DATENSICHERHEITSVORSCHRIFT

für das Verwenden der Meldedaten

durch die

MARKTGEMEINDE GAMING,

3292 Gaming, Im Markt 1

zum Aufbau und Betrieb des Zentralen Melderegisters

(§ 4 Abs. 4 der Meldedatensicherheitsmaßnahmen-Verordnung, BGBl. II Nr. 174/2001)

1. Geltungsbereich

Die folgende Datensicherheitsvorschrift regelt die Datensicherheitsmaßnahmen beim Verwenden von Daten zum Aufbau und Betrieb bis zur Aufnahme des Echtbetriebes des Zentralen Melderegisters (im folgenden: „ZMR“) durch die Meldebehörde der Marktgemeinde Gaming bzw. den Bürgermeister der Marktgemeinde Gaming, der gemäß § 16b Abs. 6 Meldegesetz 1991, in der Fassung des Art. I des Bundesgesetzes BGBl. I Nr. 28/2001, tätig wird.

Die folgende Datensicherheitsvorschrift wird für den Bereich der Systeme, über die der Zugang zum ZMR erfolgen soll, erlassen.

Sie gilt für die Bediensteten der Marktgemeinde Gaming bzw. ihres Dienstleisters sowie für die Bediensteten des Betreibers des ZMR (= des Bundesministers für Inneres) und diejenigen Personen, die die Räume, in denen Arbeitsplätze oder sonstige Komponenten des Systems installiert sind, betreten.

Der Umfang der Datenverwendung im System umfaßt sämtliche in § 4 Zif. 8 DSG 2000 angeführten Handhabungen.

2. Zulässigkeit der Datenverwendung

Daten dürfen nur auf Grund von generellen oder speziellen Aufträgen von Organen (Bürgermeister, Vizebürgermeister) der Marktgemeinde Gaming oder des Bundesministers für Inneres im Rahmen der durch die Zuständigkeitsregelungen erfolgten Aufgabenstellungen in Vollziehung des Meldegesetzes verwendet werden.

3. Der Verantwortliche gemäß § 4 MeldeDS-VO

3.1. Bestellung eines Verantwortlichen für die Datensicherheitsmaßnahmen

Jede Meldebehörde hat zumindest einen Verantwortlichen für die Datensicherheitsmaßnahmen im Rahmen der Datenverarbeitung für das ZMR zu bestellen und dem Betreiber des ZMR zu benennen; dieser Verantwortliche kann vom Betreiber des

ZMR ermächtigt werden, Zugriffsberechtigungen für den Betrieb des ZMR zu erteilen, sofern der Betreiber des ZMR die Berechtigungen nicht selbst vergibt.

3.2. Aufgaben eines Verantwortlichen für die Datensicherheitsmaßnahmen

Der Verantwortliche hat nach Maßgabe des jeweiligen Standes der Technik und der organisatorischen Möglichkeiten den Zugriffsschutz zu personenbezogenen Daten und die erforderlichen Datensicherheitsmaßnahmen zu organisieren und umzusetzen. Er hat insbesondere die Zuständigkeiten und Regeln für die Programmverwaltung in seinem Bereich festzulegen, sowie die Voraussetzungen für den physischen Zugriff auf die Daten des ZMR in seinem Zuständigkeitsbereich zu schaffen. Es obliegt diesem Verantwortlichen, alle Personen, die am Betrieb des Systems teilnehmen, über die Geheimhaltungsbestimmungen gem. § 15 DSG 2000 bei Dienstantritt zu belehren.

4. Sicherheitsmaßnahmen

4.1. Technische Vorkehrungen (Software-Zertifikate)

Für den Verbindungsaufbau zum ZMR sind die vom Betreiber zur Verfügung gestellten Software-Zertifikate zu verwenden. Software-Zertifikate sind Schlüssel, die den Zugang zum ZMR über dezentrale Systeme eröffnen und jedes zugriffsberechtigte System eindeutig identifizieren. Anstelle von Arbeitsplatz-Systemen kann mit einem Software-Zertifikat auch ein Gateway-System authentifiziert werden, das sich in der Verfügung des Anwenders oder eines von ihm beauftragten Dienstleisters befindet.

