

# **Datenschutz-Folgenabschätzung für das Projekt KFMS 2.0**

**1. November 2023**

## Inhaltsverzeichnis

<b>1.</b>	<b>Einleitung</b>	<b>3</b>
<b>2.</b>	<b>Angaben zum Projekt</b>	<b>3</b>
<b>2.1.</b>	<b>Projektbeschreibung</b>	<b>3</b>
<b>2.2.</b>	<b>Am Projekt Beteiligte</b>	<b>4</b>
<b>2.3.</b>	<b>Beschreibung der im Projekt verwendeten Systeme</b>	<b>5</b>
<b>2.4.</b>	<b>Nutzung der Daten</b>	<b>5</b>
2.4.1.	Verwendete Daten	5
2.4.2.	Datenverknüpfungen	6
2.4.3.	Weitergabe von Daten	6
<b>2.5.</b>	<b>Betroffene Personengruppen</b>	<b>7</b>
<b>3.</b>	<b>Datensparsamkeit</b>	<b>7</b>
<b>4.</b>	<b>Risikoidentifikation und -bewertung</b>	<b>7</b>
<b>4.1.</b>	<b>Vorbemerkung</b>	<b>7</b>
<b>4.2.</b>	<b>Vertraulichkeit der Daten im Projekt</b>	<b>9</b>
4.2.1.	Auslösende Elemente (Szenarien)	9
4.2.2.	Mögliche negative Folgen	9
4.2.3.	Wahrscheinlichkeit	9
<b>4.3.</b>	<b>Verfügbarkeit der Daten im Projekt</b>	<b>9</b>
4.3.1.	Auslösende Elemente (Szenarien)	9
4.3.2.	Mögliche negative Folgen	10
4.3.3.	Wahrscheinlichkeit	10
<b>4.4.</b>	<b>Transparenz der Datenbearbeitung</b>	<b>10</b>
4.4.1.	Auslösende Elemente (Szenarien)	10
4.4.2.	Mögliche negative Folgen	11
4.4.3.	Wahrscheinlichkeit	11
<b>4.5.</b>	<b>Integrität und Richtigkeit der Daten</b>	<b>11</b>
<b>4.6.</b>	<b>Zweckbindung der Daten</b>	<b>11</b>
4.6.1.	Auslösende Elemente (Szenarien)	12
4.6.2.	Mögliche negative Folgen	12
4.6.3.	Wahrscheinlichkeit	12
<b>4.7.</b>	<b>Sicherstellung der Betroffenenrechte</b>	<b>12</b>
4.7.1.	Auslösende Elemente (Szenarien)	12
4.7.2.	Mögliche negative Folgen	13
4.7.3.	Wahrscheinlichkeit	13
<b>4.8.</b>	<b>Ergebnis der Risikoanalyse</b>	<b>13</b>

---

# Datenschutz-Folgenabschätzung für das Projekt KFMS 2.0

## 1. Einleitung

Die Schweizerische Bundesbahnen AG («SBB») hat für eine sichere, bequeme und effiziente Nutzung der Bahnhöfe zu sorgen: Sie muss die Sicherheit gewährleisten, die Reinigungspläne optimieren, Engpässe bei Durchgängen identifizieren, die Personenflüsse richtig lenken und dafür sorgen, dass das richtige Angebot am richtigen Ort ist, zum Beispiel Billettautomaten oder Lebensmittelläden.

Um dieser Aufgabe nachzukommen, werden aggregierte (statistische) Informationen zum Belegungsgrad sowie zu den Personenflüssen innerhalb der Bahnhöfe benötigt. Die SBB will mit dem Projekt «KFMS 2.0» (Kundenfrequenzmesssystem 2.0) sicherstellen, dass die erforderlichen, anonymen Frequenzdaten im Modell Data-as-a-Service erhoben werden können.

Gleichzeitig ist es der SBB ein wichtiges Anliegen, stets im besten Interesse ihrer Kundinnen und Kunden zu handeln und dabei deren Rechte zu wahren. Die SBB hat deshalb die Ausschreibung des KFMS 2.0 so konzipiert, dass von Bahnhofsbesucher:innen keine personenbezogenen Daten erfasst werden können. Den Anbietern war vorgegeben, dass eine Identifizierung der Bahnhofsbesucher:innen auszuschliessen ist. Die Einhaltung dieser Vorgabe wurde bei der Auswertung der Angebote verifiziert.

