2030.4-J

Dienstvereinbarung über die Nutzung einer Fernadministrationssoftware bei den Justizvollzugseinrichtungen im Geschäftsbereich des Bayerischen Staatsministeriums der Justiz

Bekanntmachung des Bayerischen Staatsministeriums der Justiz vom 20. Mai 2019, Az. F4 - 1518 - VIIa - 9443/2017

(BayMBl. Nr. 381)

Zitiervorschlag: Bekanntmachung des Bayerischen Staatsministeriums der Justiz über die Dienstvereinbarung über die Nutzung einer Fernadministrationssoftware bei den Justizvollzugseinrichtungen im Geschäftsbereich des Bayerischen Staatsministeriums der Justiz vom 20. Mai 2019 (BayMBl. Nr. 381)

Zur Gewährleistung der schutzwürdigen Interessen und Belange der Beamtinnen und Beamten sowie Arbeitnehmerinnen und Arbeitnehmer (im Folgenden Beschäftigte) schließen das Bayerische Staatsministerium der Justiz und der in seinem Zuständigkeitsbereich gebildete Hauptpersonalrat beim Bayerischen Staatsministerium der Justiz gemäß Art. 73 in Verbindung mit Art. 75a Abs. 1 des Bayerischen Personalvertretungsgesetzes (BayPVG) im Sinne einer vertrauensvollen Zusammenarbeit folgende Dienstvereinbarung:

1. Allgemeines

1.1

Zur Sicherstellung des IT-Betriebs und der IT-Betreuung von Arbeitsplatz-PC (= APC) und Anwendungen ist der Einsatz von Fernadministrationssoftware notwendig. Fernadministrationssoftware wird verwendet, um Servicearbeiten über das Netz auf einem entfernten Rechner durchzuführen.

Der Einsatz der Fernadministrationssoftware ist in den bayerischen Justizvollzugseinrichtungen für drei Bereiche vorgesehen:

a) Unterstützung von Beschäftigten und Fehlerbehebung,

b) Software-Installation und -Update sowie

c) Aufklärung von Missbrauchsverdacht und Gefahrenabwehr.

1.2

Über die Fernadministrationssoftware wird keine Leistungs- und Verhaltenskontrolle der Beschäftigten durchgeführt.

2. Geltungsbereich

Die Dienstvereinbarung bezieht sich auf die individuelle Nutzung der Fernadministrationssoftware und die damit verbundene Protokollierung sowie die Gewährleistung von Datenschutz und Datensicherheit in den Justizvollzugseinrichtungen im Geschäftsbereich des Staatsministeriums der Justiz.

3. Berechtigungen und Beteiligte

3.1

Bei der Fernadministrationssoftware werden zwei Berechtigungsstufen unterschieden:

3.1.1 Berechtigungsstufe 1:

Der Verbindungsaufbau ist nur mit ausdrücklicher Zustimmung des APC-Anwenders zulässig. Die Rechte des Support-Mitarbeiters auf dem APC (Anwender- bzw. Administratorrechte) werden durch die entsprechende Anmeldung bestimmt.

Bei Anwenderrechten ist weder die Installation von Anwendungen noch die Änderung der Systemkonfiguration möglich. Der Support-Mitarbeiter kann nur auf solche Daten zugreifen, für die der jeweilige Bedienstete selbst die Zugriffsberechtigungen besitzt (z. B. Netzlaufwerke). Mit Kennwortschutz versehene Anwendungsdateien können nicht geöffnet werden (z. B. bei ZIP-Archiven, MS-Office-Dateien).

Bei Administratorrechten sind die Installation von Anwendungen und die Änderung der Systemkonfiguration auf dem APC möglich. Der Support-Mitarbeiter kann auf sämtliche gespeicherten Daten (z. B. Dokumente, Dateien und Programme) des Systems zugreifen. Mit Kennwortschutz versehene Anwendungsdateien können nicht geöffnet werden (z. B. bei ZIP-Archiven, MS-Office-Dateien).

3.1.2 Berechtigungsstufe 2:

Die Verbindung kann ohne Zustimmung des Beschäftigten erfolgen. Bei den Rechten des Support-Mitarbeiters auf dem APC handelt es sich um Administratorrechte. Die Installation von Anwendungen, deren Aktualisierungen und die Änderung der Systemkonfiguration auf dem APC sind möglich. Der Support-Mitarbeiter kann auf sämtliche gespeicherten Daten des Systems (z. B. Dokumente, Dateien und Programme) zugreifen. Mit Kennwortschutz versehene Anwendungsdateien können nicht geöffnet werden (z. B. bei ZIP-Archiven, MS-Office-Dateien).

3.2

Folgenden Benutzergruppen, die in dieser Dienstvereinbarung als „Support-Mitarbeiter“ bezeichnet werden, steht die Fernadministrationssoftware zur Verfügung:

Mitarbeiter

- der IT-Leitstelle der Bayerischen Justizvollzugsakademie,
- der örtlichen IT-Leitung mit der Berechtigungsstufe 1 für ihren Zuständigkeitsbereich oder
- eines beauftragten Unternehmens mit der Berechtigungsstufe 1 gemäß Nr. 3.1.1.

