Short Public Report

1. Name und Version des IT-basierten Services:

ADMIRAL-Card-System, Version in der im August 2014 zur Verfügung stehenden Funktionalität

2. Betreiber des IT-basierten Services:

Firmenname:

ADMIRAL Casinos & Entertainment AG (ACE)

Adresse:

ADMIRAL Casinos & Entertainment AG (ACE)
Wiener Straße 158
2352 Gumpoldskirchen
Österreich

Kontaktperson:

Ing. Emil Huber

3. Zeitrahmen der Evaluierung:

Mai 2013 – August 2014

4. EuroPriSe Experten, die das IT-basierte Service evaluiert haben:

Name des Experten (rechtlich):

Hans-Jürgen Pollirer

Adresse des Experten (rechtlich):

c/o Secur-Data Betriebsberatungs-GmbH
Fischerstiege 9
1010 Wien
Österreich

eMail: hj.pollirer@secur-data.at

Name des Experten (technisch):

Jürgen Stöger

Adresse des Experten (rechtlich):

c/o Secur-Data Betriebsberatungs-GmbH
Fischerstiege 9
1010 Wien
Österreich

eMail: j.stoeger@secur-data.at

5. Zertifizierungsstelle:

Name: EuroPriSe Certification Authority
Adresse: Joseph-Schumpeter-Allee 25
53227 Bonn
Germany
eMail: contact@european-privacy-seal.eu

6. Spezifikation des Zertifizierungsgegenstandes (ToE):

Die Objekte des Zertifizierungsgegenstandes umfassen

- ADMIRAL-Card-System Services
  - Registrierung und Anlage der Kunden(karten)
  - Erfassung der Anwesenheitszeiten
  - Erfassung des Einsatzverhaltens
  - Durchführung von Abfragen
  - Erteilung und Aufhebung von Zutrittssperren bzw. Zutrittsverboten
  - Verarbeitung von Logdaten
  - Bonitätsprüfung bzw. -befragung
  - PEP-Check
- Schnittstellen des ADMIRAL-Card-Systems
- Schnittstelle zum Bundesrechenzentrum (BRZ)
- Schnittstellen/Verbindungen zum Internet

Die Objekte der Zertifizierung umfassen nicht:

- Sonst. Rechenzentrumsbetrieb
- Netzwerke von Dritten (z.B. Internet)
- ACE-Hotline
- Serverhousing bei Dienstleister A1
- Videoüberwachung der Drehkreuze
- Beobachtungsprotokoll

7. Kurzbeschreibung des IT-basierten Services:

Die ADMIRAL Casinos & Entertainment AG (ACE) – eine 100%ige Tochtergesellschaft der Novomatic AG – betreibt an mehreren Standorten in Österreich Entertainment Casinos. Bedingt durch eine grundlegende Novellierung des Österreichischen Glücksspielgesetzes (Bundesgesetz) und der entsprechenden Landesgesetze ergeben sich höhere Anforderungen in Bezug auf die Spielerschutzmaßnahmen. Die ACE hat daher auf

Basis des bereits 2011 mit dem European Privacy Seal ausgezeichneten NOVO-CARD™-Ampelsystems das ADMIRAL-Card-System entwickelt. Wie bereits das Vorsystem berücksichtigt auch das neue ADMIRAL-Card-System die Forschungsergebnisse der Abteilung Suchtforschung & Suchttherapie der Medizinischen Universität / Allgemeines Krankenhaus Wien. Beim ADMIRAL-Card-System handelt es sich um ein automationsunterstütztes System für Kunden der Automatensalons mit Maßnahmen zur Zutrittskontrolle und zum Spielerschutz.