Die Software-Zertifikate für die Gateway- und/oder Arbeitsplatz-Systeme für den ZMR-Betrieb sind von eigens dazu mit Administrationsrechten ausgestatteten Benutzern über eine entsprechende Datenanwendung des Betreibers zu bestellen und werden in der Folge vom Betreiber zur Verfügung gestellt.

Die Software-Zertifikate sind von den beim Bundesministerium für Inneres, Sektion IV – Gruppe EDV gemeldeten administrationsberechtigten Benutzern (unter Verwendung der ihnen vom Betreiber zur Verfügung gestellten TAN-Codes auf den entsprechenden Rechnern zu installieren.

Wird ein Gerät, das den Zugang zum ZMR ermöglicht, aus dem Behördenbereich oder einer Dienststelle entfernt, ist sicher zu stellen, dass eine unberechtigte Verwendung der Software-Zertifikate ausgeschlossen ist. Im Hinblick auf die besondere Schutzwürdigkeit der Software-Zertifikate ist sicherzustellen, dass bei Abbau von Gateway- oder Arbeitsplatz-Systemen (Workstations), die Software-Zertifikate deinstalliert und bis zum allfälligen Installieren auf einem neuen Rechner sicher verwahrt werden.

Sollte ein Software-Zertifikat nicht mehr benötigt werden, so ist dieser Umstand umgehend dem Betreiber (Abteilung IV/8 des Bundesministeriums für Inneres) (fern-)schriftlich zur Kenntnis zu bringen.

Der Zugriff auf Software-Zertifikate durch Unbefugte ist jedenfalls durch geeignete bauliche, technische und organisatorische Maßnahmen zu verhindern.

4.2 Zutritt zu Räumen

Durch organisatorische und technische Vorkehrungen ist sicher zu stellen, dass der Zutritt zu Räumen, in denen sich eine Zugriffsmöglichkeit auf das ZMR befindet, grundsätzlich nur Bediensteten der Behörde möglich ist.

Darüberhinaus ist der Aufenthalt im (in den) Raum (Räumen) des Systems nur den Bediensteten des Dienstleisters in Erfüllung dienstlicher Aufträge, ferner dem Wartungs- und Reinigungspersonal für die Dauer der erforderlichen Tätigkeit, sowie Angehörigen des Betreibers in Erfüllung ihrer dienstlichen Aufträge, gestattet.

Für den Fall, dass der Zutritt von Personen, die weder dem Personal, welches berechtigt ist, am Betrieb des Systems teilzuhaben, noch sonst den oa. zutrittsberechtigten Personen zuzurechnen sind, erforderlich ist, ist ausnahmslos dafür Sorge zu tragen, dass eine Einsichtnahme in das ZMR durch entsprechende Maßnahmen (z.B. entsprechende Aufstellung der Datensichtgeräte, örtliche Abgrenzung durch entsprechende Möblierung, Reduktion der Helligkeit des Bildschirmes auf jenes Maß, das ein Ablesen von Informationen unmöglich macht, etc.) nicht möglich ist.

Überdies ist über den Zutritt Angehöriger von Firmen, die in den Räumlichkeiten des Systems Arbeiten zu verrichten haben, sowie über Bedienstete, die nicht der Gemeinde bzw. dem Dienstleister angehören, während der Betriebszeit des Systems ein Besucherbuch zu führen, in welches Name, Firma, Dienststelle, Zeitpunkt des Zutritts und Verlassens des Raumes (der Räume) des Systems, einzutragen sind.

Die Bediensteten, die am Betrieb des Systems teilhaben, haben die Pflicht, den Zutritt unbefugter Personen nach Möglichkeit zu verhindern.

Mitgliedern der Datenschutzkommission und des Datenschutzrates ist nach erfolgter Ausweisleistung der Zutritt zu gewähren, sofern sie im dienstlichen Auftrag tätig werden. Auf Verlangen sind die für deren Aufgabenerfüllung erforderlichen Auskünfte zu erteilen und die Einsicht in schriftliche Unterlagen zu gewähren. Im Fall des Zutritts eines Mitgliedes der Datenschutzkommission oder des Datenschutzrates sind umgehend der Verantwortliche für die Datensicherheitsmaßnahmen VB Siegfried Weber und der Bürgermeister der Marktgemeinde Gaming zu verständigen.

