Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Berliner Beauftragte für Datenschutz und Informationsfreiheit
Friedrichstr. 219, 10969 Berlin

Berliner Verkehrsbetriebe (BVG)
Leiter Vorstandsstab Datenschutz
Herrn [redacted]
10096 Berlin

Geschäftszeichen: (bitte angeben) 54.3447.66
Abteilung: II B
Bearbeiter(in): [redacted]
Telefon: 030 13889-0
Durchwahl-Nr.: 410

Datum: 18. April 2019

Datenschutz-Folgenabschätzung zum Einsatz von Videotechnik in Fahrzeugen, Bahnhöfen, Haltestellen und Betriebsanlagen der BVG
Ihr Schreiben vom 29. Januar 2019

Datenschutzrechtliche Bewertung

Sehr geehrter [redacted]

wir danken Ihnen für die Übersendung der Datenschutz-Folgenabschätzung (DSFA) zum Einsatz von Videotechnik in den von Ihnen verantworteten o. g. Bereichen, in der Fassung vom 16. Januar 2019 (Version 2.0), die von Ihnen gemäß unserer Anmerkungen in unserem Schreiben vom 19. November 2018 nochmals überarbeitet wurde. Wir danken Ihnen insbesondere für die detaillierten Erläuterungen, mit denen Sie auf unsere Anmerkungen reagiert haben.

A. Bewertung

Wir möchten Ihnen nunmehr unsere abschließende Bewertung Ihrer Datenschutz-Folgenabschätzung mitteilen:

Die Ausführungen sind nicht ausreichend, da wesentliche Betrachtungen der Risikoidentifikation sowie Darstellung möglicher Risikoquellen in der vorgelegten DSFA, Version 2.0, fehlen. Technisch organisatorische Maßnahmen sind zu allgemein beschrieben und werden nicht in Bezug auf identifizierte Risiken gesetzt. Somit ist auch kein Rückschluss auf die wirksame Minimierung der Risiken möglich.

Zu Ihren Ausführungen teilen wir Ihnen im Einzelnen Folgendes mit:

Zu 1. Bewertung der Notwendigkeit und Verhältnismäßigkeit

Wir teilen Ihre Auffassung, dass Einsatzbereiche von Videotechnik, die in ihrer Ausprägung vergleichbar sind, zusammengefasst und vergleichbar beurteilt werden können. Wir begrüßen, dass Sie bei unterschiedlicher Ausprägung der Videotechnik eine Differenzierung zwischen den Einsatzbereichen und somit eine gesonderte Abwägung für Einzelfälle vorgenommen haben

und künftig vornehmen werden. Wir danken Ihnen zudem für die Erläuterung der Kategorisierung und der korrigierten Punktzahlvergabe zur Einordnung einzelner Bahnhöfe.

Gleichwohl halten wir daran fest, dass Faktoren wie Umfeld und Komplexität des Bahnhofs für sich genommen keine Rechtfertigung für eine Videoüberwachung nach § 20 Berliner Datenschutzgesetz (BlnDSG) darstellen. Vielmehr muss sich daraus eine Beeinträchtigung des Hausrechts oder der Aufgaben der BVG ergeben, zu deren Beseitigung die Videoüberwachung erforderlich ist.

Zudem muss eine Abwägung vorgenommen werden, bei der sich keine Anhaltspunkte ergeben, dass schutzwürdige Interessen der betroffenen Personen überwiegen. Dies ist bei dem von Ihnen angewandten Punktesystem, welches – selbst nach ihrer Berichtigung – pauschal dazu führt, dass sämtliche Bahnhöfe mit Videotechnik ausgestattet werden müssen, zumindest zweifelhaft.

Zu 2. Bewertung der Risiken und Abhilfemaßnahmen

Die Ausführungen in der vorgelegten DSFA, Version 2.0, wurden hinsichtlich der zu betrachtenden Risiken für Betroffenenrechte von Ihnen gegenüber der Fassung vom 6. September 2018 in Bezug auf angeforderte Angaben um eine ausführlichere Interessensabwägung ergänzt. Die Erforderlichkeit der Verarbeitung wird nun auf den Seiten 11 und 12 ausführlicher begründet. Zudem wurden ab Seite 42 Angaben zu Eintrittswahrscheinlichkeiten von Vertraulichkeits-, Integritätsbruch und Verlust ergänzt, allerdings nicht mit den für diesen Abschnitt erforderlichen Begründungen für die als gering erachtete Einstufung der Risiken für Betroffene.

