Hinweise zur Videoprotokollierung von administrativen Tätigkeiten bei Verarbeitungen personenbezogener Daten

Stand: 16.03.2108

Die Datenschutzgrundverordnung (DSGVO) fordert in Artikel 5, dass Verantwortliche nicht nur die Grundsätze der Datenverarbeitung (Artikel 5 Abs.1) einhalten, sondern die Einhaltung auch nachweisen können müssen (Artikel 5 Abs. 2, „Rechenschaftspflicht“).

„Verantwortlicher“ ist nach Artikel 4 Nr. 7 (DSGVO) „die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“.

Die Nachweispflicht erstreckt sich auch auf die Umsetzung technisch-organisatorischer Sicherheits- und Datenschutzmaßnahmen (Artikel 24 Abs. 1). Bedient sich ein Verantwortlicher eines Auftragsverarbeiters (Artikel 4 Nr. 8), so bleibt er für die Einhaltung der Grundsätze verantwortlich (Artikel 28); der Auftragsverarbeiter hat entsprechende Informationen zuzuliefern. Dazu gehört auch der Nachweis, dass die Verarbeitung nur gemäß den Weisungen des Auftraggebers erfolgt (Artikel 28 Abs. 3 lit 3).

Eine Maßnahme zur Führung des Nachweises ist die Protokollierung von Tätigkeiten. Dies bezieht sich zum einen auf Inhalte der Verarbeitung (Wer hat wann welche Daten wie verarbeitet?), zum anderen auf administrative Tätigkeiten. Administrative Tätigkeiten sind solche, die die Änderungen an Verfahren und Verfahrensweisen bewirken, z.B. Konfigurationsänderungen, Berechtigungsänderungen oder Softwareupdates. Die Dokumentationsanforderungen sind im Detail in § 3 Abs. 2 und Abs. 4 der Datenschutzverordnung Schleswig-Holstein (DSVO) festgelegt, die über den Gültigkeitsbeginn der Datenschutzgrundverordnung am 25. Mai 2018 hinaus weiter gilt.

<u>Protokollierung administrativer Tätigkeiten</u>

Protokollierungsanforderungen können auf unterschiedliche Weise umgesetzt werden, etwa mit handschriftlichen oder elektronischen Aufzeichnungen (z.B. Ticketsystem) oder durch automatisierte Einträge in Datenbanken oder Log-Dateien.

Relevante Informationen sind:

a) Zeit („Wann?“),
b) Urheber bzw. Auslöser („Wer?“)
c) Aktivität/ Ereignis („Was?“)

Dabei sind nicht nur die ausgeführten Tätigkeiten (etwa: Änderung einer Berechtigung) relevant, sondern auch Informationen über die Veranlassung der Tätigkeit (Warum wurde die Berechtigung geändert? Wer hat den Auftrag erteilt?). Somit reicht eine rein technische Protokollierung der ausgeführten Tätigkeiten nicht aus, um den Nachweis zu führen. Häufig wird

die Protokollierung mit einem Ticketsystem verknüpft, das Informationen über die Veranlassung der Änderung beinhaltet.

Daneben stellt sich die Frage, welchen Bedarf an Verlässlichkeit und Integrität die Protokollinformationen haben: Eine handschriftliche Protokollierung kann unvollständig sein; eine Protokolldatei im Zugriff eines Administrators könnte durch diesen manipuliert oder gelöscht werden. Anhand des Bedarfs muss entschieden werden, welche Protokollierungsmaßnahmen erforderlich und angemessen sind. Daneben ist zu berücksichtigen, ob und wenn ja welche personenbezogenen Daten in den Protokollierungsinformationen enthalten sind. Wird beispielsweise die „Reparatur" von Datensätzen in einer Datenbank protokolliert, so sind auch Datenbankinhalte Gegenstand der Protokollinformation.

