Nutzungsbedingungen für das PVP-Standardportal

Ausgangslage
Gemäß § 42 des Jagdgesetzes hat der Jagdnutzungsberechtigte jeden Abschuss von Wild, welcher dem Abschussplan unterliegt, innerhalb einer Woche der Behörde zu melden. Dabei können die Abschussmeldungen (sowie die Eintragungen in die Abschussliste) gemäß § 32 Abs. 1 der Jagdverordnung – nach Maßgabe vorhandener technischer Möglichkeiten – in elektronischer Form erfolgen. Der Jagdnutzungsberechtigte hat der Behörde, dem Jagdverfügungsberechtigten sowie dem Obmann der Hegegemeinschaft jederzeit Einsicht in die Abschussliste zu gewähren. Das Tagebuch des Kontrollorgans in elektronischer Form wird dabei automatisch mitgeführt.

Dem Jagdnutzungsberechtigten, dem Jagdverfügungsberechtigten, dem Jagdschutzorgan, dem Kontrollorgan sowie dem Obmann der Hegegemeinschaft soll daher eine Zugriffsmöglichkeit unter Einhaltung der nachstehenden Sicherheitsanforderungen zur Anwendung:

Jagdverwaltung (JVW)

über das **externe Stammportal des Amts der Vorarlberger Landesregierung** eingerichtet werden.

Damit treten die oben genannten Personen als Teilnehmer/Benutzer am Portalverbundsystem auf. Dazu sind zum Zweck der Sicherstellung des technischen und organisatorischen Zugangs zu der genannten Anwendung in der Portalverbundvereinbarung die folgenden Bedingungen einzuhalten.

Ziele
Das vorliegende Dokument soll die technischen und organisatorischen Sicherheitsmaßnahmen spezifizieren, welche von Benutzerinnen und Benutzern bei der Nutzung von Anwendungen zu treffen bzw. einzuhalten sind.
Ziel dieser Maßnahmen ist die Gewährleistung von

- Vertraulichkeit (Geheimhaltung der Information),
- Integrität (Schutz vor unbefugter Veränderung der Information) und
- Zurechenbarkeit (Nachvollziehbarkeit der Verarbeitungsvorgänge).

ORGANISATORISCHE MASSNAHMEN

Zugriff zur Jagdverwaltung (JVW)

Um an die Behörde in der Anwendung „Jagdverwaltung“ (JVW) die Abschussmeldungen digital mitteilen zu können, wird die Handy-Signatur benötigt.
Es wird ein aktueller Browser vorausgesetzt, d.h. die Anwendung kann mit einem Microsoft Edge, Google Chrome, Firefox oder Safari in der aktuellsten Version bedient werden. Mit dem Internet Explorer 11 kann die Anwendung nicht bedient werden. Außerdem kann die JVW auch mit mobilen Endgeräten (Tablet, Smartphone) bedient werden.
Die Benutzer dürfen die Zugangsdaten keinen anderen Personen bekannt- bzw. weitergeben.

TECHNISCHE MASSNAHMEN

Erlaubte Endgeräte

Für den Zugang zu der genannten Anwendung sind nur vertrauenswürdige Endgeräte zugelassen. Als vertrauenswürdig gelten die Endgeräte dann, wenn diese unter eigener Kontrolle stehen, mit Passwort geschützt sind und einen aktuellen Viren- und Malewareschutz besitzen. Ausdrücklich verboten ist die Verwendung von öffentlich zugänglichen Endgeräten (wie z.B. Internetcafe).

DATENSCHUTZ

Belehrung über die Bestimmungen des Datenschutzes

Benutzerinnen und Benutzer erhalten voraussichtlich Kenntnis über personenbezogene Daten (das sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen), die Ihnen ausschließlich aufgrund der zugeordneten Rolle anvertraut oder zugänglich gemacht werden.

Die Benutzerin/der Benutzer, nimmt daher zur Kenntnis,

- dass personenbezogene Daten natürlicher Personen dem Schutz durch die europäische Datenschutzverordnung (DSGVO), durch das innerstaatliche Datenschutzgesetz (DSG) und das Landes-Datenschutzgesetz unterliegen,
- dass auch juristische Personen durch das Datenschutzgesetz (DSG) ein Anspruch auf Geheimhaltung der sie betreffenden personenbezogenen Daten zukommt,
- dass personenbezogene Daten, die ihr/ihm anvertraut oder zugänglich gemacht wurden, unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten, geheim zu halten sind, soweit kein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen personenbezogenen Daten besteht (Datengeheimnis, vgl., §6 DSG),
- dass allfällige weiterreichende andere Bestimmungen über die Geheimhaltungspflichten ebenfalls zu beachten sind,
- dass es insbesondere untersagt ist, unbefugten Personen oder unzuständigen Stellen schutzwürdige personenbezogene Daten mitzuteilen oder ihnen die Kenntnisnahme zu ermöglichen,
- dass es untersagt ist, personenbezogene Daten zu einem anderen Zweck als für die Besorgung der übertragenen Aufgaben zu verarbeiten,
- dass personenbezogene Daten nicht unbefugt beschafft werden dürfen (beispielsweise keine unautorisierten Abfragen),
- dass Verletzungen des Datenschutzes und der Datensicherheit zu melden sind, und
- dass diese Verpflichtungen auch nach Beendigung ihrer/seiner Tätigkeit und nach dem Ausscheiden aus der Funktion fortbestehen.