Da mit KFMS 2.0 keine Personendaten erfasst werden, besteht auch kein Risiko einer Datenschutzverletzung. Dennoch hat die SBB entschieden, die vorliegende Datenschutz-Folgenabschätzung («DSFA») durchzuführen. Zunächst soll die Einhaltung der Vorgabe gemäss Ausschreibung (kein Personenbezug) dargelegt werden. Sodann soll die vorliegende DSFA aufzeigen, wie die SBB über den Datenschutz hinausgehend ihre Verantwortung im Umgang mit Daten wahrnimmt, z.B. indem sie die Datenverwendung auf den Verwendungszweck gemäss Projektziel beschränkt oder einem denkbaren (obwohl im konkreten Fall unbegründeten) "Überwachungsgefühl" einzelner Bahnhofsbesucher:innen mit gezielten Informationsmassnahmen entgegenwirkt.

## 2. Angaben zum Projekt

### 2.1. Projektbeschreibung

[Hier ist das Projekt zu beschreiben und darzulegen, welche Interessen damit verfolgt werden.](#)

Wie in der Einleitung erwähnt, hat die SBB für eine sichere, komfortable und effiziente Nutzung der Bahnhöfe zu sorgen. Dafür sind aggregierte Informationen über den Belegungsgrad und die Personenflüsse innerhalb der Bahnhöfe unerlässlich.

Das Projekt KFMS 2.0 zielt darauf ab, der SBB die Messung von Frequenzdaten und daraus abgeleiteten Kennzahlen, wie z.B. Personenflüsse und Belegungsgrade, zu ermöglichen. Für bestimmte, stark frequentierte Flächen ist zudem vorgesehen, dass Auswertungen und Erkenntnisse zur Flächennutzung generiert werden können. Dies könnte beispielsweise die statistische durchschnittliche Aufenthaltsdauer von Bahnhofsbesucher:innen oder die Erkennung von Engpässen beinhalten.

KFMS 2.0 knüpft funktional an das bestehende Kundenfrequenzmesssystem an, das in gewissen Bahnhöfen seit Jahren im Einsatz ist, das Ende des Lebenszyklus erreicht hat und neu ausgeschrieben werden muss. Mit KFMS 2.0 werden zusätzlich durchschnittliche Aufenthaltsdauern, Personendichten und typische Laufwege für stark frequentierte Flächen gemessen. Somit kann die sichere und bequeme Nutzung dieser Flächen optimiert werden.

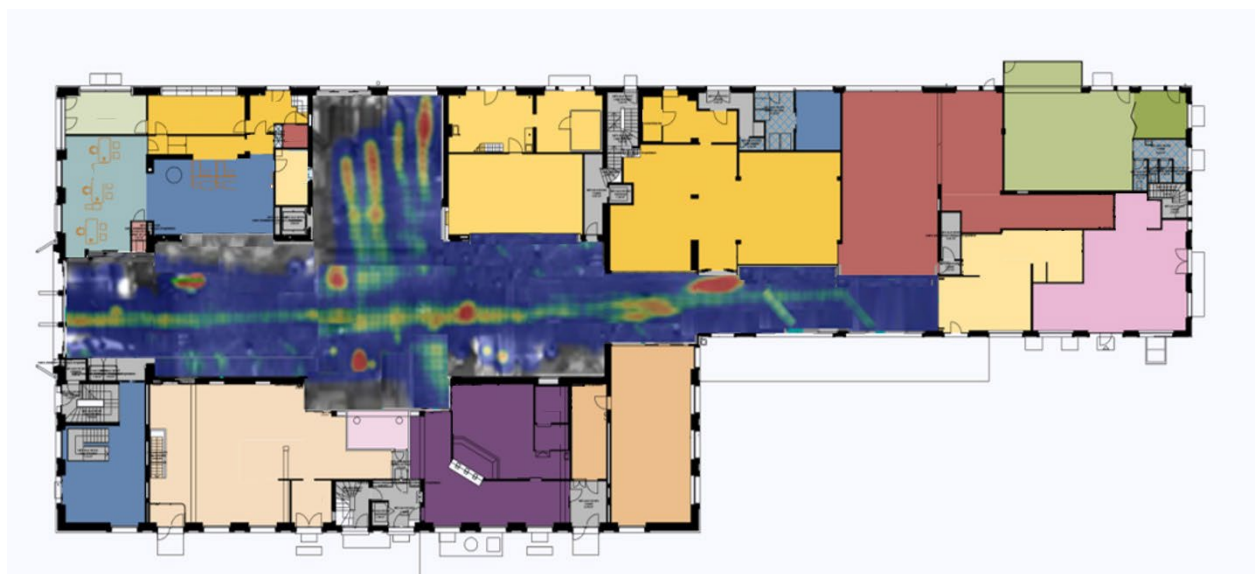


Abbildung 1: Beispiel der durchschnittlichen Personendichte innerhalb einer stark frequentierten Fläche