Jeder Kunde muss sich vor Betreten eines Automatensalons durch Vorlage eines amtlichen Lichtbildausweises legitimieren. Nach Überprüfung der Volljährigkeit werden die Personaldaten durch automatisches Auslesen der Ausweisdaten sowie manuelle Eingaben erfasst und der Ausweis eingescannt. Über eine an das System angeschlossene Kamera wird zusätzlich ein aktuelles Lichtbild des Kunden angefertigt, im System gespeichert und auf der ADMIRAL-Card aufgedruckt. Im Zuge der Registrierung wird für jeden Kunden eine einzigartige Kundennummer vergeben, die eine eindeutige Identifizierung im System ermöglicht. Weiters wählt der Kunde im Registrierungsprozess einen vierstelligen PIN-Code. Im Zuge des Registrierungsprozesses bestätigt der Kunde seine ausdrückliche datenschutzrechtliche Zustimmung zur Verwendung seiner personenbezogenen Daten sowie der Erfassung der Daten über sein Besuchs- und Spielverhalten (einschließlich Nettospielzeit) und allfällige Abfragen von Bonitätsdaten. Nach erfolgter Registrierung erhält der Kunde seine ADMIRAL-Card, bei der es sich um eine Kombicard mit einem Smartchip und einem RFID-Chip handelt. Auf der Karte selbst werden keinerlei personenbezogene Daten gespeichert, sondern nur die mehrstellige Kundennummer. Die ADMIRAL-Card ermöglicht dem Kunden die Öffnung des vor dem Spielbereich angebrachten Drehkreuzes und die Inbetriebnahme eines Spielautomaten in Kombination mit dem PIN-Code des Kunden. Durch die zentrale Speicherung der Daten und die Vernetzung aller Filialen wird die im Glücksspielgesetz vorgesehene Überprüfung der Spielfrequenz und des Einsatzverhaltens möglich.

Das ADMIRAL-Card-System ist ein abgestuftes Warnsystem zur Erkennung von gefährdeten Spielern. Grundlage für den Status eines Kunden, wobei die Stufe Grün = unbedenklich, Gelb = potentiell gefährdet und Rot = Sperre bedeutet, ist der auf Basis des laufenden Monitoring monatlich durchgeführte Screening-Prozess. Im Screening-

Prozess werden 2 Altersgruppen unterschieden, und zwar die Altersgruppe 1 mit Personen von 18 - < 26 Jahren und Altersgruppe 2 mit Personen ≥ 26 Jahren. Diese Differenzierung wurde aufgrund wissenschaftlicher Studien festgelegt. Berücksichtigt wird ferner die Höhe der Nettoverluste, wobei für die Altersgruppe 1 ein Schwellenwert von EUR 500;00 und für die Altersgruppe 2 ein solcher von EUR 1.000;00 festgelegt wurde. Die Berechnung erfolgt auf Basis der Nettoverluste der letzten drei Monate. Als weiterer Parameter wird die Anzahl der Anwesenheitstage berücksichtigt, wobei bei Altersgruppe 1 ein Schwellenwert von > 90 Besuchen im Halbjahr und für die Altersgruppe 2 ein solcher von > 120 Besuchen im Halbjahr festgelegt ist. Überschreiten die Nettoverluste die entsprechenden Grenzwerte, so wird eine Bonitätsauskunft eingeholt. Der Kunde wird jedenfalls über die Einholung einer Bonitätsauskunft und deren Ergebnis von Präventionsbeauftragten informiert.

Parallel wird die potentielle Spielsuchtgefährdung des Kunden anhand der Anzahl der Besuchstage geprüft. Der Screeningprozess liefert Informationen über die finanzielle Existenzgefährdung und die Spielsuchtgefährdung des entsprechenden Kunden. Darüberhinaus hat der Kunde auch die Möglichkeit, einen freiwilligen Zutrittsverzicht auf Dauer oder eine bestimmte Zeitdauer vorzunehmen.

Bei den erfassten und verarbeiteten Daten, wie Ausweisdaten, Lichtbild und Spielverhalten handelt es sich um das Minimum an Daten, das für die verpflichtende Identitätsprüfung sowie für den Spielerschutz notwendig sind. Den datenschutzrechtlichen Grundsatz der Datenvermeidung und Datensparsamkeit wird voll und ganz Rechnung getragen. In Hinblick auf die Transparenz des ADMIRAL-Card-Systems ist auf die in den einzelnen Entertainment-Casinos aufliegenden Flyer „Entertainment mit Verantwortung“ und „Prävention ist der beste Spielerschutz“ zu verweisen, die sowohl Informationen über das ADMIRAL-Card-System selbst wie auch Tipps zum verantwortungsvollen Umgang mit dem Glücksspiel, einen Selbsttest und Hinweise auf die Möglichkeiten der Selbstkontrolle sowie Kontaktadressen über die Behandlungseinrichtungen enthalten. Da bei einer Verhängung eines Zutrittsverbotes oder beim freiwilligen Zutrittsverzicht eine hohe Wahrscheinlichkeit gegeben ist, dass der Kunde spielsüchtig ist, handelt es sich bei diesen beiden Datenarten um sensible Daten. Der sowohl nach der EU-DSRL als auch durch das österreichische Datenschutzgesetz vorgesehenen ausdrücklichen Zu-