Beispiele zur Umsetzung einer Protokollierung mit erhöhten Anforderungen an Vertraulichkeit, Integrität oder Nachvollziehbarkeit sind vollautomatisierte Protokollierung, eine Speicherung ohne Zugriff der Administration (z.B. auf einem dedizierten Protokollserver) oder eine automatisierte Alarmierung bei auffälligen oder ungewöhnlichen Protokolleinträgen (etwa Log-Ins außerhalb von Dienstzeiten, Rücksetzung von Passwörtern, etc.).

Dabei sind auch Anforderungen der Mitbestimmung und das datenschutzrechtliche Zweckbindungsgebot zu beachten. Daher ist es erforderlich, alle Festlegungen in einem **Protokollierungskonzept** niederzulegen, das auch Aussagen zur Auswertung und Aufbewahrungsdauer von Protokolldaten trifft.

<u>Videoprotokollierung</u>

Nicht jede Software erlaubt es, administrative Änderungen über Protokolldateien vollständig nachzuvollziehen. Dies ist häufig der Fall, wenn für administrative Änderungen Softwareoberflächen (Graphical User Interfaces, GUI) zum Einsatz kommen. Eine Möglichkeit der Protokollierung besteht dann darin, eine **Aufzeichnung** der Bildschirmausgaben aufzunehmen. Diese enthalten nicht nur vorgenommene Änderungen in Form von Texteingaben oder Auswahl von Menüpunkten, sondern den gesamten Bildschirminhalt oder zumindest den Inhalt des Fensterns, in dem gearbeitet wird. Somit können auch Inhaltsdaten (etwa Ausgaben von Datenbankabfragen oder Datenanzeigen der Software) Bestandteil der Protokolle werden, wenn sie auf dem Bildschirm ausgegeben werden.

Eine solche Aufzeichnung kann sowohl mit Hilfe von Tools softwareseitig vorgenommen werden als auch mit Hilfe einer Videokamera, die den Bildschirminhalt filmt. Darüber hinaus kommen bei Fernwartungen Tools zum Einsatz, die ebenfalls über Aufzeichnungsmöglichkeiten verfügen. Werden Tools für eine überwachte Fernwartung eingesetzt (Fernwartung unter Aufsicht, Tasttatur- und Mauskontrolle durch die Aufsicht), so können diese Freischaltungen häufig ebenfalls protokolliert werden (wer hat wann Tastatur bzw. Maus kontrolliert; wer konnte den Bildschirminhalt sehen). Zum Einsatz kommen auch sogenannte Sprungserver, auf den sich die Wartenden anmelden und über die sie die zu wartenden System erreichen. Eine Aufzeichnung kann dann auf diesem Sprungserver erfolgen und beeinträchtigt weder das System des Wartenden noch das gewartete System; es erlaubt somit mit auch die Wartung von Systemen, die direkt keine Videoaufzeichnung zulassen (z.B. System mit Kommandozeileninterfaces).

Auf diese Weise können Wartungsvorgänge zentral protokolliert werden. Ebenso kann die Wartungstätigkeit eines Auftragsverarbeiters auf den Systemen eines Verantwortlichen protokolliert werden (gleiches gilt für Tätigkeiten eines Unterauftragnehmers, die auf Systemen eines Auftragsverarbeiters protokolliert werden).

Durch die vollständige (Video-)Protokollierung der Bildschirmausgaben entstehen Datenbestände von personenbezogenen Daten, die bei einer Protokollierung auf Kommandozeilenebene (eingegebene Kommandos) oder mit Hilfe von Logdateien häufig gar nicht oder nicht in diesem Detailierungsgrad entstanden wären. Dies ist in einigen Situation sinnvoll (etwa, um bei unbefugten Suchanfragen auch auf die Ergebnisse rückschließen zu können), führt aber in anderen Situationen zu einer überbordenen Datenspeicherung. Ebenso wird die Arbeitsweise der handelnden Personen deutlich detaillierter protokolliert, etwa das Suchen nach Menüpunkten in GUI; dies könnte zu einer Leistungs- oder Verhaltenskontrolle verwendet werden.