## 2.2. Am Projekt Beteiligte

[Hier ist aufzuführen, wem das Projekt gehört und an der DSFA beteiligt ist.](#)

Am vorliegenden Projekt sind folgende Personen bzw. Stellen involviert:

- Verantwortliche: SBB AG
- Businessseinheit SBB AG: Immobilienbewirtschaftung (IM-BW-BDM)
- Beteiligte Businessseinheiten: SBB IT (DSO-IMS), Finanzen (IM-F-CSC), Beschaffung (DSRV-STs), Rechtsdienst (RC-T)
- Dienstleister: "der Anbieter"<sup>1</sup>
- Datenschutzberater: Fachstelle Datenschutz (RC-T)

---

<sup>1</sup> Zur Sicherstellung der Vertraulichkeit wird der Name des Anbieters in diesem Dokument nicht erwähnt.

## 2.3. Beschreibung der im Projekt verwendeten Systeme

[Hier sind die vom Projekt verwendeten Systeme zu beschreiben.](#)

Das vom Anbieter angebotene KFMS 2.0 arbeitet mit optischen 3D-Sensoren, die an Decken in den relevanten Bereichen angebracht werden. Anhand veränderter Höhenprofile in ihrem Messbereich (vgl. 2.4.1 «Messdaten») schliessen diese Sensoren in Echtzeit auf Personenbewegungen (vgl. 2.4.1 «Ereignisdaten»), die in ihren Messbereichen stattfinden. Die Ereignisse (Personenbewegungen) werden zu Frequenzzahlen (blosse Zählraten) summiert. Die weitere Verarbeitung und Auswertung erfolgt in einer zentralen Infrastruktur. Dies bedeutet, dass sämtliche Personenbewegungen anonym gemessen und ausschliesslich aggregiert ausgewertet werden. Eine personenbezogene Bearbeitung findet somit zu keinem Zeitpunkt statt.

Die zur Detektion von Bewegungen vorgesehene 3D-Sensortechnologie ist seit vielen Jahren für die Messung von Frequenzzahlen an verschiedenen Bahnhöfen der SBB im Einsatz. Durch die zentrale Verarbeitung der Frequenzdaten wird die lokal benötigte Infrastruktur minimal gehalten. Die beschriebene Konfiguration und Wartung der Sensoren erfolgen auf der zentralen Infrastruktur des Anbieters. Die Serverinfrastruktur ist durch eine mehrschichtige Firewall vor unbefugtem Zugriff geschützt. Jeder Sensor sendet Daten direkt an die zentrale Infrastruktur des Anbieters. Diese Datenübermittlung zwischen Sensoren und der zentralen Infrastruktur erfolgt über eine verschlüsselte SSL/TLS-Verbindung. Hierbei kommen modernste Authentifizierungsverfahren und Security Tokens zum Einsatz. Zudem wird der Zugriff auf die Daten mittels umfangreicher Zugriffskontrolle eingegrenzt. Zugang zu den Daten haben nur Benutzer, die die nötigen Rollen und Berechtigungen besitzen. Diese Zugriffsregeln werden regelmässig kontrolliert und angepasst, um sicherzustellen, dass ausschliesslich autorisierte Benutzer Zugriff haben.

## 2.4. Nutzung der Daten

[Hier ist zu beschreiben, welche Daten wie bearbeitet werden.](#)

### 2.4.1. Verwendete Daten

Das Projekt unterscheidet folgende Datenarten: Messdaten, Ereignisdaten, Frequenzdaten und Kenngrössen.

**Messdaten:** Aus der Vogelperspektive werden Messdaten aus der Veränderung des Höhenprofils des Messbereichs generiert. Die Messdaten werden nicht gespeichert.

**Ereignisdaten:** Die aus den Messdaten (Veränderung des Höhenprofils) abgeleiteten Ereignisdaten stellen die kleinste Einheit von gespeicherten Daten dar. Es handelt sich dabei um aus den Messdaten berechnete, anonyme Personenbewegungen: Aus der Veränderung des Höhenprofils im Messbereich wird das Ereignis abgeleitet, dass eine Personenbewegung auf der Zähllinie stattfindet. Dieses Zähldatum ist die einzige Angabe, die ein:e Bahnhofsbesucher:in im KFMS 2.0 hinterlässt. Die Ereignisdaten

(Zähl­daten) werden je nach Bedarf entweder von ausgewählten Sensoren an die zentrale Infrastruktur zur weiteren Verarbeitung verschlüsselt übertragen. Dort werden sie spätestens nach 4 Wochen gelöscht. Oder die Ereignis­daten werden in den Sensoren in regelmässigen Intervallen (z.B. minütlich) zu Frequenz­daten (s. nachfolgend) aggregiert (Summe aller Ereignisse innert 60 Sekunden) und dann an die zentrale Infrastruktur übertragen.

