happens in accordance with data protection regulations as well as requirements necessary for the ADMIRAL-Card-System and legal retention periods.

Compliance with general data protection principles and duties regarding purpose-specification and -limitation, proportionality and quality of data has been achieved adequately.

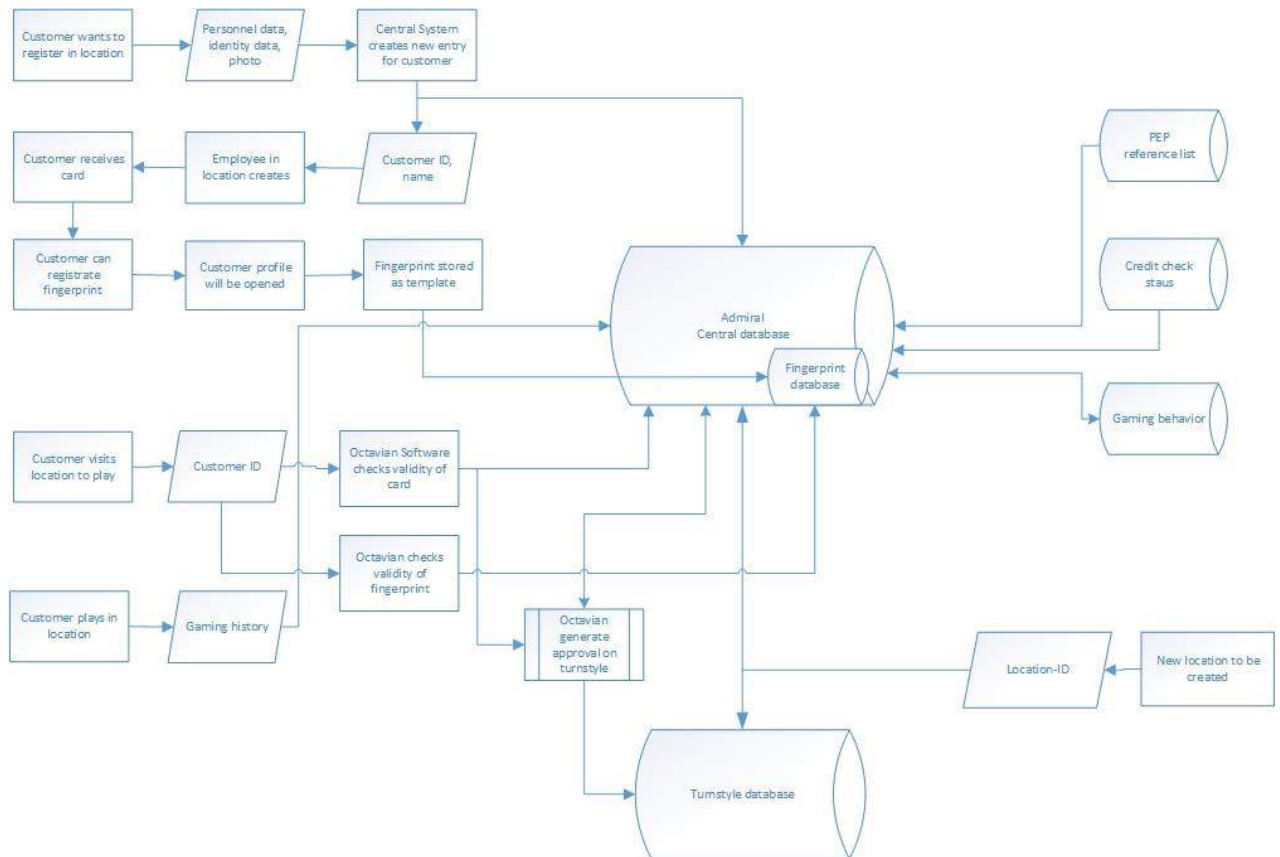
Relevant service agreements have been concluded with all of the involved processors, in complete accordance with data protection regulations. Due to ACE's conscious refusal of remote maintenance access as well as the fact that external maintenance staff is only allowed to work under supervision of the ACE, access to personal data by staff members of all processors can be almost completely excluded.

Transparency with regard to automated individual decisions concerning the behaviour of the Data Subject is fulfilled adequately by documentation and direct information given by staff present in the relevant entertainment-casino.

Before the legal validity of the GDPR the ADMIRAL-Card-System has been reported to the Austrian Data Protection Commission and after prior checking according to Article 20 of the directive 95/46/EC registered in the Data Protection Register.

In summary, it can be said that the ADMIRAL-Card-System is a very innovative computer-assisted model to prevent gaming addiction which can be rated as compliant with the EuroPriSe criteria regarding privacy and data security.

15. Data flow:



16. Privacy-enhancing functionalities:

In consequence of the Österreichisches Glücksspielgesetz (federal law) as well as relevant federal state laws and subsequent requirements referring to protective actions against compulsive gambling, ACE has developed the ADMIRAL-Card-System based on experience gained during operating the NOVOCARD™-Ampelsystem. This system contains comprehensive actions to prevent gaming addiction. Due to automatic data processing with a central storage of data, a network combining all entertainment casinos as well as an adequate consideration of data avoidance and minimization, data quality and protection of personal data against unauthorized access the principles of the GDPR are considered sufficiently.

17. Issues demanding special user attention:

The ADMIRAL-Card is a smart card with a contactless chip. As unauthorized reading cannot be precluded, data subjects are recommended to protect the ADMIRAL-Card by using specific customary protective covers.

18. Compensation of weaknesses:

Not applicable.

19. Decision table on relevant requirements:

<i>EuroPriSe Requirement</i>	<i>Decision</i>	<i>Remarks</i>
Data Avoidance and Minimisation	adequate	The data basis consisting of necessary master- and transaction-data of the customer has been extended by a fingerprint given by the customer on the basis of an explicit consent. Anonymization or Pseudonymization is because of the necessary personal functional attribution of the ADMIRAL-Card-System not possible.
Transparency	adequate	Leaflets in 11 different languages made available in the entertainment casinos not only describe the system in detail, but also inform about free and anonymous advisory services.
Technical-Organisational Measures	adequate	Regarding this criteria, physical and data access authorization systems have to be mentioned, as well as network security and backup and recovery procedures.
Data Subjects' Rights	adequate	Data Subject information about his rights according to chapter III GDPR is provided exemplarily.

Experts' Statement

We affirm that the above-named IT product / IT-based service has been evaluated according to the EuroPriSe Criteria, Rules and Principles and that the findings as described above are the result of this evaluation.

Vienna, June 23rd, 2020 Prof. KommR Hans-Jürgen Pollirer

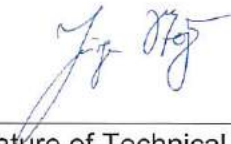


Place, Date

Name of Legal Expert

Signature of Legal Expert

Vienna, June 23rd, 2020 Mag. Jürgen Stöger



Place, Date

Name of Technical Expert

Signature of Technical Expert

Recertification Result

The above-named IT product / IT-based service passed the EuroPriSe evaluation.

It is certified that the above-named IT product / IT-based service facilitates the use of that product or service in a way compliant with European regulations on privacy and data protection.

Place, Date

Name of Certification Authority

Signature