Das Dokument beinhaltet weiterhin nicht hinreichende Betrachtungen, die im Rahmen einer DSFA für den Anwendungsfall einer über viele Standorte und Fahrzeuge verteilte Videoüberwachung mit zentraler Speicherung und Auswertungsmöglichkeit mit täglich etwa einer Million betroffener Personen notwendig sind. Die von uns angeforderten Ergänzungen in Hinblick auf Art 35 Abs. 7 lit. c und lit. d Datenschutz-Grundverordnung (DS-GVO) fehlen allerdings.

Grundsätzlich erfolgt in den aktualisierten Unterlagen eine Bewertung einiger möglicher Auswirkungen auf die Rechte und Freiheiten der Betroffenen. Diese sind jedoch in der Risikobetrachtung methodisch nur in Bezug auf die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit gegliedert und orientieren sich nicht an Risikoszenarien aus der Sicht der Betroffenen selbst.

Es erfolgt abschließend die Einschätzung eines geringen Gesamtrisikos unter der Grundannahme, dass eine beabsichtigte oder unbeabsichtigte Beeinflussung der Verarbeitung durch Dritte nur schwer möglich sei. Gerade dieses Szenario jedoch wäre als Risiko in Bezug auf die Betroffenen zu betrachten. Als Dritte sind auch Beschäftigte zu betrachten, die aus eigenem und nicht aus dienstlichem Interesse auf die Daten zugreifen.

Auf mögliche Auswirkungen der Verarbeitung auf die Betroffenen, wie beispielsweise die Vermeidung von legitimen Handlungen an videoüberwachten Orten aufgrund des Vorhandenseins der Videoüberwachung, wird nicht eingegangen. Auch eine denkbare, wenn auch aktuell nicht beabsichtigte Ausweitung des Einsatzzwecks als mögliches Risikoszenario, wird nicht betrachtet. Hieraus entstehende Rückwirkungen auf Betroffene und etwaige Schadensszenarien wurden nicht betrachtet.

Betroffenenrechte werden punktuell in einem Kapitel zu Interessenabwägung ab S. 18 ff behandelt. Darin genannte mitigierende Maßnahmen, wie beispielsweise eine Verpixelung von öffentlichem Straßenland oder Privathäusern, werden nicht in Bezug zu dem für die Umsetzung dieser Mitigationsmaßnahme ursächlichen Risiko gesetzt.

a) Anmerkungen zu den im Dokument betrachtenden Risiken für Betroffene

Insbesondere in Hinblick auf das Schutzziel Vertraulichkeit ist die Granulierung der betrachteten Risiken hinsichtlich der denkbaren Schadensszenarien zu grob. In der Interessenabwägung werden auf Seite 18 „Rückschlüsse auf äußere Merkmale" sowie „Ort und Zeit" des Aufenthaltsorts der Betroffenen der über Standorte und Fahrzeuge verteilten Infrastruktur hinweg als Szenario skizziert. Diese finden sich allerdings in der Risikobetrachtung nicht wieder. Risiken aus der Erkennbarkeit von legitimen Handlungen der Betroffenen sind in diesem Kontext nicht mitbetrachtet worden.

Eine Zweckentfremdung regulärer Zugriffe, beispielsweise durch interne Mitarbeiter, wird in der Risikoabwägung nicht mitbetrachtet, obwohl für das Risiko einer Beobachtung von Kollegen als mitigierende Maßnahme eine Betriebsvereinbarung (Zentrale Dienstvereinbarung – ZDV) genannt wird.

Für den im Dokument beschriebenen Ausnahmefall eines außerplanmäßigen Aufschaltens auf bestimmte Kameras aus der Leitstelle ist eine Benachrichtigung per E-Mail an den Gesamtpersonalrat sowie den Datenschutzbeauftragten vorgesehen. Es fehlt ein Hinweis auf eine lückenlose Dokumentation des für Aufschaltungen oder Aufnahmen initiierenden Ereignisses. Ein automatisiertes Verfahren, das ggf. auch Begründungen speichert, ist diesem Vorgehen per E-Mail Benachrichtigung vorzuziehen. Dies wäre gleichsam einer Datenschutzkontrolle zugänglich und nicht technisch an E-Mail-Kommunikation gebunden und damit auch zugleich revisionssicher mit einer Zugriffskontrolle und der automatisierbaren Berücksichtigung der Löschfristen für Protokolle nach § 62 Abs. 4 BlnDSG auszustatten.

