



Einwohnergemeinde Moosseedorf

Weisung Datenschutz und Informationssicherheit

Gemeinderat
... April 2005

Inhaltsverzeichnis

1	ALLGEMEINE BESTIMMUNGEN	3
1.1	WEITERFÜHRENDE INFORMATIONEN	3
1.2	ZWECK	3
1.3	GELTUNGSBEREICH	3
1.4	VERANTWORTUNG DER ANWENDERINNEN UND ANWENDER	3
1.5	RECHTLICHE GRUNDLAGEN	3
1.6	MITGELTENDE UNTERLAGEN IM ANHANG ZUR WEISUNG	4
2	DATENSCHUTZ	5
2.1	BEGRIFF	5
2.2	EINSICHTSRECHT	5
2.3	DATENSPERRE	5
2.4	AUSKUNFTERTEILUNG AN DRITTE	5
2.5	DATENBEARBEITUNG DURCH DIE GEMEINDE	5
3	INFORMATIONSSICHERHEIT	6
3.1	BEGRIFF	6
3.2	NUTZUNG DER IN DER GEMEINDEVERWALTUNG EINGESETZTEN INFORMATIONSMITTEL	6
3.3	DATENSICHERUNG	6
3.4	BERECHTIGUNGSKONZEPT	7
3.4.1	<i>Zutritt</i>	7
3.4.2	<i>Zugang und Zugriff</i>	7
3.5	NUTZUNG INTERNET	7
3.6	NUTZUNG E-MAIL	8
4	SCHLUSSBESTIMMUNGEN	9
4.1	ZUSTÄNDIGKEIT	9
4.2	MASSNAHMEN BEI MISSBRAUCH	9
4.3	GÜLTIGKEIT	9
5	ANHANG	9

1. Allgemeine Bestimmungen

1.1 Weiterführende Informationen

Diese Weisung enthält nicht explizit alle Informationen zum Datenschutz und der Datensicherheit. Sind Fragen offen, ist es Aufgabe der Mitarbeiterin oder des Mitarbeiters, sich die fehlende Information zu beschaffen. Die Verantwortlichen für den IT-Betrieb und den Datenschutz der Gemeindeverwaltung sind dafür die ersten Ansprechpersonen. Ausserdem wird auf die Rechtsgrundlagen und die mitgeltenden Unterlagen in Kapitel 1.4 und 1.5 verwiesen.

1.2 Zweck

Die Weisung regelt die Nutzungs- und Überwachungsvorschriften für die Informatikmittel der Gemeindeverwaltung sowie den Gebrauch von Internet und E-Mail. Damit wird die Sicherstellung der Nutzung der Informatikmittel und die Sicherheit der Daten und Anwendungen bezweckt. Die Gewährleistung des Datenschutzes und der Persönlichkeitsrechte, die durch die Bearbeitung schützenswerter Daten tangiert sind, ist ein weiteres Ziel dieser Weisung.

1.3 Geltungsbereich

Die Weisung gilt für alle Mitarbeitenden der Gemeindeverwaltung und die Behördenmitglieder mit Zugang zu Informatikmitteln und schützenswerten Daten der Gemeinde. Temporäre Arbeitskräfte und externe Vertragspartner der Gemeinde mit Zugang zu Informatikmitteln und schützenswerten Daten werden der Weisung ebenfalls unterstellt und müssen die inhaltliche Kenntnisnahme unterschriftlich bestätigen.

1.4 Verantwortung der Anwenderinnen und Anwender

Grundsätzlich gilt die Eigenverantwortlichkeit für den recht- und zweckmässigen Einsatz der vorhandenen Informatikmittel und für den sorgfältigen Umgang mit schützenswerten Daten in physischer oder elektronischer Form. Dazu gehört auch der Erwerb und die Weiterentwicklung des Wissensstandes, der für die kompetente und verantwortungsvolle Aufgabenerfüllung notwendig ist. Die Gemeinde sorgt für die entsprechenden Weiterbildungsangebote.

Die Gemeinde bezeichnet eine Datenschutz- und IT-verantwortliche Person und betraut diese mit der Umsetzung und Aktualisierung der vorliegenden Weisung. Die Verantwortung und die Kompetenz, die dieser Position zukommen, entsprechen der Aufgabenstellung.