stimmung zur Verarbeitung sensibler Daten wird durch eine entsprechende Zustimmungserklärung zur Verarbeitung nachgekommen. Darüber hinaus wird der Kunde durch den jeweiligen Präventionsbeauftragten auch explizit darüber informiert, dass es sich bei den sensiblen Daten um besonders geschützte Informationen handelt. Entsprechende Hinweise finden sich auch im Flyer „Entertainment mit Verantwortung“ sowie auf der Rückseite der Zustimmungserklärung.

In Bezug auf die gesetzliche Aufbewahrungsfrist ist festzuhalten, dass nach den Bestimmungen des österreichischen Glücksspielgesetzes die Identitätsdaten 5 Jahre aufzubewahren sind, nicht jedoch die Daten zum Spielverhalten. Eine Löschung der personenbezogenen Daten erfolgt entweder auf Begehren des Kunden unter Einhaltung der gesetzlichen Aufbewahrungsfrist oder automatisch nach Ablauf dieser unter der Voraussetzung, dass der Kunde in den vergangenen 5 Jahren kein Entertainment-Casino betreten hat.

Die für die Authentisierung der Zutritte der Betroffenen in den Spielbereich notwendige Hardware und Software wurde von einem externen Dienstleister geliefert bzw. entwickelt und wird von diesen auch gewartet. Die für die Auswertung der Anwesenheitstage und Anwesenheitsdauer notwendige Software wurde ebenfalls von einem externen Dienstleister entwickelt und wird von diesem auch gewartet. Das Serverhousing erfolgt beim Dienstleister A1. Mit allen Dienstleistern wurden entsprechende ADV-Verträge abgeschlossen. In Bezug auf die automationsunterstützte Verhängung eines Zutrittsverbots ist die Transparenz dieser Entscheidung sowohl durch die Informationsbroschüren als auch durch ein aufklärendes Gespräch mit dem Filialverantwortlichen sichergestellt.

8. Grenzüberschreitender Datenverkehr:

Das ADMIRAL-Card-System wird nur in Österreich eingesetzt. Ein grenzüberschreitender Datenverkehr findet somit nicht statt.

9. Werkzeuge zur Herstellung des IT-Produktes/Betreiber des IT-basierten Services:

- Windows/Linux
- Apache/PHP

- Oracle DBMS
- Firebird DBMS

10. Version der für die Evaluierung verwendeten EuroPriSe-Kriterien:

EuroPriSe Kriterien November 2011

11. Ergebnisse der Evaluierung:

Bei Betrachtung der „grundlegenden Verarbeitungsaspekte“ kann festgestellt werden, dass die ACE mit dem ADMIRAL-Card-System ein System unter voller Beachtung der datenschutzrechtlichen Rahmenbedingungen entwickelt hat, das die modernen Erkenntnisse der Suchtforschung noch besser berücksichtigt als das Vorsystem.

In Bezug auf die „verarbeiteten personenbezogenen Daten“ ist festzuhalten, dass diese genau spezifiziert sind und die Verarbeitung dieser Daten nur mit ausdrücklicher Zustimmung des Betroffenen erfolgt. Die ACE kommt ihrer Informationspflicht vollinhaltlich nach; für die Erfüllung der Grundrechte auf Auskunft, Richtigstellung und Löschung wurden entsprechende wirkungsvolle Prozesse aufgesetzt.

Bei der Evaluierung des „grundlegenden technischen Aufbaus“ zeigt sich, dass dem Kriterium „Datenvermeidung und -sparsamkeit“ besondere Beachtung zugemessen wird. So werden nur jene Daten ermittelt und verarbeitet, die sowohl für die Identifizierung eines Betroffenen als auch für die Berechnung des Spielverhaltens und einer möglichen Zutrittssperre benötigt werden.

