Datenschutzbeauftragter des Kantons Basel-Stadt

Henric Petri-Strasse 15, Postfach 205
CH-4010 Basel

Tel: +41 61 201 16 40
E-Mail: datenschutz@dsb.bs.ch
www.dsb.bs.ch

Vorabkontrolle: Schlussbericht

Alarmpikettfahrzeuge der Kantonspolizei

Status:	final
Datum:	26. April 2019
Verfasser(in):	Beat Rudin / Katja Gysin
Vertraulichkeit:	Öffentlich zugänglich gemacht im Sinne von § 20 IDG

Inhaltsverzeichnis

1 Zusammenfassung

1.1 Prüfungsbefund

Die Kantonspolizei Basel-Stadt hat sieben Alarmpikettfahrzeuge Tesla Modell X beschafft. Das Vorhaben ist nach dem Beschaffungsentscheid, aber vor dem Einsatz der Fahrzeuge, dem Datenschutzbeauftragten zur Vorabkontrolle im Sinne von § 13 des Informations- und Datenschutzgesetzes vorgelegt worden.

Der Datenschutzbeauftragte beschränkt sich bei der Vorabkontrolle seiner gesetzlichen Aufgabe entsprechend auf die *Datenschutzfragen*, also auf das Bearbeiten von Personendaten. Es stellt sich die Frage, ob durch den Betrieb der Fahrzeuge Personendaten erhoben und allenfalls bekannt gegeben werden. Falls das der Fall ist, muss geprüft werden, ob die Bearbeitung recht- und verhältnismässig ist.

Der Datenschutzbeauftragte hat über die Kantonspolizei bei der Herstellerin Informationen zu diesen Fragen eingeholt. Mit einer technischen Prüfung durch die cnlab security ag wurden die erhaltenen Informationen soweit möglich verifiziert oder plausibilisiert.

Im Resultat hat sich gezeigt:

- Die *Bild-/Videodaten*, die alle ausserhalb der Fahrzeuge aufgenommen werden, werden nur temporär auf einem internen flüchtigen Speicher festgehalten.
- Nur im Falle eines *sicherheitsrelevanten Vorfalles* (Auslösung oder Fast-Auslösung des Airbags, was während der Lebensdauer eines Fahrzeuges zwischen nie und sehr selten stattfinden dürfte) werden die Aufnahmen wenige Sekunden vor dem Ereignis auf einem fest eingebauten Speicher festgehalten, verschlüsselt an die Herstellerin übermittelt und danach auf dem Speicher im Fahrzeug gelöscht. Das Risiko einer Persönlichkeitsverletzung erscheint damit sehr gering. Um die Gefahr einer Identifikation gänzlich auszuschliessen, sollte die Kantonspolizei Basel-Stadt prüfen, ob sie diese automatische Übermittlung deaktivieren lassen will.
- Optional ist die Funktion einer *Dashcam* verfügbar; sie muss aber vom Fahrzeughalter eigens aktiviert werden. Die Kantonspolizei Basel-Stadt hat darauf verzichtet und will die Dashcams auch in Zukunft nicht einrichten. Falls sie darauf zurückkommen möchte, ist dieses Vorhaben dem Datenschutzbeauftragten zur Vorabkontrolle vorzulegen.
- *Sprach-/Audiodaten* werden nur aufgenommen, wenn der Sprachbefehlsknopf am Lenkrad aktiviert wird. Sie werden in Echtzeit verschlüsselt an einen von der Herstellerin beauftragten Drittanbieter für die Umwandlung von Sprach- zu Textbefehlen weitergeleitet und als umgewandelter Text am Armaturenbrett angezeigt. Die Sprachbefehle werden nur temporär im Fahrzeug gespeichert und nach der Bearbeitung gelöscht. Die Messung des Datenverkehrs zwischen Fahrzeug und Internet ergab, dass das beobachtete Aufkommen und Datenvo-

lumen für den Dienst plausibel erscheint. Ein allfälliger Personenbezug ist im Falle der Alarmpikettfahrzeuge nicht direkt herstellbar, da Aussenstehende grundsätzlich keine Kenntnis haben, wer sich zu einem bestimmten Zeitpunkt im Fahrzeug befindet.