4. Sonderberechtigungen

4.1

In folgenden Fällen ist die Zustimmung des Beschäftigten zum Aufbau einer Fernadministrationszugangsverbindung entbehrlich (Berechtigungsstufe 2):

4.1.1

bei Bedrohung des Justiznetzes durch Viren oder sonstige Schadprogramme, sofern der Bedrohung nicht in anderer Weise entgegengewirkt werden kann;

4.1.2

zur Fehlerbehebung, sofern der Beschäftigte dem im Vorfeld zugestimmt hat;

4.1.3

zur Fehlerbehebung am Wochenende bzw. an sonstigen dienstfreien Tagen nach einer durchgeführten Softwareverteilung, sofern die Maßnahme die Betriebsfähigkeit des APC sichert.

4.2

Bei durch Tatsachen begründetem Missbrauchsverdacht oder begründetem Verdacht auf einen dienst-, arbeits- oder datenschutzrechtlichen Verstoß können unter Beachtung der Verhältnismäßigkeit sowie der datenschutzrechtlichen Vorschriften personenbezogene Missbrauchskontrollen durchgeführt werden.

4.3

In den Fällen gemäß den Nrn. 4.1.1, 4.1.3 und 4.2 ist der Beschäftigte unter Mitteilung der Grundlage und der erfolgten Maßnahmen unverzüglich zu informieren.

4.4

Durch Maßnahmen nach Nr. 4.2 gewonnene Daten werden auf Anordnung des für die Sicherheit des Justiznetzes zuständigen Beschäftigten (sog. Ressort-CERT) durch die Support-Mitarbeiter ausgewertet und der zuständigen Stelle übergeben. Der von der Kontrolle betroffene Beschäftigte ist von der zuständigen Stelle über Umfang, Zweck und Ergebnis einer solchen Missbrauchskontrolle zu unterrichten und ihm ist vor der Einleitung weiterer Maßnahmen Gelegenheit zur Stellungnahme zu geben, soweit nicht Gründe der Unaufschiebbarkeit oder der Geheimhaltung einer Maßnahme entgegenstehen. Die zuständige Personalvertretung ist unverzüglich zu unterrichten, sofern dies durch den Beschäftigten beantragt wird. Der Beschäftigte ist hierüber zu belehren.

Unterlagen sind nach Gebrauch unverzüglich zu vernichten, soweit Rechtsvorschriften nicht entgegenstehen.

4.5

Jeder Zugriff entsprechend der Berechtigungsstufe 2 muss unabhängig von der Protokollierung dokumentiert und begründet werden.

5. Rahmenbedingungen

5.1

An die Fernadministrationssoftware werden folgende Anforderungen gestellt:

5.1.1

Die Fernadministrationssoftware muss über einen Passwort-Schutz und einen Freigabemodus verfügen.

5.1.2

Die Kontrolle des Systems und der Zugang zum System des Beschäftigten müssen durch einen optischen Hinweis angezeigt werden. Der Beschäftigte kann sich damit über den Zustand eines Fernadministrationszugangs informieren.

5.1.3

Im kooperativen Betrieb (Standardfall) können sowohl der Beschäftigte als auch der Support-Mitarbeiter, der den Fernadministrationszugang nutzt, Maus und Tastatur kontrollieren. Der Beschäftigte kann jederzeit einseitig die Verbindung beenden.

5.1.4

Im exklusiven Modus (bei Softwareverteilung) können nur über den Fernadministrationssoftwarezugang Tastatur und Maus kontrolliert werden; der Beschäftigte hat hierauf keine Zugriffsmöglichkeit mehr und aus Sicherheitsgründen auch keine Möglichkeit, die Verbindung zu trennen.

5.1.5

Die Kommunikation zwischen APC und dem Support-Mitarbeiter ist zu verschlüsseln.

5.2

Für Support-Mitarbeiter gelten folgende Regelungen:

5.2.1

Der Support-Mitarbeiter darf nur mit Zustimmung des Beschäftigten vom übernommenen Bildschirm Hardcopys erstellen, ausdrucken oder elektronisch ablegen.

5.2.2

Der Support-Mitarbeiter darf nur zur Problembearbeitung auf die Daten des Systems zugreifen.

5.2.3

Anwenderdaten (z. B. erstellte Dokumente, Dateien, Ordner etc.) dürfen nur mit Zustimmung des Beschäftigten vom APC des Beschäftigten zur Weiterverwendung, Weiterverarbeitung oder zu anderen Zwecken gespeichert, übermittelt, kopiert oder gelöscht werden.

5.2.4

Sofern externe Dienstleister die Fernadministrationssoftware nutzen, müssen deren Mitarbeiter durch das Unternehmen mit den datenschutzrechtlichen Vorschriften vertraut gemacht und auf Einhaltung des Datenschutzes verpflichtet worden sein. Darüber hinaus sind sie durch die Justizverwaltung nach dem Verpflichtungsgesetz zu verpflichten.