4.3. Zugriffsberechtigungen

4.3.1 Jedem Benutzer des Systems werden nach Maßgabe der rechtlichen, technischen und organisatorischen Voraussetzungen die für seinen Aufgabenbereich erforderlichen Zugriffsberechtigungen vom Betreiber des ZMR individuell zugewiesen, sofern nicht der gemäß Punkt 3 Verantwortliche vom Betreiber (hier: Abteilung IV/8 des Bundesministeriums für Inneres) ermächtigt wird, die Zugriffsberechtigungen für den Betrieb des ZMR selbst zu erteilen.

Der Datenschutz ist in diesem Zusammenhang nach Maßgabe der technischen Möglichkeiten durch die Verwendung der vom Betreiber vergebenen Benutzeridentifikationen und Kennwörter sicherzustellen.

Kennwörter sind jedenfalls geheimzuhalten und müssen in periodischen Zeitabständen geändert werden.

Benutzer werden jedenfalls nach dreimaliger Falscheingabe am System automationsgestützt gesperrt; die Freigabe der Benutzerberechtigung erfolgt nur über (fern-)schriftlichen Antrag von einem dazu berechtigten Administrator (bzw. gemäß Punkt 3 Verantwortlichen) beim Betreiber.

4.3.2. Sofern der gemäß Punkt 3 Verantwortliche vom Betreiber (hier: Abteilung IV/8 des Bundesministeriums für Inneres) ermächtigt wird, die Zugriffsberechtigungen für den Betrieb des ZMR selbst zu erteilen, hat er für seinen Zuständigkeitsbereich die Zugriffsberechtigungen für das ZMR für die einzelnen Benutzer individuell zuzuweisen. Er hat hiebei insbesondere für die Erfassung der Zugriffsberechtigten und deren einzelne Berechtigungen zum System zu sorgen und die Aufgabenbereiche der Zugriffsberechtigten, den Umfang der Zugriffsberechtigung(en) zum ZMR (Update, Anfragen) festzulegen, sowie die Veränderungen (einschließlich des Entzugs der Berechtigungen) im Bereich des auf das ZMR zugriffsberechtigten Personals umzusetzen.

4.3.3. Benutzer sind vom gemäß Punkt 3 Verantwortlichen von der weiteren Benutzung für immer oder für eine bestimmte Zeit von der Ausübung ihrer Zugriffsberechtigung auszuschließen, wenn

1. sie diese zur weiteren Erfüllung der ihnen übertragenen Aufgaben nicht mehr benötigen oder

2. sie die Daten nicht entsprechend den für den Betrieb des ZMR maßgeblichen Bestimmungen verwenden.

Der oa. Entzug der Zugriffsberechtigung ist vom gemäß Punkt 3 Verantwortlichen dem Betreiber des ZMR unverzüglich mitzuteilen, sofern ihm die Datenerfassung für die Benutzerverwaltung des ZMR nicht vom Betreiber übertragen wurde.

4.3.4. Benützung von Schnittstellen

Bei Nutzung der Schnittstellen zum ZMR (Applikationsgateways) sind jedenfalls zur Identifikation des Benutzers sowie zur Protokollierung der Datenverarbeitung die Stammdaten eines Benutzers (Familienname, Vorname, User-ID, SV-Nr., und Berechtigung) an das BMI-Portal zu übermitteln.

4.4. hinsichtlich der Betriebsräume

Der Raum des Systems stellt eine Sicherheitszone dar (Einzelplatzsystem). Bei Mehrplatzsystemen ist eine Unterteilung in mehrere Sicherheitszonen vorzunehmen (Server/Arbeitsplätze). Die Sicherheitszonen sind jeweils durch geeignete Maßnahmen vor dem Zutritt unberechtigter bzw. unbefugter Personen zu schützen.

Die Aufstellung von EDV-Geräten, insbesondere Bildschirmen bzw. deren Betrieb hat unter Bedachtnahme darauf zu erfolgen, dass außenstehende Personen, wie Parteien, Angehörige und sonstige Unbefugte, deren Eintritt in den Raum (die Räume) des Systems durch den Dienstbetrieb notwendig wird, nicht Einblick in das ZMR haben können (entsprechende Aufstellung der Geräte, entsprechende Vorkehrung bei der Möblierung).