- Durch weitere Sensoren werden *Informationen zum Fahrzeugzustand* (inkl. Fahrverhalten) *und zu den Fahrzeuginsassen* erhoben, auf internen Speichermedien festgehalten und anschliessend an die Herstellerin übermittelt. Die Herstellerin kann die Personen höchstens singularisieren, aber allein aufgrund der Fahrzeugidentifikationsnummer nicht bestimmen, wer die Person ist. Für die Kantonspolizei Basel-Stadt sind diese Daten zur Person der Fahrerin oder des Fahrers zuordenbar, weil die Kantonspolizei aufgrund der Einsatzplanung bzw. Einsatzleitung ohnehin weiss, wer ihrer Mitarbeitenden als Fahrerin oder Fahrer oder als weitere Teammitglieder eingeteilt ist. Ausserdem müssen Blaulichtfahrzeuge nach der Verordnung vom 19. Juni 1995 über die technischen Anforderungen an Strassenfahrzeuge (SR 741.41) mit einem Datenaufzeichnungsgerät ausgerüstet sein, so dass im Fall von Kollisionen auch weitere Informationen aus den 30 Sekunden vor dem Ereignis bekannt sind. Die Kantonspolizei Basel-Stadt muss (z.B. in einer Dienstvorschrift) die notwendigen Rechtsgrundlagen für die Bearbeitung der auf Mitarbeitende beziehbaren Daten schaffen und durch organisatorische Massnahmen sicherstellen, dass die Daten auch nur so bearbeitet werden, wie dies gerechtfertigt und verhältnismässig ist.
- Die *Geolokalisierung* (z.B. durch Nutzung eines Navigationssystems) ist datenschutzrechtlich nur relevant, wenn die Daten einen Personenbezug aufweisen. Das darf in Bezug auf die Herstellerin und die Dienstanbieter ausgeschlossen werden.
- Wenn die Datenübermittlungen an die Herstellerin und von ihr beauftragte Drittanbieter recht- und verhältnismässig sind, ist es unerheblich, mit welchen Mitteln die Datenübertragung stattfindet (Mobilfunk, WLAN, Kabel). Um das Risiko einer (ungerechtfertigten) Übertragung besser kontrollieren zu können, ist der Ersatz der Tesla-SIM-Card durch die *SIM-Card eines Schweizer Providers* zu begrüssen.
- Es ist dafür zu sorgen, dass künftige *Änderungen in der Konfiguration* der Hard- und Software auf ihre datenschutzrechtliche Relevanz überprüft und gegebenenfalls dem Datenschutzbeauftragten zur Vorabkontrolle vorgelegt werden.

1.2 Zusammenfassung der Empfehlungen

Der Datenschutzbeauftragte empfiehlt:

E1 die Deaktivierung der automatischen Übermittlung von Bilddaten bei sicherheitsrelevanten Vorfällen zu prüfen.

E2 das allfällige Vorhaben, entgegen der Zusicherung vom 27. Dezember 2018 die Dashcam in Alarmpikettfahrzeugen doch zu aktivieren, dem Datenschutzbeauftragten zur Vorabkontrolle vorzulegen.

E3 bei Aktualisierungen der Firmware sicherzustellen, dass die Funktionen der Dashcam den Vorgaben der Kantonspolizei noch entsprechen.

E4 die Nutzung der Synchronisierungsfunktion mit Daten aus Mobiltelefonen der Fahrzeuginsassen zu regeln.

E5 für die Bearbeitung der durch Sensoren erhobenen Daten, die auf Mitarbeitende beziehbar sind, die notwendigen personalrechtlichen Rechtsgrundlagen (z.B. eine Dienstvorschrift) zu schaffen und

E6 durch organisatorische Massnahmen sicherzustellen, dass die Daten auch nur so bearbeitet werden, wie dies gerechtfertigt und verhältnismässig ist.

