

Short Public Report

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

NOVOCARD™-Ampelsystem, function as provided in March 2011

2. Provider of the IT-based service:

Company Name:



Austrian Gaming Industries GmbH (AGI)

Address:

Wiener Straße 158
2352 Gumpoldskirchen
Austria

Contact Person:

Emil Huber

3. Time frame of evaluation:

February 2010 – April 2011

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

Name of the Legal/Technical Expert:

Hans-Jürgen Pollirer

Address of the Legal/Technical Expert:

c/o Secur-Data Betriebsberatungs-GmbH

Fischerstiege 9

1010 Wien

Austria

eMail: hj.pollirer@secur-data.at

5. Certification Body:

Name: Unabhaengiges Landeszentrum fuer Datenschutz - ULD

Address: Holstenstr. 98

24103 Kiel

Germany

eMail: europrise@datenschutzzentrum.de

6. Specification of Target of Evaluation (ToE):

The target of evaluation does include:

- NOVOCARD™-Ampelsystem Services
 - Registration and creation of the customer (card)
 - Logging of times of attendance
 - Queries regarding attendance times and access bans
 - Issuing and cancelation of prevention of access or prohibition of entry
 - Processing of log-data
- Server Hosting

- Interfaces (connection to the internet)
- Commissioning of external processors
- Credit interviews

The target of evaluation does not include:

- Other processes carried out by the data processing centre
- Third party networks (e.g. internet)
- Helpline
- Video surveillance of the turnstiles
- Websites (novomatic.com, gluecksspielsucht.at)

7. General description of the IT-based service:

The Austrian Gaming Industries GmbH (AGI) – a 100% subsidiary of the Novomatic AG – operates entertainment casinos in several locations of Lower Austria. Based on the requirements of § 6a NÖ Spielautomatengesetz and the Austrian Glücksspielgesetz AGI has developed a program to prevent gaming addiction – the NOVOCARD™-Ampelsystem – in cooperation with the Department for Addiction Research & Treatment, University Hospital of Psychiatry and Psychotherapy of the Medical University of Vienna. This computer-assisted system controls Data Subjects' access to the entertainment casinos.

Before entering the entertainment casino each data subject has to prove his identity by submitting a photo ID. After verification of the data subject's legal age, his personal data is entered in a register form on which he declares his consent to the processing of his data under data protection law by his signature. His photo ID is subsequently scanned and, with his personal data, entered into the central computer, thus enabling control of all locations in Lower Austria. After registration is complete, the data subject receives the NOVOCARD™, a readable smart card with a contactless chip containing a serial number, which has to be signed by him to enable opening the turnstile directly in front of the games area. Cumulative sums of the number of days and durations of attendances are recorded. There is no exact history of days and durations of attendances. Each data subject is observed over a period of 180 days. Relevant deadlines are the 1st January and the 1st July. If the data subject has not entered the game area on more than

89 days within a period of 180 days, his gaming habit is considered harmless and he is in the GREEN phase. If the data subject has played on 90 or more days within a period of 180 days, subsequent calculations test if he also belongs to the critical 5 %-group. This 5 %-group identifies the top 5 % of data subjects in terms of their number of days and durations of attendance. Data subjects belonging to the 5 % group are handed a letter warning them about the dangers of livelihood-threatening gaming. During an interview with the person in charge of the location, the data subject is also asked about his creditworthiness. Simultaneously, these data subjects reach the RED phase and receive an access ban. This ban allows for a cool-down phase for the data subject. After expiration of the access ban, the data subject is put back into the GREEN phase. The more often an access ban is imposed, the longer it lasts. After the seventh occurrence, the ban is imposed without time limit. Furthermore, the data subject may request an access ban on his own behalf, either permanently or for a given period of time. In entertainment casinos random ID inspections are performed to prevent misuse of the NOVOCARD™.

The data collected and processed, such as ID including photo and signature as well as days and durations of attendances, represent the minimum of data necessary for the obligatory identification verification and the calculation of the 5 % group. Data avoidance and minimisation fully comply to general data protection principles, e.g. only the sums of days of attendance and hours of gaming are recorded and stored but not exact dates, times and entertainment casino locations. Regarding the transparency of the NOVOCARD™-Ampelsystem, the leaflet “Automatenspiel mit Zutrittskontrolle” has to be pointed out, containing statements about legal foundations, specific actions regarding registration, data collection and data storage, identity control, actions for legal protection of young persons and player protection with a description of the NOVOCARD™-Ampelsystem, preventative actions as well as tips regarding the exercise of right of access and objection of processing, as well as relevant safety guidelines for the safekeeping and protection against unauthorized reading of the NOVOCARD™.