**Frequenz­daten** widerspiegeln die Anzahl der Bahnhofsbesucher:innen, welche innerhalb eines bestimmten Zeitfensters eine Fläche betreten und wieder verlassen oder Linien (Querschnitte) durchqueren. Die Frequenz­zahlen ergeben sich aus der Summe von Ereignissen innerhalb eines bestimmten Zeitfensters und werden regelmässig an die zentrale Infrastruktur übermittelt. Es handelt sich um eine Aggregation nicht personenbezogener Ereignis­daten.

**Kenngrossen** beziehen sich auf Messobjekte als Ganzes (z.B. eine stark frequentierte Fläche in einem Bahnhof). Sie stellen entweder einen Zustand zu einem bestimmten Zeitpunkt (z.B. Personendichte um 12.00 Uhr) oder statistische Werte in einem bestimmten Messintervall dar (z.B. durchschnittliche Aufenthaltsdauer zwischen 17:00 und 19:00 Uhr), beziehen sich jedoch nie auf einzelne Personen.

**Wichtig:** Wie vorstehend beschrieben sind die Ereignis­daten aus anonymen Höhenprofilveränderungen abgeleitete Personenbewegungen. Die daraus summierten Frequenz­daten und Kenngrossen sind eine Aggregation anonymer Ereignis­daten. Aus diesen Daten einen Personenbezug herzustellen, ist nicht möglich. Im Übrigen ist selbst eine Singularisierung<sup>2</sup> ausgeschlossen, da die Veränderungen in den Höhenprofilen nicht einmal einzelnen (nicht bestimm­baren) Personen zugeordnet werden können. Frequenz­daten und Kenngrossen liegen zudem ausschliesslich in aggregierter Form vor.

#### 2.4.2. Datenverknüpfungen

Statistische Zusammenhänge zwischen Frequenz­daten und Daten aus anderen Quellen (z.B. Wetterdaten) können helfen, die eingangs erwähnten Ziele zu erreichen (z.B. Bahnhofs­nutzung in Abhängigkeit zum Wetter und daraus abgeleitet Tourenpläne oder der Gesamtumsatz am Bahnhof in Relation zur Bahnhoffrequenz).

Hierbei werden stets nur aggregierte Zahlen verwendet. Es werden keine individualisierten Daten, geschweige denn personenbezogene Daten verknüpft.

#### 2.4.3. Weitergabe von Daten

Die Daten werden SBB-intern verwendet. Es werden aggregierte, schematische Daten (Frequenz­zahlen, Kenngrossen) auf der Webseite der SBB publiziert und bei

---

<sup>2</sup> Unter Singularisierung versteht man das Phänomen, dass ein Datensatz so speziell ist, dass er sich nur auf eine individuelle Person beziehen kann, die aber nicht bekannt oder identifizierbar ist.

nachgewiesenem Interesse an öffentliche Institutionen oder Vertragspartner (z.B. Planungsbüro für Dimensionierung der Publikumsfläche) weitergegeben.

## **2.5. Betroffene Personengruppen**

Hier ist zu beschreiben, welche Personengruppen von der Datenbearbeitung betroffen sind.

“Betroffen” vom Betrieb des KFMS 2.0 sind Personen, die sich im Bahnhof (oder genauer in bestimmten Flächen) bewegen oder aufhalten. Allerdings lassen sich die Personen nicht identifizieren und die Daten werden stets anonym gemessen. Eine Bearbeitung von Personendaten kann nicht stattfinden.

Auch findet keine Segmentierung der Bahnhofsbesucher:innen (bspw. nach Alter, Geschlecht oder ähnlichem) statt; das wäre auf Basis der Ereignisdaten (reine Zähldaten) auch gar nicht möglich.

## **3. Datensparsamkeit**

An dieser Stelle ist zu prüfen, ob das Projekt "datensparsam" ist. Es geht um die datenschutzrechtliche Anforderung, Datenbearbeitungen auf das dem Zweck angemessene, erhebliche und notwendige Mass zu beschränken. "Daten" meint für den datenschutzrechtlichen Grundsatz der Datensparsamkeit dabei immer "Personendaten".

Es werden keine Personendaten erhoben, weshalb die datenschutzrechtliche Anforderung, Datenbearbeitungen auf das dem Zweck angemessene, erhebliche und notwendige Mass zu beschränken, keine Anwendung findet.

Wie unter den vorstehenden Ausführungen unter Ziff. 2.4 «Nutzung der Daten» dargelegt wird, verwendet die SBB aber selbst die nicht-personenbezogenen Daten “sparsam”. Dort wird im Einzelnen beschrieben, dass die verwendeten 3D-Sensoren die Messdaten in Echtzeit bearbeiten und nur die relevanten anonymen Zähldaten weiterleiten. Messdaten werden nicht gespeichert und systembedingt werden keine Personendaten erfasst.

