Vereinbarung über die Ziele und Grundsätze bei der Einführung und Nutzung von Fernsteuerungs-, Fernwartungs- und Auswertungssoftware nach § 81 NPersVG

Bek. d. MI v. 27.4.2007 – Nds MBl. Nr. 20/2007 S. 401

Zwischen der Niedersächsischen Landesregierung, vertreten durch das Ministerium für Inneres und Sport

einerseits

und dem Deutschen Gewerkschaftsbund DGB – Bezirk Niedersachsen Bremen Sachsen-Anhalt – und

dem dbb beamtenbund und tarifunion - landesbund niedersachsen –

andererseits

wird gemäß § 81 des Niedersächsischen Personalvertretungsgesetzes (NPersVG) in der Fassung vom 22.01.2007 (Nds. GVBl. 2007, S. 11) folgende Vereinbarung geschlossen:

I. Ziele

Die Verhandlungspartner stimmen darin überein, dass in der niedersächsischen Landesverwaltung zum Schutz der Beschäftigten vor einem unbefugten ebenso wie vor einem unkontrollierten Zugriff auf den Arbeitsplatz-PC, bzw. die Terminalserver-Sitzung, einschließlich der Daten und Programme sowie einer Verhaltens- und Leistungskontrolle Schutzmaßnahmen getroffen werden müssen. Dazu werden die folgenden Grundsätze zur Durchführung vereinbart.

II. Grundsätze zur Durchführung

1. Allgemeines

(1) Es werden die Grundsätze für den Umgang mit Fernsteuerungs-, Fernwartungs- und Auswertungssoftware festgelegt, die den kontrollierten Zugriff auf Benutzer-PC (Clients) und während der Terminalserver-Sitzungen erlauben.

(2) Diese Vereinbarung dient dem Schutz der Beschäftigten insbesondere vor

- einem unbefugten ebenso wie vor einem unkontrollierten Zugriff auf den Arbeitsplatz-PC bzw. die Terminalserver-Sitzung einschließlich der Daten und Programme,
- einer Verhaltens- und Leistungskontrolle und
- einer Nutzung von Daten für personalrechtliche Vorgänge (ausgenommen im Zusammenhang mit nachgewiesenen Dienstpflichtverletzungen), z.B. für Beurteilungen.

Sie dient außerdem der Gewährleistung der Informationssicherheit (Datensicherheit).

Beschreibung

Programme zum Fernzugriff auf Arbeitsplatz-PC und während der Terminalserver-Sitzungen sind ein Hilfsmittel für die Administration von Computernetzwerken. Sie ermöglichen die Wartung, Steuerung und Auswertung von fremden Rechnern in einem Netz von einem anderen Arbeitsplatz aus. Entsprechend den Funktionen der Software ist sowohl ein steuernder Eingriff als auch nur ein Lesezugriff möglich. Die Programme werden zur Fehlersuche und Fehlerbeseitigung, zur Softwareaktualisierung oder zur Auswertung im Rahmen der Hard- und Softwareinventarisierung eingesetzt. So kann die Anwenderin oder der Anwender dieser Programme (im Wesentlichen die Administration) z.B.

- eine Übersicht der Hardwarekomponenten und der aktiven Software erhalten,
- den Bildschirm angezeigt bekommen,
- Software auf dem Rechner installieren oder deinstallieren,
- Eingriffe in Dateien vornehmen,
- steuernd in den Dialog eingreifen,
- den gesteuerten Rechner neu starten,
- die Bedienung übernehmen.

In der Regel gibt es jeweils ein Programm für den steuernden Rechner und eines für den gesteuerten Rechner. Beide Programme müssen zur Fernsteuerung aktiv sein.

2. Eingesetzte Programme

(1) Zum Nachweis der eingesetzten Fernwartungs-, Fernsteuerungs- oder Auswertprogramme erhalten die betroffene Behörde und ihre Personalvertretung (wenn möglich elektronisch) rechtzeitig die jeweiligen aktuellen Produktblätter, aus denen sämtliche Produktfunktionen in vollem Umfang hervorgehen.

(2) Bei wesentlichen funktionalen Änderungen der eingesetzten Software sowie beim Einsatz neuer Software sind die oder der Datenschutzbeauftragte, die oder der IT-Sicherheitsbeauftragte und die Personalvertretung zu beteiligen.