1.5 Rechtliche Grundlagen

Die rechtlichen Grundlagen sind in erster Linie in den Datenschutzgesetzen von Bund und Kanton enthalten. Weil für die Gemeindeverwaltung eine hohe Dichte von Spezialregelungen gilt, sind als Grundlage für diese Weisung alle auf der Basis der Datenschutzgesetzgebung erlassenen Spezialgesetze, Verordnungen, Richtlinien etc. aufgezeichnet worden. Auf sie wird im folgenden Kapitel verwiesen.

1.6 Mitgeltende Unterlagen im Anhang zur Weisung

Als mitgeltende Unterlagen zu dieser Weisung werden bezeichnet:

- Das Berechtigungskonzept für den Zugriff auf die über das TDLZ der Tankred Holding AG betriebenen SW-Applikationen
- Das Konzept der Schlüsselkontrolle
- Das Verzeichnis der Datensammlungen mit schützenswertem Inhalt gemäss der Liste, die dieser Weisung zu Grunde liegt
- Die Liste der Rechtsgrundlagen und weiteren Anforderungen von Bund, Kanton und Gemeinde gemäss der Liste, die dieser Weisung zu Grunde liegt
- Prüfungsschema des Datenschutzbeauftragten für die Datenbekanntgabe
- Benutzererklärung, womit die Mitarbeitenden bestätigen, vom Weisungsinhalt Kenntnis genommen zu haben und die Verpflichtung zu übernehmen, sich daran zu halten
- Austrittsbestätigung, womit die austretenden Mitarbeitenden, Behördenmitglieder sowie externe Auftragnehmer, den letzten Abschnitt des Punkts 3.2 dieser Weisung bestätigen

2 Datenschutz

2.1 Begriff

Ziel des Datenschutzes ist, die Privatsphäre und Persönlichkeitsrechte jedes Menschen umfassend zu schützen. Dieser Schutz ist gewahrt, wenn die bearbeiteten Daten bei der Gemeinde und ihren Organen bleiben und nicht unrechtmässigerweise weitergegeben werden.

Besonders schützenswerte Daten gemäss Art. 3 des Bundesgesetzes über den Datenschutz (DSG) sind:

- Daten über religiöse, weltanschauliche, politische oder gewerkschaftlichen Ansichten oder Tätigkeiten,
- Daten zur Gesundheit, der Intimsphäre oder der Rassenzugehörigkeit
- Daten bezüglich Massnahmen der sozialen Hilfe
- Daten zu administrativen oder strafrechtlichen Verfolgungen und Sanktionen

Zusätzlich zu dieser Definition sind alle jene Verhandlungen und Beschlüsse besonders schützenswert, die die Gemeindebehörde als solche bezeichnet.

2.2 Einsichtsrecht

Die Gemeinde führt ein Verzeichnis der von ihr geführten Datensammlungen. Dieses Verzeichnis ist öffentlich. Jede Person hat das Recht, über die eigenen Daten Auskunft zu erhalten.

2.3 Datensperre

Jede Person kann die Weitergabe ihrer Daten sperren lassen, es sei denn, dass Rechtsgrundlagen dagegen sprechen.

2.4 Auskunfterteilung an Dritte

Für die Auskunftserteilung an Dritte stützt sich die Gemeinde auf das Prüfungsschema für die Datenbekanntgabe des Datenschutzbeauftragten.

2.5 Datenbearbeitung durch die Gemeinde

Personendaten dürfen nur gesammelt und bearbeitet werden, soweit sie für die Aufgabenerfüllung der Gemeinde benötigt werden, und wenn dafür eine Rechtsgrundlage besteht.

Im Berechtigungskonzept ist geregelt, wer welche Daten bearbeiten darf.

3 Informationssicherheit

3.1 Begriff

Unter Informationssicherheit verstehen wir die Sicherung besonders schützenswerter Daten vor missbräuchlicher Verwendung, Beschädigung und Verlust.

3.2 Nutzung der in der Gemeindeverwaltung eingesetzten Informationsmittel

Unter Informationsmittel werden alle hardware- und softwareseitigen Geräte, Systeme, Programme und physischen Dossiers verstanden, die in der Gemeindeverwaltung zur Bearbeitung zur Verfügung gestellt werden.