Auf Seite 19 wird in Abschnitt 5 der Interessensabwägung ein Einsichtsrecht für betroffene Beschäftigte beschrieben. Den internen Mitarbeitern werden demnach offenbar mehr Möglichkeiten zur Schaffung von Transparenz zugestanden, als externen Betroffenen. In möglichen Auseinandersetzungen werden so asymmetrische Bedingungen gegenüber externen Betroffenen geschaffen. Eine Berücksichtigung dieser Situation als Risiko für die Gruppe der externen Betroffenen erfolgt nicht.

b) Anmerkungen zu den Maßnahmen zum Schutz der Betroffenen

Es fehlen technische Konkretisierungen der vorgesehenen Maßnahmen zur Garantie der Vertraulichkeit, insbesondere bei der Absicherung der Transportwege, beispielsweise durch Verschlüsslung der Signale von der Kamera hin zu Monitoren im Fahrzeug bzw. zur Leitstelle sowie zum Aufzeichnungsserver. Auf Seite 43 wird der Übertragungsweg als „über ein BVG-eigenes Netzwerk" beschrieben, wobei etwaige Schutzmaßnahmen, wie beispielsweise die physische Absicherung der Leitungen sowie Verschlüsselung ungenannt bleiben. Besonders kritisch wären mobile Übertragungswege über Funkschnittstellen von erwähnten Fahrzeugen aus, die generell zu verschlüsseln sind.

Auf Seite 18 wird im Sinne der Wahrung der Vertraulichkeit eine Verpixelung von nicht dem Zweck nach zu betrachtenden Bereichen des Aufnahmewinkels erwähnt. Zur Realisierung wird nicht weiter ausgeführt, ob dies nur bei der Anzeige der Abbildung an den Monitoren der Leitwarte geschieht oder vor der Aufzeichnung in den „Ringspeicher" in den Fahrzeugen und den zentralen Servern.

Die Beschreibung der Absicherung des Zugriffs auf die gesicherten Daten beschränkt sich auf den Hinweis des Einsatzes eines verschlüsselten Dateisystems (auf den Seiten 4 und 14), eines Identitätsmanagements via ActiveDirectory sowie die allgemeine Aussage, es existiere ein „Zugriffsschutz via Passwort", wobei nicht dargelegt wird, ob sich dies auf den Systemzugang,

den Zugriff auf die Daten in der Betrachtungsanwendung oder die Verschlüsselung bezieht. Diese Maßnahmen werden in Hinblick auf die Realisierung nicht weiter beschrieben. Der Verweis auf ein entsprechendes Infrastruktur-Sicherheitskonzept fehlt, dies wäre aber an diesen Stellen zur weiteren Analyse erforderlich.

In den Betrachtungen zur Datenintegrität auf Seite 42 wird nicht auf technische Garantien hinsichtlich des Integritätsschutzes der im Einsatz befindlichen Hardware eigegangen. Hinsichtlich des Verfügbarkeits- und Integritätsschutzes wird in der Auflistung technisch-organisatorischer Maßnahmen auf Seite 13 die Maßnahmen „Verschlüsselung/Codierung", „Datensicherung" sowie „Einsatz eines abgeschotteten Systems" genannt. Entsprechende Konzepte, wie beispielsweise ein Sicherungs- und Wiederherstellungskonzept oder ein Verschlüsselungskonzept wären hierfür erforderlich oder müssten im Rahmen des Infrastruktur-Sicherheitskonzepts mit abgebildet sein. Da dies auch Auswirkungen auf die Vertraulichkeit haben könnte, wäre dies als Risikokategorie mit zu betrachten. Auf diese Konzeptionen sowie Test und Audits sollte in diesen Abschnitten verwiesen werden. Ein technisches IT-Sicherheitskonzept liegt in der Einreichung nicht mit vor.

Ein Rollen- und Berechtigungskonzept zur Einschränkung der Zugriffe wird im Dokument mehrfach genannt. Es finden sich Hinweise auf eine Trennung von Nutzer- und Administratorrechten sowie einer gesonderten Berechtigung für einen Polizeiarbeitsplatz in der Leitstelle. Das eigentliche Dokument wurde nicht vorgelegt.