3. Datensicherheit

(1) Zum Schutz vor unbefugten Fernzugriffen sind die Rechte für den Fernzugriff auf den notwendigen Kreis an Beschäftigten im First- und Second-Level-Support (erste Ansprechpartner bzw. Fachleute zu speziellen Problemen) zu beschränken. Die eingeräumten Zugriffsrechte sind zu protokollieren und den zuständigen Personalvertretungen unverzüglich mitzuteilen. Die im First- und Second-Level-Support eingesetzten Beschäftigten haben sich vor dem Fernzugriff angemessen zu authentisieren.

(2) Zum Schutz der Integrität (Garantie der Unverfälschtheit) der Daten ist durch die Umsetzung geeigneter technischer und / oder organisatorischer Maßnahmen (z. B. Rechtebeschränkung auf den Schreibzugriff, Verpflichtung auf besondere Sorgfaltspflicht) sicherzustellen, dass das Risiko eines Fehler verursachenden Eingriffs minimiert wird.

4. Datenschutz

Für Zwecke der Fehleranalyse und -behebung dürfen personenbezogene Daten oder Dateien mit personenbezogenen Daten nur mit vorheriger Zustimmung der Benutzerin oder des Benutzers kopiert oder übertragen werden. Im Übrigen ist der Zugriff auf und das Herunterladen von Dateien untersagt.

5. Unterrichtung der Benutzerinnen und Benutzer

(1) Der Fernzugriff ist nur mit der vorherigen Zustimmung der Benutzerin oder des Benutzers zulässig. Im Falle der Fernsteuerung wird nach einer telefonischen Kontaktaufnahme eine Meldung oder ein Symbol auf dem Bildschirm des ferngesteuerten Rechners angezeigt. Die Übernahme und Übergabe der Steuerung muss mit einem persönlichen Passwort geschützt sein. Die Benutzerin oder der Benutzer des ferngesteuerten PCs (Arbeitsplatz-PC oder Terminalserver-Sitzung) kann auf dem Bildschirm die Aktivitäten der Administration bzw. Systembetreuung verfolgen. Software, die dieses nicht ermöglicht, darf nicht eingesetzt werden.

(2) Automatische Updates der System- und Anwendungssoftware sind ohne Zustimmung zulässig. Eine Information der Benutzerin oder des Benutzers hat zu erfolgen.

6. Mitschnitt von Sitzungen

Der Mitschnitt von Sitzungen ist zum Zwecke einer leichteren Störungsdokumentation zulässig, wenn die Benutzerin oder der Benutzer vor Beginn zustimmt. Die Benutzerin oder der Benutzer ist zu Beginn einer Sitzung in der elektronischen Fernzugriffsabfrage (siehe Nr. 6) auf die Möglichkeit des Mitschnitts und ihr bzw. sein Verweigerungsrecht hinzuweisen. Soweit Inhalt bzw. Umfang der Dokumentation für die Benutzerin oder den Benutzer erst während der Sitzung erkennbar werden, ist ein Widerspruch auch zu diesem Zeitpunkt zu ermöglichen. Die Entscheidungen der Benutzer sind in der Datenbank der Service-Desk-Anwendung zu protokollieren (z. B. Mitschnitt erlaubt / verweigert). Sofern dies wirtschaftlich und programmtechnisch darstellbar ist, sollte eine elektronische Antwortmöglichkeit mit der Bestätigung der Fernzugriffsabfrage vorgesehen werden.

7. Auswertung von Inventarisierungsdaten

Die im Rahmen von Programmen zur standardisierten und automatisierten Inventarisierung erstellten Protokolle und Ergebnisse dürfen in einer geeigneten Form ausgewertet werden, um Geschäftsprozesse zu unterstützen. Dies gilt insbesondere für den Bereich der Störungsbehebung durch den Service-Desk. Hiervon sind personenbezogene Daten auszuschließen.

8. Verantwortlichkeit

(1) Die für den First- und Second-Level-Support eingesetzten Beschäftigten und deren Führungskräfte sind für den gewissenhaften Umgang mit den eingesetzten Programmen verantwortlich. Insbesondere dürfen sie programmtechnisch vorhandene Möglichkeiten einer Verhaltens- und Leistungskontrolle nicht nutzen bzw. deren Nutzung nicht anordnen oder zulassen.

(2) Die für den First- und Second-Level-Support eingesetzten Beschäftigten und, soweit erforderlich, deren Führungskräfte, sind auf Kosten des Dienstherrn im Umgang mit der Software zu unterweisen und über die Bedingungen und Risiken der Nutzung sowie über den Inhalt dieser Vereinbarung aufzuklären. Sie sind auf die strafrechtlichen Konsequenzen bei Verstößen gegen die Verschwiegenheitspflicht hinzuweisen. Sie haben die Teilnahme an der Unterweisung und die Kenntnis der Bedingungen und Risiken der Nutzung sowie die Kenntnis

dieser Vereinbarung schriftlich zu bestätigen. Die Bestätigungen werden zu ihren Personalakten genommen (Anlage).