E7 die Erfassung und Übermittlung von Strassenabschnittsdaten nicht zu aktivieren.

E8 wesentliche datenschutzrechtlich relevante Änderungen der Hardware-/ Software-Konfiguration erneut dem Datenschutzbeauftragten zur Vorabkontrolle vorzulegen.

2 Vorhaben, involvierte Personen, Unterlagen

2.1 Zur Vorabkontrolle unterbreitetes Vorhaben

Vorhaben	Beschaffung von sieben Alarmpikettfahrzeugen der Kantonspolizei

2.2 Angaben zur verantwortlichen Dienststelle

Verantwortliche Dienstelle	Kantonspolizei Basel-Stadt
Adresse	Spiegelhof, 4001 Basel
Dienststellenleitung	Oberst Martin Roth, Kommandant
Departement	Justiz- und Sicherheitsdepartement des Kantons Basel-Stadt

2.3 Involvierte Personen

Seitens der Kantonspolizei waren in die Vorabkontrolle involviert: der Kommandant, das Ressort Organisation und Technik, das Ressort Einsatzlogistik und der Dienst Recht.

Seitens des Datenschutzbeauftragten waren in diese Vorabkontrolle involviert: Beat Rudin, Datenschutzbeauftragter, Katja Gysin, Stellvertretende Datenschutzbeauftragte, Thomas Sterchi, IT-Sicherheit, und Lucas Maciejewski, juristischer Volontär.

Technische Unterstützung für die Abklärung spezifischer Fragen wurde von cnlab security AG im Auftrag der Kantonspolizei geleistet.

2.4 Eingereichte Unterlagen

Titel	Verfasserin/ Verfasser	Datum
Beschaffungsbeschluss Alarmpikett-Fahrzeuge	JSD	08.03.2018
Kundendatenschutzrichtlinie Tesla	Tesla	20.04.2018 (erhalten)
Stellungnahme Tesla, E-Mail	Datenschutzver-	18.12.2018

	antwortlicher Tesla Europa	
Projektbeschrieb für Vorabkontrolle Tesla Alarmpikettfahrzeuge	JSD	27.12.2018
Antworten von Tesla auf Fragenkatalog Kantonspolizei (1)	Tesla	20.02.2019
Antworten von Tesla auf Fragenkatalog Kantonspolizei (2)	Tesla	15.03.2019
Stellungnahme Tesla, E-Mail	Datenschutzverantwortlicher Tesla Europa	22.03.2019
Antworten von Tesla auf Fragenkatalog Kantonspolizei (3)	Tesla.	08.04.2019
Zwischenbericht cnlab security AG	cnlab security AG	05.04.2019
2. Zwischenbericht cnlab security AG	cnlab security AG	11.04.2019

3 Ausgangslage, Fragestellung, Vorgehen

3.1 Ausgangslage

Die Beschaffung von sieben Alarmpikettfahrzeugen der Marke Tesla, Model X, wurde dem Datenschutzbeauftragten erstmals am 20. April 2018, nach dem Beschaffungsentscheid, zur Kenntnis gebracht. In einer unverbindlichen Stellungnahme vom 2. Mai 2018 hat der Datenschutzbeauftragte auf verschiedene datenschutzrechtliche Fragestellungen hingewiesen, deren Abklärung und risikoorientierte Einschätzung von der beschaffenden Stelle vorzunehmen seien. Im Dezember 2018 wurde das Projekt dem Datenschutzbeauftragten erneut vorgelegt.