Ein auf Seite 28 erwähntes Löschkonzept liegt ebenfalls nicht vor. Insbesondere fehlen Details zur Realisierung des erwähnten Ringspeichersystems, mit dem eine Speicherfrist von 48 Stunden sichergestellt wird. Lediglich der Sonderfall einer nachträglichen Löschung bei stromlosen Fahrzeugen bei erneutem Fahrtantritt wird auf Seite 6 konkretisiert.

Auf Seite 13 wird als technisch organisatorische Maßnahme zur Wahrung der Transparenz die „Protokollierung" genannt, hinsichtlich der Auswertbarkeit relativiert auf „Zum größten Teil wird nicht protokolliert, welcher Mitarbeiter den Vorgang ausgeführt hat." mit der Folge: „Nur mit viel Aufwand kann abgeleitet werden, wer was wann getan hat."

Die Konzeption zur sicheren Übermittlung von aus dem System exportieren Aufnahmen an Behörden wird auf den Seiten 44 und 45 erwähnt, liegt aber im Detail nicht vor.

Hinsichtlich der Transparenz für Betroffene fehlt die Angabe des nach Art. 13 DS-GVO geforderten Zwecks. Dieser fehlt in der Hausordnung in § 5 der an die Fahrgäste gerichteten öffentlich verfügbaren Information zur Videoüberwachung. Eine in der Situation erkennbare Markierung der betroffenen Bereichsgrenzen wäre zur Wahrung der Betroffenenrechte in Hinblick auf Transparenz nützlich.

B. Hinweise und Empfehlungen

Da die Datenschutz-Folgenabschätzung laufend überarbeitet und an neue Entwicklungen angepasst werden muss, möchten wir Ihnen für die folgenden Überarbeitungen abschließend folgende Hinweise und Empfehlungen geben:

Im Prozess der Erstellung einer Datenschutz-Folgenabschätzung hilft das Kurzpapier Nr. 5 mit dem Titel „Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO" weiter, dass Sie auf unserer Internetseite unter: https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/kurzpapiere/ finden.

Wir weisen darauf hin, dass bei der Erstellung der Datenschutz-Folgenabschätzung eine Einbeziehung von unabhängigen Interessenvertretern erfolgen sollte. Denkbar wäre z. B. die Einbin-

dung eines Fahrgastverbands, der internen und externen Mitarbeiter, der im überwachten Bereich aktiven Dienstleister oder Unternehmer sowie Vertreter von Sicherheitsorganen.

Viele dieser Betroffenengruppen müssen zur Erfüllung ihrer Aufgaben die überwachten Bereiche passieren und haben keine Handlungsoption, der Überwachungsmaßnahme auszuweichen.

Eine Betrachtung aus Sicht der jeweiligen Betroffenengruppen führt ggf. zu einer differenzierteren Sicht auf mögliche Risiko- und Schadensszenarien. Diese noch zu identifizierenden Risiken sind in Hinblick auf ihre Eintrittswahrscheinlichkeit und mögliche Schadenhöhen zu beurteilen (folgend aus dem Erwägungsgrund 75 ff. zur DS-GVO).

Bei der Beurteilung der Risiken kann das Kurzpapier Nr. 18 mit dem Titel „Risiko für die Rechte und Freiheiten natürlicher Personen" weiterhelfen, dass ebenfalls unter dem o. g. Link auf unserer Internetseite abrufbar ist.

Bei der Risikoidentifikation ist aus der Perspektive der Betroffenen auszugehen, für die zu identifizieren ist, zu welchen Schäden es für natürliche Personen auf Grundlage der Datenverarbeitung kommen kann. Hierbei sind Handlungen und Ereignisse Initiatoren für Schadenereignisse, die physischer, materieller oder immaterieller Natur sein können. Betroffene sind Mitarbeiter, Fahrgäste, Dienstleister sowie weitere Personenkreise, die sich in den betroffenen Bereichen aufhalten, oder sogar zur Erfüllung ihrer Aufgaben aufhalten müssen.

Negative Folgen von Abweichungen der geplanten Verarbeitung sind mit zu betrachten. So ist auch ein nicht sachgemäßer Umgang mit den Daten in einem der Verarbeitungsschritte für Bertoffene ein Risiko. Es ist dabei unerheblich, ob es sich dabei um eine beabsichtigte oder unbeabsichtigte Beeinflussung der Verarbeitung handelt.