9. Erstellung und Aufbewahrung von Protokollen, Protokolldateien und Mitschnitten

(1) Beim Einsatz einer Fernwartungs-, Fernsteuerungs- oder Auswertungssoftware werden automatisiert Protokolldateien erstellt, die festhalten, wann wer welche Funktionen auf welchem Rechner ausgeführt hat.

(2) Protokolldateien und Mitschnitte werden für den Zeitraum von sechs Monaten aufbewahrt, darüber hinaus nur bei Vorliegen von konkreten Anhaltspunkten für eine Straftat.

(3) Protokolldateien dürfen von der zuständigen Personalvertretungen unter Beteiligung der zuständigen Administratorin oder des zuständigen Administrators und der oder des behördlichen Datenschutzbeauftragten eingesehen werden. § 22 Abs. 4 NDSG bleibt unberührt.

(4) Protokolldateien dürfen von der zuständigen Administratorin oder dem zuständigen Administrators unter Beteiligung der oder des behördlichen Datenschutzbeauftragten eingesehen werden, wenn dies zur Aufgabenerfüllung erforderlich ist.

10. Verhaltens- und Leistungskontrolle, personenbeziehbare Auswertung von Protokolldateien und Mitschnitten

(1) Die Nutzung der sich aus dem Einsatz von Fernzugriffs- und Inventarisierungssoftware ergebenden Möglichkeiten einer Verhaltens- und Leistungskontrolle ist nicht gestattet.

(2) Eine personenbeziehbare Auswertung von Protokolldateien oder Mitschnitten ist nur bei hinreichendem Verdacht der Verletzung dienstrechtlicher bzw. arbeitsvertraglicher Pflichten oder auf Anordnung eines Gerichts bzw. einer Strafverfolgungsbehörde zulässig.

(3) Mit Ausnahme gerichtlich oder von einer Strafverfolgungsbehörde angeordneter Auswertungen ist vor einer beabsichtigten Auswertung die Zustimmung der zuständigen Personalvertretung einzuholen. Sie hat das Recht, an den ihrer Zustimmung unterliegenden Auswertungen teilzunehmen. Ziffer 10 Abs. 3 gilt entsprechend.

11. Informationsrechte

Der betroffenen Behörde, ihrer Personalvertretung, ihrer Frauenbeauftragten, ihrer Schwerbehindertenvertretung, der oder dem behördlichen Datenschutzbeauftragten und der oder dem IT-Sicherheitsbeauftragten werden auf Wunsch alle Informationen über die eingesetzten bzw. einzusetzenden Programme vom Ministerium für Inneres und Sport zur Verfügung gestellt. § 22 Abs. 4 NDSG bleibt unberührt.

12. Rechte der Beschäftigten

Die Beschäftigten sind vor der Einführung und während der weiteren Nutzung von Fernsteuerungs-, Fernwartungs- und Auswertungssoftware von der betroffenen Behörde rechtzeitig und umfassend zu informieren.

14. Inkrafttreten

Diese Vereinbarung tritt mit Wirkung vom 25.4.2007 in Kraft.

Anlage

zur Vereinbarung über die Ziele und Grundsätze bei der Einführung und Nutzung von Fernsteuerungs-, Fernwartungs-, Auswertungssoftware

Bestätigung durch Frau / Herrn (Name)

Hiermit bestätige ich meine Teilnahme an der Unterweisung zu dem Programm

_____

am _____.

Ich wurde dabei über die Funktionalitäten des Programms, die technischen Möglichkeiten und die Einsatzbereiche aufgeklärt.

Außerdem wurde mir die „Vereinbarung über die Ziele und Grundsätze bei der Einführung und Nutzung von Fernsteuerungs-, Fernwartungs-, Auswertungssoftware“ in der aktuellen Fassung erläutert und ausgehändigt. Insbesondere wurde ich über die Bedingungen und Risiken der Nutzung der Software aufgeklärt und über das Verbot einer Verhaltens- und Leistungskontrolle der betroffenen Benutzerinnen und Benutzer sowie über meine Sorgfaltspflicht im Umgang mit dem Programm zum Schutz der Datenintegrität unterrichtet.

_____

(Ort, Datum)

_____

(Unterschrift der oder des Beschäftigten)