In Bezug auf die „Transparenz und Produktbeschreibung“ konnte festgestellt werden, dass der Betroffene bei seinem Erstbesuch eines Entertainment-Casinos genau darüber informiert wird, dass es sich beim ADMIRAL-Card-System um ein elektronisches System handelt, das eine Kommunikation zwischen Registrierungspflicht sowie Zutritts- und Beobachtungskontrolle umfasst. Darüber hinaus bieten die beiden in den Entertainment-Casinos aufliegenden Flyer detaillierte Informationen.

Die „gesetzliche Grundlage“ des ADMIRAL-Card-Systems ergibt sich aufgrund der Bestimmungen der mit 1. Jänner 2011 in Kraft getretenen Novelle des österreichischen Glücksspielgesetzes sowie der entsprechenden Landesgesetze.

Zur Frage der „Eingriffstiefe in das Grundrecht auf Datenschutz“ ist anzumerken, dass die gesetzlichen Anforderungen in Bezug auf die Identitätsprüfung, die Überprüfung der Spielfrequenz sowie der Ausspruch einer sofortigen Zutrittssperre im Anlassfall nur durch eine automationsunterstützte Verarbeitung sowie durch zentrale Speicherung der Daten und die Vernetzung der einzelnen Standorte der Entertainment-Casinos erfüllt werden können.

Die Verarbeitung der als „sensibel einzustufenden Datenarten“ basiert auf der ausdrücklichen Zustimmung der Betroffenen.

Bei der Beurteilung der „besonderen Erfordernisse bei den verschiedenen Verarbeitungsschritten“ ist anzumerken, dass besonders der interne Datenzugriff durch ein entsprechendes wirkungsvolles Zugriffsberechtigungssystem abgesichert ist.

Die ACE hat dem Stand der Sicherheitstechnik entsprechende technische Maßnahmen umgesetzt, mit denen der Verlust von Daten und unbefugte, nicht autorisierte Zugriffe auf Daten, Programme, Datenträger und Informationssysteme des ADMIRAL-Card-Systems wirkungsvoll verhindert werden.

Zu diesen Maßnahmen zählen

- die Redundanz bei Server-Systemen und Rechenzentrumsstandorten, mit der ein störungsfreier Betrieb des ADMIRAL-Card-Systems gewährleistet wird;
- die Umsetzung restriktiver physischer Zutritts- und Zugriffskontrollmaßnahmen zu den Räumlichkeiten, Servern und Datenträgern der ACE durch Einsatz eines elektronischen Zutrittskontrollsystems;
- die Umsetzung logischer Zugriffskontrollmaßnahmen durch Einsatz von Login-Kontrollen und Berechtigungskonzepten auf Betriebssystem-, Datenbank- und Applikationsebene;
- auf aktuellem Softwarestand gehaltene Informationssysteme (regelmäßige Updates und Sicherheitspatches bei Betriebssystemen, Datenbanken und Applikationen);
- die Ausarbeitung und Implementierung eines Notfallvorsorgekonzepts, mit dem eine rasche Wiederherstellung von Informationssystemen des ADMIRAL-Card-Systems im Notfall bewerkstelligt werden kann.

Das Netzwerk der ACE, das für das ADMIRAL-Card-System betrieben wird, ist durch folgende Schutzmaßnahmen gegen externe Angriffe geschützt:

- performantes, redundant ausgeführtes Firewallsystem
- VPN-Verschlüsselung der Kommunikation zu den Automatensalons nach dem aktuellen Stand der Sicherheitstechnik.
- Netzwerksegmentierung durch Einsatz eines eigenen VLAN für die Informationssysteme des ADMIRAL-Card-Systems

Auch im Bereich des Sicherheitsmanagements wurden bei der ACE umfangreiche Sicherheitsprozesse definiert, die als exzellent zu bewerten sind. Das Unternehmen betreibt ein Informationssicherheits-Managementsystem und ist nach dem internationalen Standard ISO/IEC 27001 zertifiziert. Im Rahmen einer schriftlich fixierten Informationssicherheitspolitik sind die Grundsätze und Ziele der Informationssicherheit sowie die Verantwortlichkeiten dokumentiert. Ebenso sind dokumentierte Verfahren zum Security Incident Management und zum Test- und Freigabemanagement entwickelt und in Kraft gesetzt worden.

Die „Löschung der Daten nach Beendigung der Voraussetzung“ erfolgt entsprechend den datenschutzrechtlichen Bestimmungen unter Beachtung der systemseitigen Erfordernisse und der gesetzlichen Aufbewahrungsfristen.