Um den 21. Dezember 2018 herum wurde in Medienberichten kolportiert, von diesen Fahrzeugen würden Bild- und Tonaufnahmen gemacht und an Tesla (fortan: die Herstellerin) übermittelt. Der Datenschutzbeauftragte hat dabei verlauten lassen, dass sich Datenschutzfragen stellen würden, wenn Personendaten bearbeitet, d.h. aufgenommen und übermittelt würden. Ob das der Fall sei, könne aber erst nach Abschluss der Vorabkontrolle gesagt werden. Die Aussage, dass die Fahrzeuge «wegen des Datenschutzes» in der Garage stünden, war unzutreffend, da sie ohnehin erst nach Abschluss der Ausrüstung und Schulung der Fahrerinnen und Fahrer eingesetzt werden sollten. Diese Zeit sollte auch für die Prüfung der datenschutzrechtlichen Aspekte genutzt werden.

Aufgrund der im Dezember 2018 von der Kantonspolizei gelieferten Umschreibung des Projektes wurde in der Folge der weitere Informationsbedarf ermittelt und – zur Verifikation der von der Herstellerin zu erwartenden Informationen – eine technische Prüfung vorbereitet.

3.2 Vorgehen

Basierend auf den von der Kantonspolizei am 27. Dezember 2018 erhaltenen Ausführungen zu den Rechtsgrundlagen und auf den Angaben zu den vom Alarmpikettfahrzeug potentiell bearbeiteten Datenarten wurde in Zusammenarbeit mit der cnlab security AG ein erweiterter Fragenkatalog zuhanden der Herstellerin erstellt. Es wurden insbesondere Fragen zu den Bildaufnahmen, den Audioaufnahmen, der Speicherung von Daten und der Übermittlung von Daten gestellt. Dieser Fragenkatalog wurde der Herstellerin von der Kantonspolizei zur Beantwortung übermittelt. Eine erste Stellungnahme, datiert vom 20. Februar 2019, wurde von der Herstellerin an die Kantonspolizei übermittelt und nachfolgend dem Datenschutzbeauftragten und der cnlab security AG zur Verfügung gestellt. Da noch nicht alle gestellten Fragen beantwortet wurden bzw. sich aus den Antworten neue Fragen ergaben, wurde der entsprechend erweiterte Fragenkatalog der Herstellerin erneut vorgelegt. Am 15. März 2019 hat die Herstellerin die Antworten zu bestimmten Fragen nachgeliefert und am 8. April die Mehrzahl der gestellten Fragen schriftlich beantwortet.

Parallel zur Beantwortung von rechtlichen und technischen Fragen durch die Herstellerin hat die cnlab security AG im Auftrag der Kantonspolizei und in Absprache mit dem Datenschutzbeauftragten verschiedene technische Prüfschritte an den drei bereits ausgelieferten Fahrzeugen der Kantonspolizei vorgenommen. Mit Datum vom 5. April 2019 hat die cnlab security AG einen ersten Zwischenbericht an die Kantonspolizei und den Datenschutzbeauftragten geliefert. Am 11. April 2019 hat der Datenschutzbeauftragte von der Kantonspolizei einen aufdatierten Zwischenbericht der cnlab security AG erhalten.

3.3 Fragestellung, Abgrenzungen

Moderne Fahrzeuge produzieren eine grosse Menge an Informationen zu verschiedenen Zwecken, seien es für den Betrieb oder die Sicherheit relevante Informationen, seien es Informationen, die den Fahrzeugführer unterstützen oder auch Informationen, welche der Fahrzeugherstellerin bzw. den von ihr assoziierten Drittanbietern in der Weiterentwicklung ihrer Produkte nützen.

Der Datenschutzbeauftragte ist sich bewusst, dass auch Fahrzeuge anderer Marken und Machart, die bereits heute im Gebrauch der kantonalen Verwaltung stehen, Informationen und potentiell Personendaten bearbeiten und bekanntgeben. Deren Prüfung ist nicht Gegenstand dieser Vorabkontrolle. Der vorliegende Bericht beinhaltet einzig die Prüfung datenschutzrechtlicher Fragen im Zusammenhang mit den beschafften Alarmpikettfahrzeugen Tesla, ausgehend vom Zustand und den Einrichtungen der drei bereits ausgelieferten Fahrzeuge.