6. Protokollierung

6.1

Bei der Protokollierung werden die Standard-Einstellungen wie vom Software-Hersteller empfohlen verwendet.

Dabei werden nur Informationen über Verbindungsauf- und -abbau, den jeweiligen Zeitpunkt, Zustimmung des Beschäftigten, Fernadministrations-Server, Ziel-APC und Dateitransfer protokolliert.

6.2

Eine Protokollierung von Aktionen und Arbeitsabläufen des Beschäftigten erfolgt innerhalb der Fernadministrationssoftware nicht.

6.3

Die Protokolldateien der Fernadministrationssoftware sind zentral und vor unberechtigtem Zugriff geschützt zu speichern. Eine automatisierte Löschung erfolgt nach Ablauf von 90 Tagen.

In den Fällen nach Nr. 4.2 werden auf Anordnung des für die Sicherheit des Justiznetzes zuständigen Beschäftigten (sog. Ressort-CERT) die protokollierten Daten vor der automatisierten Löschung gesichert.

6.4

Die Protokolldaten dürfen ausschließlich zur Datenschutzkontrolle, zur Verfolgung von Missbrauch und zur Sicherstellung eines ordnungsgemäßen Betriebes der Systeme verwendet werden.

7. Kontrollen des Einsatzes der Fernadministrationssoftware

7.1

Zur Überwachung der Einhaltung der Nutzungsregelungen können unter Beachtung der Verhältnismäßigkeit sowie der datenschutzrechtlichen Vorschriften Kontrollen bei den Support-Mitarbeitern, insbesondere Stichproben- und Verdachtskontrollen, durchgeführt werden.

7.2

Die Kontrollen werden auf Anordnung des für die Sicherheit des Justiznetzes zuständigen Beschäftigten (sog. Ressort-CERT) durchgeführt. Die gewonnenen Daten werden auf Anordnung des für die Sicherheit des Justiznetzes zuständigen Beschäftigten (sog. Ressort-CERT) durch die für den Betrieb der

Fernadministrationssoftware zuständigen Mitarbeiter in Bezug auf die Einhaltung der Nutzungsregelungen ausgewertet (keine Leistungskontrolle) und dem Ressort-CERT anonymisiert übergeben.

Der von der Kontrolle betroffene Support-Mitarbeiter ist über Umfang, Zweck und Ergebnis einer solchen Kontrolle unverzüglich zu unterrichten.

8. Personalvertretungen

8.1

Der Hauptpersonalrat bei dem Bayerischen Staatsministerium der Justiz hat, soweit es zur Durchführung seiner Aufgaben erforderlich ist, jederzeit das Recht auf Auskunft und Information in sämtlichen die Fernadministration betreffenden Fragen. Dies gilt auch für die damit verbundenen Fragen, die sich aus der Protokollierung, Auswertung und Durchführung von Kontrollen sowie der Gewährleistung von Datenschutz und Datensicherheit ergeben.

8.2

Im Übrigen werden dem Hauptpersonalrat bei dem Bayerischen Staatsministerium der Justiz Auswertungen zur Verfügung gestellt, soweit dies für die Durchführung seiner Aufgaben erforderlich ist.

9. Sanktionen

Verstöße gegen diese Dienstvereinbarung können dienst- und arbeitsrechtliche sowie auch strafrechtliche Konsequenzen haben.

10. Übertragung von Aufgaben des IT-Betriebs an Dienstleister

Soweit das Staatsministerium der Justiz Aufgaben des IT-Betriebs und der IT-Betreuung an Dienstleister (z. B. private Unternehmen, staatliche Rechenzentren) überträgt, stehen diesen die Befugnisse bzw. Verpflichtungen nach Maßgabe der hierüber geschlossenen Dienstleistungsvereinbarungen zu.

11. Gleichstellungsklausel

Alle Personen-, Status- und Funktionsbezeichnungen in dieser Dienstvereinbarung gelten jeweils in männlicher und weiblicher Form.

12. Inkrafttreten, Laufzeit, Außerkrafttreten

12.1

Die Dienstvereinbarung tritt am Tage nach ihrer Veröffentlichung in Kraft.

Sie kann mit einer Frist von sechs Monaten zum Ende eines Kalendermonats schriftlich gekündigt werden. In diesem Fall werden unverzüglich Verhandlungen zum Abschluss einer neuen Dienstvereinbarung aufgenommen.

12.2

Nach Außerkrafttreten der Dienstvereinbarung wegen Kündigung gelten ihre Regelungen bis zum Abschluss einer neuen Dienstvereinbarung weiter.

München, den 20. Mai 2019

Bayerisches Staatsministerium der Justiz	Hauptpersonalrat bei dem Bayerischen Staatsministerium der Justiz
Prof. Dr. Frank Arloth	Ralf Simon
Ministerialdirektor	Vorsitzender