Im Ergebnis kann festgehalten werden, dass das KFMS 2.0 den Grundsatz der Datensparsamkeit erfüllt. Zunächst, weil überhaupt keine personenbezogenen Daten erhoben werden. Über dies hinaus geht das KFMS 2.0 aber auch mit den nicht personenbezogenen Daten sparsam um.

## **4. Risikoidentifikation und -bewertung**

### **4.1. Vorbemerkung**

Nachfolgend erfolgt das Kernstück der DSFA. Es werden allfällige Risiken, die sich für die Betroffenen aus dem Projekt ergeben könnten, geprüft. Die Prüfung berücksichtigt die wichtigsten Anliegen des Datenschutzes. Ganz generell lässt sich zum üblichen Vorgehen in einer DSFA folgendes festhalten:

Es geht darum, allfällige Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Personen zu beschreiben. Nicht untersucht werden Rechts- oder Reputationsrisiken.

Betrachtet werden dabei (a) auslösende Elemente, d.h. Ereignisse, die den Eintritt eines Schadens auslösen könnten («was kann schiefgehen»), (b) welche negativen Folgen für die Betroffenen dabei eintreten könnten und (c) mit welcher Wahrscheinlichkeit diese eintreten würden.

#### a) Auslösende Elemente

Die Prüfung erfolgt entlang den wichtigsten Schutzziele des Datenschutzes, weil diese die Aufgabe haben, negative Folgen möglichst zu verhindern:

- Vertraulichkeit der Daten
- Verfügbarkeit der Daten
- Transparenz der Bearbeitung
- Integrität und Richtigkeit der Daten
- Zweckbindung der Daten
- Sicherstellung der Betroffenenrechte

#### b) Negative Folgen

Anschliessend wird untersucht, ob bzw. welche negativen Folgen sich für eine betroffene Person ergeben könnten, wenn eines der Schutzziele beeinträchtigt werden sollte.

Beispiele solcher Folgen können im Grundsatz – ohne der folgenden Prüfung vorgreifen zu wollen – sein: negative Gefühle, z.B. Scham, Stress, Angst, Überwachungsgefühle oder -druck.

Wie gravierend solche Folgen wären, ist eine weitere Frage, die im Anschluss ebenfalls zu berücksichtigen wäre. Es sind hier vier Schweregrade zu unterscheiden:

1 – geringfügig: Unannehmlichkeiten, mit denen die Betroffenen aber umgehen können.

2 – überschaubar: Starke Unannehmlichkeiten, mit denen die Betroffenen mit einiger Anstrengung umgehen können.

3 – substantiell: Signifikante Unannehmlichkeiten, mit denen Betroffene nur mit ernsthaften Schwierigkeiten umgehen können.

4 – gross: Signifikante oder sogar finale Unannehmlichkeiten, mit denen Betroffene nicht umgehen können.

#### c) Wahrscheinlichkeit

Unterschieden werden vier Wahrscheinlichkeitsstufen:

1 – sehr tief: Die negativen Folgen können nach derzeitigem Stand kaum eintreten.

2 – tief: Die negativen Folgen können zwar eintreten, aber dies scheint sehr unwahrscheinlich.

3 – mittel: Die negativen Folgen sind möglich, aber nicht allzu wahrscheinlich.

4 – hoch: Die negativen Folgen sind sehr wahrscheinlich.

Diesem Prüfschema folgt die SBB vorliegend mit Anpassungen, weil im vorliegenden Projekt keine Personendaten bearbeitet werden.



## 4.2. Vertraulichkeit der Daten im Projekt

Hier werden die Risiken geprüft, die sich aus einer Verletzung der Vertraulichkeit der Daten für die betroffenen Personen ergeben können, d.h. aus einer Bekanntgabe von Daten bzw. einem Zugriff auf Daten durch unbefugte Personen.

### 4.2.1. Auslösende Elemente (Szenarien)

#### a) Szenario: Daten gelangen an unbefugte externe Personen

Zunächst ist daran zu erinnern, dass keine Personendaten erhoben werden, weshalb solche auch nicht weitergeben werden können.

Das Potenzial, dass Daten nicht autorisierten externen Personen zugänglich wären, ist nahezu eliminiert. Das Rechenzentrum des Anbieters ist sicherheitstechnisch «state of the art» (z.B. mehrstufige Firewall-Infrastruktur) und alle übertragenen Daten sind verschlüsselt.