Die „allgemeinen Datenschutzprinzipien und -pflichten“, wie die „strikte Zweckbindung“, die „Begrenzung des Datenumfanges“ und die „Datenqualität“ werden ausgezeichnet eingehalten.

Die mit den „Auftragsverarbeitern“ abgeschlossenen ADV-Verträge entsprechen voll und ganz den datenschutzrechtlichen Bestimmungen. Aufgrund der von der ACE bewusst nicht installierten Fernwartungszugänge sowie aufgrund der Tatsache, dass externes Wartungspersonal ausschließlich unter Aufsicht der ACE tätig werden kann, ist ein unbefugter Zugriff auf personenbezogene Daten durch Mitarbeiter der Auftragsverarbeiter nahezu ausgeschlossen.

Die Transparenz hinsichtlich der „automatisierten Einzelentscheidung“ bei der Feststellung des Besucherverhaltens wird sowohl durch schriftliche Unterlagen als auch durch

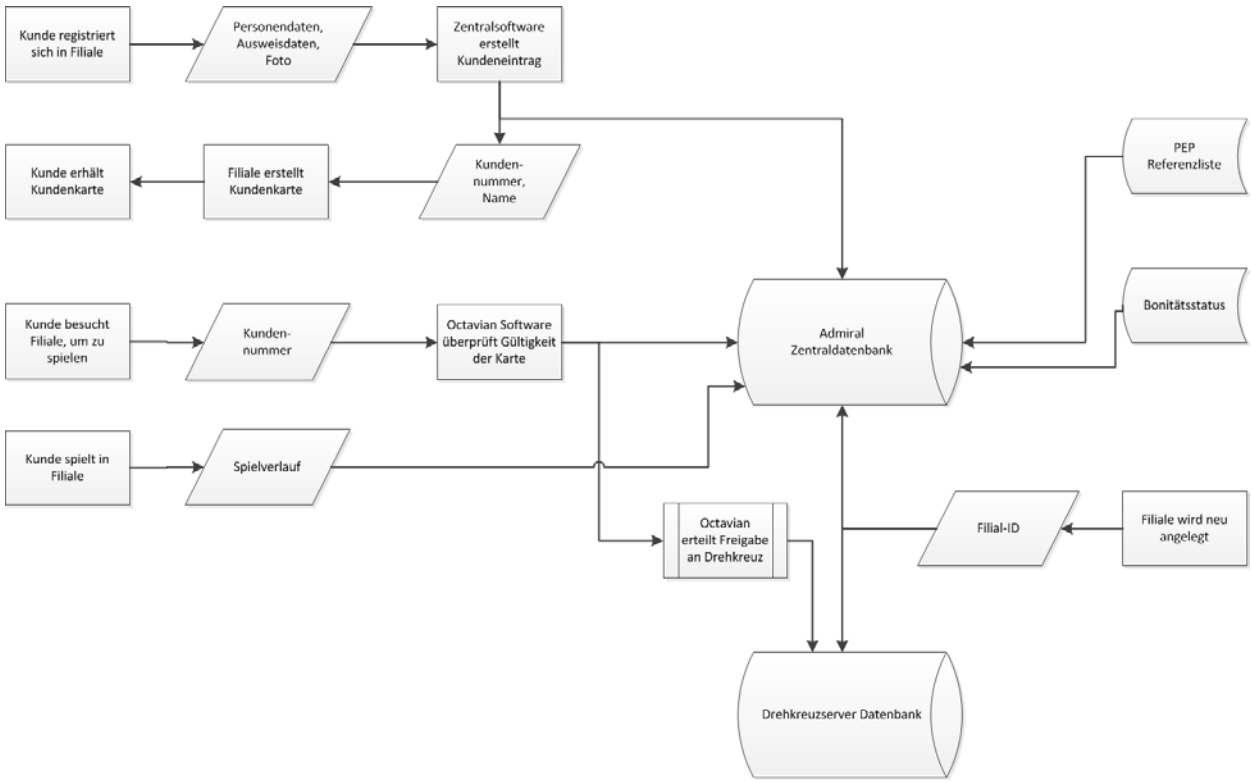
direkte Information durch das im jeweiligen Entertainment-Casino anwesende Personal in ausreichender Weise erfüllt.