Dies unterstreicht, dass eine Videoprotokollierung besondere Beachtung verdient. Relevante Punkte aus Datenschutzsicht sind dabei:

- Die Tatsache der Videoprotokollierung administrativer Tätigkeiten ist allen Beteiligten bekannt zu machen und ist mitbestimmungspflichtig.
- Keine Aufzeichnung von Audiodaten oder weiterer Informationen (z. B. von Personen, die Wartungen überwachen oder den Raum betreten). Eine Videokamera, die einen Bildschirm filmt, ist daher ungeeignet.
- Abspeicherung der Bildschirmaufzeichnungen pro Wartungsauftrag bzw. Administrationstätigkeit, damit spezifische Zugriffe, Auswertungen und Löschungen erfolgen können.
- Videoprotokollierungen nur von Administrationstätigkeiten, nicht aber von regulärer Arbeit wie Erstellen/Lesen von E-Mails, Internetrecherche etc. außerhalb einer Administrationstätigkeit.
- Zuordnung der Aufzeichnungen zu Tickets oder anderer Dokumentation einzelner Administrationsaufträge (optimal so, dass aus der Aufzeichnung das bearbeitete Ticket und aus dem Ticket die Aufzeichnung ersichtlich sind).
- Möglichkeit, einzelne Aufzeichnungen als besonders schützenswert zu kennzeichnen (etwa bei besonderen Verfahren oder wenn bekannt ist, dass gespeicherte personenbezogene Daten in der Aufzeichnung enthalten sind).
- Einhaltung der Zweckbindung: Die Aufzeichnung und ihrer Auswertung erfolgen zu Zwecken der Datenschutzkontrolle, nicht als „Anleitung“ oder „Videotutorial“ zur Wartung.
- Festlegung von Aufbewahrungsfristen der Protokolle in Anhängigkeit der administrierten Verfahren, der Administrationstätigkeit und des Inhalts der Aufzeichnung (nur Wartungsbefehle oder auch Anzeige der gespeicherten Daten) sowie der Kontrolle der aufgezeichneten Tätigkeiten.
- Eine bloße Aufzeichnung ersetzt die Kontrolle der Tätigkeiten nicht.
- Zugriffsschutz für die Aufzeichnungen zur Sicherung ihrer Vertraulichkeit, Integrität und Zweckbindung. Diese dürfen daher im Tagesgeschäft nicht zugreifbar sein.

- Planung einer Eingriffsmöglichkeit in die Aufzeichnungen, falls eine Löschungsverpflichtung auch in den Aufzeichnungen durchgeführt werden muss.
- Bei der Festlegung, wie und durch wen Protokolle unter Einhaltung der Zweckbindung ausgewertet werden, sind Personalvertretungen und Datenschutzbeauftragte einzubinden. Dies ist ggf. auch bei einzelnen spezifischen Auswertungen, etwa zur Aufdeckung doloser Handlungen, zu beachten.

Zu beachten bleibt, dass eine Wartung nicht nur interaktiv, sondern auch mit Hilfe von Konfigurationsdateien, Skripten und Gruppenrichtlinien erfolgen kann. In diesem Fall sind in der Videoaufzeichnung nur das Einspielen der Konfigurationsdatei bzw. die Aktivierung von Skripten oder Gruppenrichtlinien zu beobachten, nicht aber die damit durchgeführten Administrationstätigkeiten. Daher sind diese separat zu dokumentieren.

Videoaufzeichnung mit Anleitungscharakter

Davon unabhängig können aus Wartungen oder Administrationstätigkeiten von Testsystemen oder von Systemen, die keine personenbezogene oder sonstige schützenswerte Daten enthalten, Videoaufzeichnungen mit Anleitungscharakter („Tutorial“) erstellt werden; hier würde auch eine Audioaufzeichnung (z.B. Erläuterung vorgenommener Tätigkeiten) möglich sein.

Bei Fragen oder Beratungswünschen können Sie sich gerne an uns wenden:

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)
Holstenstraße 98
24103 Kiel
Telefon: +49 (0) 431 988-1200
E-Mail: mail@datenschutzzentrum.de
https://www.datenschutzzentrum.de/