#### b) Szenario: Unbefugte interne Zugriffe

Der Anbieter regelt die Zugriffe seiner Mitarbeitenden durch ein Zugriffskonzept. Ausserdem gelten Weisungen und vertragliche Vereinbarungen, welche die Vertraulichkeit sicherstellen. Aber auch hier gilt: Personenbezogene Daten werden gar nicht erst erfasst, weshalb ein unbefugter Zugriff auf Personendaten auch nicht möglich ist.

### 4.2.2. Mögliche negative Folgen

Träte ein solches Szenario ein, wären die Folgen für die betroffene Person geringfügig. Die eingesetzten Sensoren nutzen ausschliesslich Veränderungen der Höhenprofile aus der Vogelperspektive (Messdaten), welche nicht gespeichert werden. Gespeichert werden einzig Zählraten. Es ist kein realistisches Szenario ersichtlich, in dem einzelne Personen identifiziert werden könnten, und auch andere negative Auswirkungen auf die betroffenen Personen im Fall einer Verletzung der Vertraulichkeit der entsprechenden Daten sind nicht erkennbar.

### 4.2.3. Wahrscheinlichkeit

Wir halten die Wahrscheinlichkeit für sehr tief, dass negative Folgen eintreten.

## 4.3. Verfügbarkeit der Daten im Projekt

Geprüft werden Risiken, die sich daraus ergeben können, dass Daten nicht mehr verfügbar sind.

### 4.3.1. Auslösende Elemente (Szenarien)

Es sind verschiedene auslösende Elemente denkbar, bspw.

- dass Daten zwar noch vorhanden sind, aber nicht mehr verwendet werden können, weil ein technischer Zugriff ausfällt,

- dass unbefugte Aussenstehende die Verfügbarkeit beeinträchtigen, bspw. durch eine DDoS-Attacke,
- dass Daten durch Mitarbeitende versehentlich gelöscht werden.

Hiergegen werden die in Ziff. 4.2.1 beschriebenen Massnahmen (Schutz des Rechenzentrums des Anbieters, Verschlüsselung der Daten) ergriffen.

#### 4.3.2. Mögliche negative Folgen

Solche sind für die Betroffenen im Fall einer Nicht-Verfügbarkeit der Daten nicht denkbar. Negative Folgen entstünden einzig für die SBB, welche keine Frequenzdaten mehr verfügbar hätte und als Folge die mit KFMS 2.0 verfolgten Ziele nicht mehr erreichen könnte.

#### 4.3.3. Wahrscheinlichkeit

Der Eintritt negativer Folgen aufgrund einer Verletzung der Verfügbarkeit ist äusserst unwahrscheinlich bis unmöglich ("sehr tief").

### **4.4. Transparenz der Datenbearbeitung**

Es werden Risiken geprüft, die sich daraus ergeben können, dass eine Datenbearbeitung für die Betroffenen intransparent sein könnte.

#### 4.4.1. Auslösende Elemente (Szenarien)

Wie vorstehend beschrieben, werden beim KFMS 2.0 keine personenbezogenen Daten verwendet. Es ist indessen denkbar, dass Betroffene irrtümlicherweise davon ausgehen, es gehe um eine personenbezogene Datenbearbeitung, bzw. dass ihre Laufwege personenbezogen aufgezeichnet würden. Dies gilt nicht zuletzt vor dem Hintergrund der Medienberichterstattung, die im Anschluss an die erste Publikation der Ausschreibung im Februar erfolgte und den Eindruck hätte erwecken können, die SBB wolle bei der Frequenzmessung mit Personendaten arbeiten.

Die SBB hat Massnahmen getroffen, transparent darzulegen, was KFMS 2.0 bezweckt und wie die SBB dabei vorgeht. Die Bahnhofbesucher:innen, die Medien und damit die Öffentlichkeit wurden und werden entsprechend transparent informiert. Entsprechende Informationen sind auf der Webseite der SBB zugänglich.

Ausserdem hat die SBB die Ausschreibung dahingehend angepasst, als dass sie auf die ursprünglich optional geplante Segmentierung nach Alter oder Geschlecht – die ebenfalls nicht zu einer Bearbeitung von Personendaten geführt hätte – verzichtet und hervorgehoben hat, dass beim KFMS 2.0 keine personenbezogenen Daten bearbeitet werden.

Die SBB wird auch weiterhin Massnahmen treffen, um das genannte Risiko weiter zu mildern. Geplant sind zusätzliche Informationen über KFMS 2.0 auf der Webseite sowie Medienmitteilungen vor der Umsetzung des Projekts.

Ausserdem wird der Kundendienst instruiert, dass er gegenüber Bahnhofsbesucher:innen auskunftsfähig ist und auf geäusserte Ängste und Bedenken angemessen reagieren kann.