4.5. hinsichtlich der Hard- und Software

Sofern bei dem(n) Datensichtgerät(en) ein Betriebsschloß installiert ist, mit dessen Hilfe der Zugriff auf Daten verhindert wird, ist für den Zeitraum, in dem befugte Personen nicht im Raum (in den Räumen) des Systems aufhalten bzw. für den Zeitraum außerhalb der Betriebsstunden, dieses zu sperren und der Schlüssel so zu verwahren, dass unbefugte Personen keinen Zugriff haben können.

Jedenfalls ist bei Verlassen des Arbeitsplatzes zumindest die Bildschirmsperre zu aktivieren.

Im Falle von Betriebsstörungen, deren Behebung den Einsatz von Personen, die nicht der Gemeinde bzw. dem Dienstleister, bei dem der Gateway-Rechner installiert ist, angehören, erforderlich macht, sind die allenfalls im Zugriff befindlichen wechselbaren Datenträger aus den für den Systembenutzer zugänglichen Laufwerken zu entfernen und sicher zu verwahren, sowie der Zugriff auf Daten bzw. das unbefugte Lesen von Datenbeständen durch Hard- und/oder Softwaremaßnahmen zu verhindern.

Ein allenfalls vorhandener Server und dessen allenfalls vorhandene Konsole sind jedenfalls versperrt (z.B.: Sicherheitsschrank, Anlageraum) unterzubringen. Der gemäß Punkt 3 Verantwortliche hat Regeln betreffend die sichere Verwahrung und Ausgabe der Schlüssel für die Versperrungseinrichtung des Servers und deren Öffnung bzw. das Manipulieren am Server zu erlassen und für die Kontrolle von deren Einhaltung sowie für die Dokumentation dieser Vorgänge zu sorgen.

Für den Fall, dass der Server zu Servicezwecken aus dem Sicherheitsschrank und dieser oder ein Gateway-Rechner aus dem Bereich der Gemeinde bzw. des Dienstleiters, bei der er installiert ist, entfernt werden muß, ist dafür Sorge zu tragen, dass eine unautorisierte Verwendung nicht stattfinden kann. Bei einer Verbringung des Servers zu einer Fremdfirma, sind die Daten jedenfalls zu löschen und das Zertifikat zu deinstallieren. Dieser Vorgang ist im Schlüsselprotokoll zu dokumentieren.

4.6. hinsichtlich der Daten und externer Datenträger

Es ist sicher zu stellen, dass geeignete, dem jeweiligen Stand der Technik entsprechende und wirtschaftlich vertretbare Vorkehrungen getroffen werden, um eine Vernichtung oder Veränderung der Daten durch Programmstörungen (Viren) zu verhindern.

Das Auftreten von Programmstörungen, die den Datenbestand gefährden können, ist dem Betreiber des ZMR unverzüglich mitzuteilen.

Sämtliche personenbezogene Daten sind geheimzuhalten.

Sämtliche Datenträger sind so zu verwahren, dass sie vor unbefugtem Zugriff geschützt sind (versperrbare Kassetten, Schränke, Fächer, etc.). Der Zugriff zu den Datenträgern ist vom Verantwortlichen gemäß Punkt 3 zu organisieren und zu dokumentieren. Analoges gilt für Datensicherungen.

Ausdrucke oder sonstige schriftliche Unterlagen, die Daten des ZMR enthalten, sind, wenn sie nicht mehr für den Dienstgebrauch benötigt werden oder nach Ablauf der in den einschlägigen Kanzlei- und Skartierungsvorschriften festgelegten Aufbewahrungsdauer, so zu sammeln und zu vernichten, dass der Inhalt der Unterlagen nichtberechtigten Personen nicht zugänglich werden kann. Datenträger, die nicht mehr benötigt werden oder nicht mehr verwendet werden können, sind einer vollständigen physischen Löschung aller Daten auf dem Datenträger durch entsprechende Programme bzw. der kontrollierten Vernichtung zuzuführen.

4.7. Dokumentation (Protokollierung)

Unbeschadet der Verpflichtungen des Betreibers des ZMR ist dafür zu sorgen, dass Aufzeichnungen geführt werden, die die Zulässigkeit der tatsächlich im Bereich des ZMR

durchgeführten Verwendungsvorgänge im notwendigen Ausmaß nachvollziehbar machen, wie insbesondere Änderungen, Abfragen und Übermittlungen.