Zuständig für die Installation, Konfiguration und die Inbetriebnahme von PCs und SW-Produkten ist die informatikverantwortliche Person der Gemeindeverwaltung.

Der Anschluss privater Peripheriegeräte an den Arbeitsstationen der Verwaltung ist nicht gestattet (Ausnahme: unterstützte Organizer und Pocket-PCs in Absprache mit der informatikverantwortlichen Person).

Der Zugriff auf die Arbeitsstation und die Daten wird mit dem persönlichen Passwort geschützt. Als Passwort ist ein alphanumerischer Begriff von mindestens 5 Stellen zu wählen. Persönliche Passwörter sind vor dem Zugriff unbefugter Dritter zu schützen und dürfen anderen Mitarbeitenden nicht weitergegeben werden.

Die Verwendung derselben User-ID für mehrere Personen ist grundsätzlich nicht gestattet. Nach dem Ausscheiden einer Person aus der Verwaltung oder Behörde darf die gleiche User-ID nicht vor zwei Jahren wieder vergeben werden.

Mitglieder der Behörde, der Verwaltung und temporär eingesetzte Vertragspartner, die berechtigt sind, Geschäftsvorfälle mit datenschutzrelevantem Inhalt elektronisch oder physisch innerhalb und ausserhalb der Büros der Gemeindeverwaltung zu bearbeiten, sind den gleichen Richtlinien unterstellt, wie sie innerhalb der Gemeindeverwaltung gelten. Bei auswärtiger Tätigkeit sind sie verantwortlich für den entsprechenden Zugriffsschutz zur Verhinderung unberechtigter Einsichtnahme und Verwendung.

Ausscheidende Mitglieder der Behörde, der Verwaltung oder externe Auftragnehmer bestätigen unterschriftlich, dass sämtliche schützenswerten Daten, die ihnen auf Grund ihrer Tätigkeit zugänglich waren, und die ausserhalb der Lokaltäten der Verwaltung redundant bearbeitet oder gespeichert wurden, unwiderruflich gelöscht, vernichtet oder der Verwaltung zurückgegeben worden sind.

3.3 Datensicherung

Die Datensicherung der Applikationen, die im Dienstleistungszentrum der Talus Informatik AG betrieben werden, ist vertraglich im Service Level Agreement geregelt.

Für nicht darunter fallende Applikationen gilt das Datensicherungskonzept.

3.4 Berechtigungskonzept

3.4.1 Zutritt

Die Zutrittsregelung ergibt sich aus dem Konzept zur Schlüsselkontrolle.

3.4.2 Zugang und Zugriff

Der Zugang und Zugriff zu den Daten und Applikationen ist funktionsgesteuert und im Berechtigungskonzept hinterlegt. Berechtigungen werden durch die datenschutzverantwortliche Person auf schriftlichen Antrag der Linienvorgesetzten zugewiesen. Die datenschutzverantwortliche Person führt darüber eine entsprechende Kontrolle.

Zur Verhinderung des unberechtigten Zugriffs sind beim Verlassen des Arbeitsplatzes (auch kurzzeitig) die Bildschirmsperre obligatorisch zu aktivieren.

Physische Dokumente sind so aufzubewahren, dass sie unberechtigten Zugriffen entzogen sind (abschliessbares Büro/Archiv, keine Einsicht auf Bildschirm und Dokumente durch unbefugte Dritte am Schalter oder in Sitzungszimmern).

3.5 Nutzung Internet

Das Internet steht für die Nutzung zur geschäftlichen Aufgabenerfüllung zur Verfügung. Das Internet ist ein Arbeitsmittel. Die Nutzung für private Zwecke ist auf ein Minimum zu beschränken.

Das Herunterladen, Kopieren und Installieren von Programmen durch die Benutzerinnen und Benutzer ist nicht gestattet. Bei besonderem Bedarf ist die Bewilligung der informatikverantwortlichen Person einzuholen.

Andere Daten oder Dateien einschliesslich Multimedia dürfen nur dann auf das Netzwerk der Verwaltung herunter geladen werden, wenn sie geschäftsrelevant sind und vom Virens Scanner nicht als sicherheitskritisch gemeldet werden.