Als nicht zielführend erachtet die SBB das Aufstellen von Hinweisschildern an Bahnhöfen, da dies eher verunsichern als aufklären würde.

#### 4.4.2. Mögliche negative Folgen

Mit den genannten Massnahmen wird auch das Szenario berücksichtigt, dass sich Bahnhofsbesucher:innen unbegründet beobachtet fühlen.

Das Restrisiko (Bahnhofsbesucher:innen fühlen sich dennoch beobachtet) stuft die SBB als geringfügig ein. Das heisst, gewisse Unannehmlichkeiten sind theoretisch möglich, mit denen diese Betroffenen aber umgehen können. Maximal und nur ganz vereinzelt könnten sie eventuell das Mass «überschaubar» erreichen, wobei diese Folge nicht aufgrund einer Personendatenbearbeitung einträte, sondern das Ergebnis einer falschen Annahme wäre, der die SBB so gut wie möglich entgegenwirkt.

Aufgrund der getroffenen Massnahmen sind Verhaltensänderungen von Bahnhofbesucher:innen aufgrund des KFMS 2.0 unwahrscheinlich (keine «Chilling Effects»).

#### 4.4.3. Wahrscheinlichkeit

Die Wahrscheinlichkeit, dass die genannten negativen Folgen eintreten, halten wir generell für sehr tief. Die allermeisten Bahnhofsbesucher:innen werden kaum solche Folgen verzeichnen. Allerdings ist bei wenigen Besucher:innen von einer leicht höheren Wahrscheinlichkeit auszugehen, weil gewisse Fehlannahmen über die Funktionsweise von KFMS 2.0 auch mit den getroffenen Aufklärungsmassnahmen nie ausgeschlossen werden können.

### 4.5. Integrität und Richtigkeit der Daten

Geprüft werden hier Risiken, die sich daraus ergeben können, dass Daten im Projekt falsch oder veraltet sein können.

Es werden im Projekt keine Personendaten bearbeitet. Es sind deshalb keine Risikoszenarien für die Betroffenen erkennbar. Falsche Einzeldaten würden höchstens die Genauigkeit der Besucherstrommessung beeinträchtigen, aber für die Betroffenen hätte dies keine Auswirkungen.

### 4.6. Zweckbindung der Daten

Geprüft werden hier Risiken, die sich daraus ergeben können, dass Daten im Projekt vom Verantwortlichen oder einem Dienstleister für Zwecke verwendet werden, die nicht geplant sind.

#### 4.6.1. Auslösende Elemente (Szenarien)

Da im Rahmen von KFMS 2.0 keine Personendaten verwendet werden, entfallen Risikoszenarien für die Betroffenen an und für sich. Denkbar wäre allenfalls, dass Frequenzdaten (aggregierte, anonyme Ereignisdaten) breiter als geplant eingesetzt werden.

#### 4.6.2. Mögliche negative Folgen

Keine negative Folge, da keine Personendaten erfasst und daher für andere Zwecke verwendet werden können.

Im über den Datenschutz hinausgehenden Szenario, dass Frequenzdaten breiter eingesetzt werden, könnte eine entsprechende Berichterstattung zu Befürchtungen führen, bspw. weil Betroffene denken könnten, es würden «Daten über sie» verkauft o.dgl. In diesem Fall wären die negativen Folgen ähnlich wie oben bei Ziff. 4.4 beschrieben.

#### 4.6.3. Wahrscheinlichkeit

Die Eintretenswahrscheinlichkeit ist nahe null, da keine Personendaten bearbeitet werden (vgl. oben).

Aber auch die Bearbeitung von den nicht-personenbezogenen Daten soll nicht über den ursprünglichen Zweck hinaus gehen. Die SBB verfügt über interne Prozesse und Kontrollmassnahmen, um eine ungesteuerte Verwendung von Daten aus dem KFMS 2.0 zu verhindern, bspw. Rollen-, Berechtigungs- und Zugriffskonzepte. Im Rahmen dieser Massnahmen würde die Angemessenheit einer entsprechenden Datenverwendung geprüft, hinzu kämen kommunikative Begleitmassnahmen. Die Eintretenswahrscheinlichkeit der genannten Folgen und damit das entsprechende Risiko ist daher als “sehr tief” zu bewerten.

### **4.7. Sicherstellung der Betroffenenrechte**

Geprüft werden hier Risiken, die sich daraus ergeben können, dass die Rechte der Betroffenen (auf Widerspruch zur Datenbearbeitung, auf Auskunft oder Löschung der Daten) nicht erfüllt werden können.

#### 4.7.1. Auslösende Elemente (Szenarien)

Hier stellt sich jeweils die Frage, ob etwa ein Widerspruch eines Betroffenen («Opt-Out») nicht umgesetzt oder ein Anspruch auf Auskunft oder Löschung nicht erfüllt wird.