Zugriffsprotokolle sind gesichert aufzubewahren und - unbeschadet anderer Regelungen betreffend die Skartierung von Aktenstücken - 3 Jahre nach erfolgtem Zugriff auf das ZMR kontrolliert zu vernichten. Davon darf in jenem Ausmaß abgewichen werden, als der von der Protokollierung oder Dokumentation betroffene Datenbestand zulässigerweise früher gelöscht oder länger aufbewahrt wird (§ 14 Abs. 5 DSG 2000).

Protokoll- und Dokumentationsdaten dürfen nicht für Zwecke verwendet werden, die mit ihrem Ermittlungszweck – das ist die Kontrolle der Zulässigkeit der Verwendung des protokollierten oder dokumentierten Datenbestandes – unvereinbar sind. Unvereinbar ist insbesondere die Weiterverwendung zum Zweck der Kontrolle von Betroffenen, deren Daten im protokollierten Datenbestand enthalten sind, oder zum Zweck der Kontrolle jener Personen, die auf den protokollierten Datenbestand zugegriffen haben, aus einem anderen Grund als jenem der Prüfung ihrer Zugriffsberechtigung, es sei denn, dass es sich um die Verwendung zum Zweck der Verhinderung oder Verfolgung eines Verbrechens nach § 278a StGB (kriminelle Organisation) oder eines Verbrechens mit einer Freiheitsstrafe, deren Höchstmaß fünf Jahre übersteigt, handelt

5. Kontrolle der Einhaltung dieser Sicherheitsvorschrift

Die Kontrolle der Einhaltung der Datensicherheitsvorschriften für das System obliegt dem gemäß Punkt 3 Verantwortlichen. Er hat dafür Sorge zu tragen, dass eine aktuelle Fassung dieser Datensicherheitsvorschrift zur Einsichtnahme durch die Benutzer an jedem System-Arbeitsplatz aufliegt. Ihm obliegt die Sammlung bzw. Aktualisierung sämtlicher Vorschriften, die sich auf den Systemarbeitsplatz beziehen.

Darüberhinaus überprüft der Betreiber (hier: Abteilung IV/8 des Bundesministeriums für Inneres) im Zusammenwirken mit der Meldebehörde durch Stichproben, ob die Verwendung der Daten des ZMR den einschlägigen Bestimmungen entsprechend erfolgt und die erforderlichen Datensicherheitsmaßnahmen ergriffen worden sind.

6. Zulässige Abweichungen von dieser Sicherheitsvorschrift

Der gemäß Punkt 3 Verantwortliche ist berechtigt, bei Gefahr im Verzug Abweichungen von dieser Datensicherheitsvorschrift anzuordnen. Sollte eine Abweichung von dieser Datensicherheitsvorschrift erforderlich geworden sein, sind ehestmöglich der Dienststellenleiter bzw. dessen Vertreter und der Betreiber des ZMR (hier: Abteilung IV/8 des Bundesministeriums für Inneres) zu verständigen. Abweichungen von der Datensicherheitsvorschrift sind schriftlich festzuhalten.

In den Anordnungen für den Katastrophenfall, die vom Bürgermeister oder Vizebürgermeister auf Grund der örtlichen Gegebenheiten zu erlassen sind, sind Datenschutzaspekte soweit als möglich zu berücksichtigen.

7. Private Dienstleister

Bedient sich die Meldebehörde für den Datenverkehr mit dem Zentralen Melderegister eines privaten Dienstleisters, ist dieser - unbeschadet der sonstigen gesetzlichen Verpflichtungen gemäß §§ 10ff DSG 2000 - zur Einhaltung aller datenschutzrechtlichen Bestimmungen und Ergreifung der in dieser Vorschrift und in der Meldedatensicherheitsmaßnahmen-Verordnung

des Bundesministers für Inneres, BGBl. II Nr. 174/2001, vorgesehenen Datensicherheitsmaßnahmen zu verpflichten.

Der Wechsel oder das Ausscheiden eines Dienstleisters ist dem Betreiber des ZMR (hier: Abteilung IV/8 des Bundesministeriums für Inneres) unverzüglich mitzuteilen.

8. Inkrafttreten

Diese Sicherheitsvorschrift tritt am 25.10.2001 in Kraft.