The leaflet “NOVOCARD™-Ampelsystem”, also available at each entertainment casino, contains a graphical, easily understandable description of the system. Because of the high probability of gambling addiction in case of an access ban – whether imposed

by the system or by the data subject himself – both types of data are sensitive.

Requirements for the explicit declaration of consent when processing sensitive data, as specified by the European directive on data protection as well as the Austrian law on data protection, are met by the relevant declaration of consent given by the data subject on its initial registration. Furthermore, the data subject is informed by the location manager that these data are sensitive and therefore especially worthy of protection.

Referring to the legal retention period, it should be noted that according to the Austrian Glücksspielgesetz identity data has to be stored for a period of 5 years, other than data concerning the gaming frequency and playing duration. In case of an access ban imposed by the data subject itself, personal data is stored until the data subject requires the erasure of these data while considering the legal retention period. For data subjects not belonging to the 5 % group, data is automatically erased on the relevant deadlines with the exception of identity data. For those data subjects belonging to the 5 % group, data will be erased in accordance with the relevant provisions of the Austrian law.

The hardware and software necessary for authenticating the data subject's access to the gaming area has been delivered and implemented by a third party provider who is also responsible for maintenance. The software responsible for the analysis of days and durations of attendance was also developed by a third party provider who is responsible for maintenance. AGI has concluded contracts regarding data protection principles with both third party providers.

Regarding the automatic imposition of an access ban, the transparency of these automated decisions is secured by the leaflet-information as well as by a briefing given by the location manager.

8. Transnational issues:

The NOVOCARD™-Ampelsystem is currently used in Lower Austria only. Data transmission to third parties does not occur.

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

MS Windows Server

Apache/PHP/SSL

SQL Server DBMS

Firebird DBMS

10. Edition of EuroPriSe Criteria used for the evaluation:

EuroPriSe criteria May 2010

11. Evaluation results:

Considering the fundamental aspects of processing it can be stated that AGI with its NOVOCARD™-Ampelsystem has developed a system for preventing gaming addiction in full compliance with data protection regulations and with involvement of specific scientific expertise.

Evaluation of the criteria concerning processed personal data has shown that all processed data are precisely specified and that data processing happens only with the explicit consent of the Data Subject.

AGI complies fully with its information duty; effective processes have been implemented to honour the relevant rights of access, correction and erasure.

In the fundamental technical construction of the NOVOCARD™-Ampelsystem data avoidance and minimization was given particular attention. Only data needed for Data Subject identification, monitoring and analysis of attendance times as well as for a possible prohibition of admittance is collected and processed.

Regarding transparency and product description, it was ascertained that the Data Subject is exactly informed on his first visit to an entertainment casino about the fact that the NOVOCARD™-Ampelsystem is an electronic system, combining the obligation of registration with control of access and observation.

Legal basis for the processing of personal data is the NÖ Spielautomatengesetz as well as the amendment of the Österreichisches Glücksspielgesetz entered into force on 1. January 2011.

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 sensitive personal data 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.

AGI has implemented state-of-the-art technical measures regarding the prevention of data loss and unauthorized access to data, programs and devices of the NOVOCARD™-Ampelsystem.

These measures comprise

- the redundancy of servers and data centers for operation of the NOVOCARD™-Ampelsystem;
- implementation of physical access control to data centers, servers and media of AGI GmbH;
- implementation of logical access control on operating system and application level;
- efficient change and patch management processes that keep devices of the NOVOCARD™-Ampelsystem up-to-date;
- implementation of a backup and recovery concept that guarantees quick recovery of data in emergency cases.

Regarding network security AGI GmbH has implemented the following measures against external attacks and intrusion:

- redundant, powerful firewalls

- state-of-the-art VPN encryption for securing the communication between the headquarter and the branches;
- network segmentation by using VLAN technology for the devices of NOVOCARD™-Ampelsystem.

Most of the general data and security management measures can be evaluated as excellent. An information security policy that describes the aims of and responsibilities for information security has been developed. Furthermore AGI 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 NOVOCARD™-Ampelsystem.

Erasure of data after the session of the requirements happens in accordance with data protection regulations as well as requirements necessary for the NOVOCARD™-Ampelsystem 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 perfectly.