Das ADMIRAL-Card-System wurde ordnungsgemäß bei der Österreichischen Datenschutzkommission (DSK) gemeldet, von dieser der „Vorabkontrolle“ unterzogen und erfolgreich im Datenverarbeitungsregister (DVR) registriert.

Zusammenfassend kann festgestellt werden, dass die ACE mit dem ADMIRAL-Card-System ein sehr innovatives automationsunterstütztes Modell zur Spielersuchtprävention entwickelt hat, das als konform mit den Anforderungen an Datenschutz und Datensicherheit entsprechend den EuroPriSe-Kriterien zu bewerten ist.

12. Data flow:

Der Datenfluss im ADMIRAL-Card-System kann nachstehender Schemaskizze entnommen werden:



13. Verbesserung der Datenschutzfunktionalitäten:

Bedingt durch die grundlegende Novellierung des österreichischen Glücksspielgesetzes (Bundesgesetz) sowie der entsprechenden Landesgesetze und der sich daraus ergebenden neuen Anforderungen in Bezug auf die Spielerschutzmaßnahmen, hat die ACE auf Basis der aus dem Betrieb mit dem European Privacy Seal ausgezeichneten NOVOCARD^{TM}-Ampelsystem gewonnenen Erfahrungen, das ADMIRAL-Card-System entwickelt. Dieses System enthält umfassende Präventions- und Spielerschutzmaßnahmen. Durch die automationsunterstützte Verarbeitung sowie die zentrale Speicherung der Daten und die Vernetzung der verschiedenen Entertainment-Casinos ist das ADMIRAL-Card-System eine vorbildliche Lösung in Bezug auf Datensparsamkeit, Datenqualität sowie Schutz der Daten vor unbefugten Zugriffen.

14. Bereiche, die besondere Aufmerksamkeit der Benutzer bedingen:

Bei der ADMIRAL-Card handelt es sich um eine Smartcard mit einem kontaktlosen Chip. Da ein missbräuchliches Auslesen nicht ausgeschlossen werden kann, wird dem Kunden empfohlen, die ADMIRAL-Card durch spezielle – handelsübliche - Schutzhüllen entsprechend zu schützen.

15. Kompensation von Schwachstellen:

Entfällt.

16. Ergebnistabelle der relevanten Anforderungen:

EuroPriSe Anforderung	*Bewertung*	*Anmerkungen*
Datenvermeidung und -sparsamkeit	exzellent	Das ADMIRAL-Card-System nutzt nur das Minimum der erforderlichen Daten.
Transparenz	adäquat	Die in den Entertainment-Casinos in sechs Sprachen aufliegenden Informationsblätter beschreiben nicht nur detailliert das ADMIRAL-Card-System, sondern enthalten auch Hinweise auf kostenfreie und Anonyme Beratungsmöglichkeiten.

EuroPriSe Anforderung	*Bewertung*	*Anmerkungen*
Technisch-organisatorische Maßnahmen	adäquat	In diesem Bereich sind besonders das Zutritts- und Zugriffsberechtigungssystem sowie Netzwerksicherheit und Backup- und Recovery-Verfahren zu nennen.
Rechte des Betroffenen	exzellent	Die Information des Betroffenen bei der Ermittlung seiner personenbezogenen Daten über das Widerrufs- und Widerspruchsrecht sowie die Erfüllung der Grundrechte auf Auskunft, Richtigstellung und Löschung erfolgen in vorbildlicher Weise.

Gutachter-Statement

Ich versichere, dass das oben genannte IT-basierte Produkt nach den EuroPriSe-Kriterien, Regeln und Prinzipien evaluiert wurde und dass die oben beschriebenen Ergebnisse das Resultat dieser Evaluierung sind.

Wien, 27. 10. 2014	Prof. KommR Hans-Jürgen Pollirer	
Ort, Datum	Name des rechtlichen Gutachters	Unterschrift

Wien, 27. 10. 2014	Mag. Jürgen Stöger	
Ort, Datum	Name des technischen Gutachters	Unterschrift

Ergebnis der Zertifizierung

Das oben genannte IT-basierte Produkt hat die EuroPriSe-Evaluierung bestanden.

Hiermit wird bescheinigt, dass das oben genannte IT-basierte Produkt eine Nutzung nach den Europäischen Vorgaben für Datenschutz ermöglicht

Ort, Datum	Name der Zertifizierungsstelle	Unterschrift