Für KFMS 2.0 gilt: Es wird auf jede Erhebung von Personendaten verzichtet. Entsprechend ist ein Opt-Out weder nötig noch möglich. Gleichermassen erübrigen sich Auskunfts- oder Löschbegehren über Personendaten: Es ist es nicht möglich, eine Auskunft über Personendaten zu erteilen (bspw. über Messdaten) oder Löschbegehren zu entsprechen.

#### 4.7.2. Mögliche negative Folgen

Wenn ein:e Bahnhofsbesucher:in dem KFMS 2.0 widerspricht oder eine Löschung von Daten verlangt, wird die SBB darauf hinweisen, dass im Rahmen des KFMS 2.0 keine Personendaten erhoben werden und es daher auch keine Personendaten zu löschen gibt. Es ist nicht auszuschliessen, dass Bahnhofsbesucher:innen ihre informationelle Selbstbestimmung dennoch als beeinträchtigt sehen.

Dem wirkt die SBB mit den unter Ziff. 4.4.1 aufgeführten Massnahmen entgegen. Die Auswirkung der genannten Folgen stufen wir als geringfügig oder vereinzelt als überschaubar ein. Aufgrund der getroffenen Massnahmen ist im Weiteren auch nicht von einer Verhaltensänderung aufgrund des KFMS 2.0 auszugehen (keine «Chilling Effects»).

#### 4.7.3. Wahrscheinlichkeit

Die Wahrscheinlichkeit, dass die genannten negativen Folgen eintreten, halten wir generell für sehr tief. Das gilt für die allermeisten Bahnhofsbesucher:innen. Allerdings ist bei vereinzelt von einer niedrigen oder mittleren Wahrscheinlichkeit auszugehen. Allerdings sind Frustrationen von Personen nie generell auszuschliessen, und die entsprechenden Risiken sind beim KFMS 2.0 nicht höher als jedem anderen Frequenzmesssystem.

### 4.8. Ergebnis der Risikoanalyse

Es ist hier eine zusammenfassende Darstellung zu geben, welche Restrisiken für die Persönlichkeit oder die Grundrechte der betroffenen Personen trotz der technischen und organisatorischen Massnahmen des Verantwortlichen verbleiben.

Die SBB hat bei der Ausschreibung festgelegt, dass das KFMS 2.0 ohne personenbezogene Daten betrieben werden muss. Die technische Lösung des Anbieters erfüllt diese Vorgabe. Der Datenschutz wird somit voll und ganz eingehalten.

Die SBB möchte über den Datenschutz hinausgehend allfälligen negativen Empfindungen der Bahnhofsbesucher:innen entgegenwirken (sog. «gefühlter Datenschutz»). Dieser wird mit diversen Massnahmen weitgehend vorgebeugt.

Andere negative Folgen ausserhalb entsprechender Empfindungen sind nicht zu befürchten.

Die SBB trifft hierzu folgende Massnahmen bzw. hat solche schon getroffen:

- Öffentliche Neuausschreibung des Projekts, in der deutlich gemacht wird, dass keine Personendaten erhoben werden;
- Verständliche und leicht zugängliche Informationen für Bahnhofsbesucher:innen auf der Webseite;
- Medienmitteilungen zum jeweiligen Stand des Projekts;

- Instruktion des Kundendienstes für Anfragen von Bahnhofsbesucher:innen zu KFMS 2.0

Die SBB beugt mit diesen Massnahmen – namentlich der Information, dass ausschliesslich anonyme Daten genutzt werden – negativen Empfindungen im Zusammenhang mit KFMS 2.0 vor. Verbleiben solche Empfindungen dennoch bei vereinzelt Personen, so sind diese Empfindungen nicht Folge einer Bearbeitung von Personendaten, sondern einer unzutreffenden Vorstellung über das Projekt. Wir nehmen an, dass es sich hier – wenn überhaupt - nur um einige wenige oder vereinzelt Personen handelt. Zudem ist davon auszugehen, dass die Folgen für diese Betroffenen überschaubar bleiben und in keinem Verhältnis zum Nutzen für die Bahnhofsbesucher:innen stehen, welche mit den KFMS 2.0 angestrebt wird. Aufgrund der getroffenen Massnahmen ist im Weiteren auch nicht von einer Verhaltensänderung aufgrund des KFMS 2.0 auszugehen (keine «Chilling Effects»).

Die Analyse ergibt gesamthaft, dass das verbleibende Restrisiko für die Persönlichkeit oder die Grundrechte der Betroffenen als *„sehr tief“* einzustufen ist. Es werden keine Personendaten erfasst oder bearbeitet.