Relevant service agreements have been concluded with both of the involved Processors, in complete accordance with data protection regulations. Due to AGI'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 AGI, any access to personal data by staff members of the two processors can be almost 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.

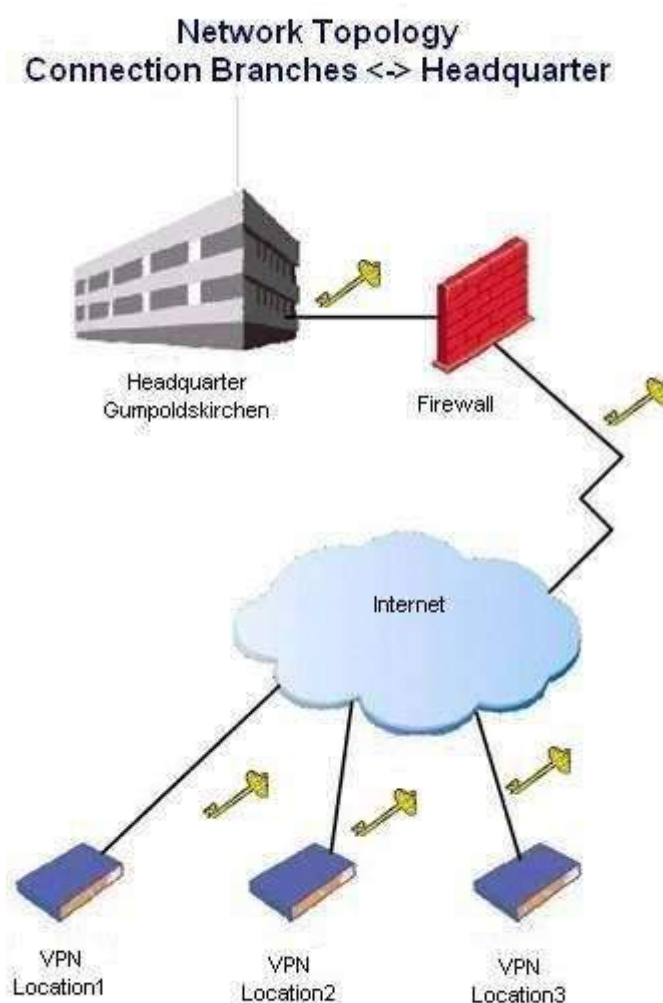
The NOVOCARD™-Ampelsystem has been reported to the Austrian Data Protection Commission and after prior checking registered in the Data Protection Register.

In summary, it can be said that AGI has developed with the NOVOCARD™-Ampelsystem 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.

12. Data flow:

Data flow in the NOVOCARD™-Ampelsystem can be gathered from the following diagram:



13. Privacy-enhancing functionalities:

As the first company in the sensitive gaming sector, AGI has developed with the NOVOCARD™-Ampelsystem a pioneering solution to deal with gaming addiction. Due to automatic data processing as well as central storage of data and a network

combining all entertainment casinos, NOVOCARD™-Ampelsystem is an ideal solution regarding data avoidance and minimisation, data quality and protection of personal data against unauthorized access.

14. Issues demanding special user attention:

The NOVOCARD™ is a smart card with a contactless chip. As unauthorized reading cannot be precluded, the Data Subject is recommended to protect the NOVOCARD™ by using specific protective covers available at the entertainment casinos.

15. Compensation of weaknesses:

Not applicable.

16. Decision table on relevant requirements:

<i>EuroPriSe Requirement</i>	<i>Decision</i>	<i>Remarks</i>
Data Avoidance and Minimisation	<i>excellent</i>	The NOVOCARD™-Ampelsystem uses only a minimum of data.
Transparency	<i>adequate</i>	Leaflets in 6 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	<i>excellent</i>	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	<i>excellent</i>	Data Subject information about the right of objection to processing and the right of access, correction and erasure when gathering personal data, is provided exemplarily.

Experts' Statement

We affirm that the above-named IT product 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, 18.4.2011 Hans-Jürgen Pollirer



Place, Date	Name of Legal/Technical Expert	Signature of Legal/Technical Expert
-------------	--------------------------------	-------------------------------------

Certification Result

The above-named IT product passed the EuroPriSe evaluation.

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

Place, Date	Name of Certification Body	Signature
-------------	----------------------------	-----------