Das Hinwegsetzen von Mitarbeitern über eine Anordnung oder Dienstvereinbarung getroffene Regelung ist demnach ein relevantes Risikoszenario.

In der Phase der Risikoidentifikation ist die Höhe des Aufwands und des eigenen Risikos, die ein Akteur bereit ist aufzubringen, unerheblich. Das identifizierte Risiko als solches ist trotzdem zu dokumentieren, um es in der Beurteilung aller gefundenen Risiken und ihren Abhilfemaßnahmen berücksichtigen zu können. Erst im Anschluss werden die Eintrittswahrscheinlichkeit und die Schadenhöhe bewertet.

Abhilfemaßnahmen zur Risikominderung, wie die realisierten technisch organisatorischen Maßnahmen, sind dann in Bezug auf die identifizierten Risiken detailliert innerhalb des Dokuments abzubilden. Relevante Dokumente, auf die verwiesen wird, sind mit einzureichen.

Bei der Umsetzung von Abhilfemaßnahmen ist auf eine Testabdeckung hinsichtlich ihrer Wirksamkeit zur Minderung der identifizierten Risiken zu achten, um hierüber einen schlüssigen Nachweis erbringen zu können.

Verbleibende Restrisiken sind zu ermitteln und zu dokumentieren. Falls ein Risiko als nicht relevant erachtet wird, ist dies zu begründen.

Folgende Fragen können Ihnen gegebenenfalls bei weiteren Überarbeitungen hilfreich sein:

1. Fragen zu den Risiken

   a) Wie wird dem Risiko einer beabsichtigten oder unbeabsichtigten Erweiterung des ursprünglich vorgesehenen Verarbeitungszwecks begegnet?

b) Welche Gruppen Dritter würden unter welchen Motivationen Interesse an der Verletzung der Vertraulichkeit, der Integrität oder Verfügbarkeit der Überwachungsmaßnahme haben und welche Risiken ergeben sich für die Betroffenen hieraus?

c) Ein unbefugter Zugriff auf die Systeme sowohl von einem potentiellen Innentäter als auch von außen ist ein als relevant zu betrachtendes Risikoszenario. Welche Risiken ergeben sich aus dieser Grundannahme und wie wird eine wirksame Minderung dieser Risiken durch die realisierten Maßnahmen erreicht?

2. Fragen zu den technisch-organisatorischen Maßnahmen

a) Welche Maßnahmen sind zur Absicherung der Transportwege von den Kameras zu den Monitoren in Fahrzeugen, der Leitwarte sowie den Aufzeichnungsservern etabliert worden?

b) Wie wird die Kontrolle der Zweckbindung und ordnungsgemäßen Verarbeitung wahrgenommen, wenn dies nicht wirksam realisiert werden kann, wie auf Seite 13 angegeben: „Nur mit viel Aufwand kann abgeleitet werden, wer was wann getan hat."?

c) Wie ist die Isolation der Systemumgebung für die zentralen Aufzeichnungssysteme sowie den Datenleitungen für Videoaufnahmen von den restlichen IT-Infrastrukturen und innerhalb der Rechenzentrums- und Applikationslandschaften realisiert?

C. Weiteres Verfahren

Wir betrachten die Angelegenheit – soweit die Prüfung der Datenschutz-Folgenabschätzung betroffen ist – als abgeschlossen.

Wir behalten uns aber vor, einzelne Bereiche, die wir anhand der uns vorliegenden Version der Datenschutz-Folgenabschätzung als problematisch identifiziert haben, sukzessive aufsichtsrechtlichen Prüfungen zu unterziehen. Diese Bereiche betreffen insbesondere:

- Prüfung der Notwendigkeit und Verhältnismäßigkeit der Videoüberwachung an einzelnen Bahnhöfen (Art. 35 Abs. 7 b DS-GVO, § 20 BlnDSG)

- Prüfung der technischen und organisatorischen Maßnahmen zur Minimierung der Risiken für Betroffene im Hinblick auf:

    - die Absicherung der Übertragungswege von den Kameras zu den Monitoren und Aufzeichnungsservern
    - das Rollen- und Berechtigungskonzept mit technischen und organisatorischen Maßnahmen, inklusive der Abgrenzung von Administrations- und Nutzerberechtigungen

Sie erhalten von uns diesbezüglich separate Anschreiben.

Mit freundlichen Grüßen

[redacted]