Eine anonyme Auswertung der Internetzugriffe innerhalb der Verwaltung kann durch die Vorgesetzten angeordnet werden. Die Mitarbeitenden werden vorgängig über die Art der Auswertung informiert.

Wenn ein persönlicher Missbrauch des Internetzugangs vermutet wird, ist eine personenbezogene Auswertung zulässig. Die betroffenen Mitarbeitenden müssen vorgängig davon in Kenntnis gesetzt werden und das Einverständnis der personalverantwortlichen Person muss vorliegen.

3.6 Nutzung E-Mail

E-Mail steht für die Nutzung zu geschäftlichen Zwecken zur Verfügung und ist insofern ebenfalls ein Arbeitsmittel. Die Nutzung zu privaten Zwecken ist auf ein Minimum zu beschränken. Die Nutzung zu eigenen kommerziellen Zwecken ist nicht erlaubt.

Die Mitarbeitenden sind verpflichtet, nicht mehr benötigte Mails periodisch, d.h. mindestens monatlich aus dem Posteingang und –ausgang zu löschen.

Die Übermittlung schützenswerter Daten über E-Mail ist nicht gestattet.

Ohne Bewilligung der informatikverantwortlichen Person ist das Übermitteln von Programmen von und zum PC-Arbeitsplatz nicht gestattet.

Das Laden, Übertragen und Weiterleiten von Daten mit rassistischem, pornographischem oder anderem widerrechtlichen Inhalt ist verboten.

4 Schlussbestimmungen

4.1 Zuständigkeit

Für die Durchsetzung dieser Weisung sind die Linienvorgesetzten und die für Datenschutz und Informationssicherheit verantwortliche Person (Gemeindevorsitzende/r) zuständig.

Die Weisung ist integrierender Bestandteil des Arbeitsvertrages mit dem Personal bzw. der Wahllokale für Behördemitglieder bzw. des Zusammenarbeitsvertrags mit externen Partnern.

Wird beobachtet, dass eine Widerhandlung gegen diese Weisung vorliegt, besteht die Verpflichtung, die für den Datenschutz und die Informationssicherheit verantwortliche Person zu verständigen.

Die Weisung dient als Grundlage für die Ausübung der internen oder externen Aufsicht über den Datenschutz und die Informationssicherheit der Gemeinde.

4.2 Massnahmen bei Missbrauch

Ein widerrechtliches, weisungswidriges Verhalten im Umgang mit Datenschutz und Informationssicherheit bedeutet eine Pflichtverletzung, die zu arbeitsrechtlichen Sanktionen führen kann oder anderweitige rechtliche Konsequenzen nach sich zieht (Disziplinarrecht).

4.3 Gültigkeit

Die vorliegende Weisung wurde an der Gemeinderats vom ... April 2005 genehmigt und tritt per 1. Mai 2005 in Kraft.

Moosseedorf, ... April 2005

Gemeinderat Moosseedorf

Peter Bill
Gemeindepräsident

Peter Scholl
Gemeindevorsitzende/r

5 Anhang

Folgende elektronische Unterlagen gelten als Bestandteile dieser Weisung:

- Das Berechtigungskonzept für den Zugriff auf die über das TDLZ der Tankred Holding AG betriebenen SW-Applikationen
- Das Konzept der Schlüsselkontrolle nachgeführt durch die Liegenschaftsverwaltung
- Das Verzeichnis der Datensammlungen mit schützenswertem Inhalt gemäss der Liste, die dieser Weisung zu Grunde liegt
- Die Liste der Rechtsgrundlagen und weiteren Anforderungen von Bund, Kanton und Gemeinde gemäss der Liste, die dieser Weisung zu Grunde liegt
- Prüfungsschema des Datenschutzbeauftragten für die Datenbekanntgabe
- Benutzererklärung, womit die Mitarbeitenden bestätigen, vom Weisungsinhalt Kenntnis genommen zu haben und die Verpflichtung zu übernehmen, sich daran zu halten
- Austrittsbestätigung, womit die austretenden Mitarbeitenden, Behördenmitglieder sowie externe Auftragnehmer, den letzten Abschnitt des Punkts 3.2 dieser Weisung bestätigen