Wenn die Kantonspolizei Basel-Stadt als öffentliches Organ des Kantons Basel-Stadt Personendaten bearbeitet (oder bearbeiten lässt), findet das baselstädtische Informations- und Datenschutzgesetz (IDG) Anwendung (§ 2 Abs. 1 i.V.m. § 3 Abs. 1 IDG). Datenschutzrechtlich relevant ist das Bearbeiten (§ 3 Abs. 5 IDG) von Personendaten (§ 3 Abs. 3 und 4 IDG). Insoweit also Personendaten bearbeitet werden, unterliegt diese Datenbearbeitung den gleichen Voraussetzungen wie jede andere Datenbearbeitung durch die Verwaltung, nämlich dem Legalitäts- und dem Verhältnismässigkeitsprinzip.

Zu prüfen ist also primär, ob Personendaten bearbeitet werden und ob diese Bearbeitung gesetz- und verhältnismässig erfolgt.

Das Alarmpikettfahrzeug Tesla verfügt über folgende technische Einrichtungen, die potentiell für die Erhebung, Speicherung und allenfalls auch Übermittlung von Personendaten geeignet sind:

- acht Aussen-Kameras (mit zugehörigen Ultraschall- und Radar-Sensoren): Bilddaten (Videodaten), die allenfalls einen Personenbezug aufweisen können;

- eine Sprachsteuerung im Fahrzeuginnern: Tondaten (Audiodaten), die allenfalls einen Personenbezug aufweisen können;

- weitere Sensoren: weitere fahrzeugzustands- oder fahrverhaltensspezifische Daten, die kombiniert mit anderen, die Fahrerin oder den Fahrer identifizierenden Informationen allenfalls einen Personenbezug aufweisen können.

Zu unterscheiden ist dabei im Hinblick auf die Rechtfertigung des Bearbeitens von Personendaten, ob – vor allem bei den ersten beiden Sensor-Arten – (Bild- und/oder Ton-)Daten (auch) über Drittpersonen bearbeitet werden, die sich im Fahrzeug oder im Umfeld des Fahrzeuges befinden, oder ob – bei allen drei Sensor-Arten, vor allem aber bei der dritten – Daten über Mitarbeitende der Kantonspolizei bearbeitet werden. Im ersten Fall muss die Rechtfertigung polizeirechtlich erfolgen, im zweiten Fall vorwiegend personalrechtlich.

Der Fokus der vorliegenden Vorabkontrolle durch den Datenschutzbeauftragten richtet sich in erster Linie auf die Bearbeitung von Personendaten von betroffenen Drittpersonen, also Bürgerinnen und Bürgern, die nicht im Dienst der Kantonspolizei stehen.

Ganz ausserhalb des Fokus des Datenschutzbeauftragten sind Fragestellungen, die nicht Personendaten betreffen, also Risiken beispielweise für die polizeiliche Aufgabenerfüllung, nicht aber für die Persönlichkeitsrechte betroffener Personen.

3.4 Rechtsgrundlagen

Das Informations- und Datenschutzgesetz regelt den Umgang der öffentlichen Organe mit Informationen und insbesondere die Voraussetzung für die Bearbeitung von Personendaten. Personendaten sind in § 3 Abs. 3 IDG definiert als Informationen, die sich auf eine bestimmte oder bestimmbare natürliche oder juristische Person beziehen. Bestimmbar sind Personen, wenn sie aufgrund der Bild- und/oder Tonaufnahmen identifizierbar sind, sei es direkt, z.B. über die Gesichts- oder Stimmaufnahme, sei es indirekt, z.B. über aufgenommene Kontrollschilder von Fahrzeugen.

Nach § 9 Abs. 1 IDG darf ein öffentliches Organ Personendaten bearbeiten, wenn dafür entweder eine gesetzliche Grundlage besteht (unmittelbare gesetzliche Grundlage) oder die Bearbeitung zur Erfüllung einer gesetzlichen Aufgabe erforderlich ist (mittelbare gesetzliche Grundlage). Besondere Personendaten – im vorliegenden Fall sind Angaben zur Gesundheit oder auch Angaben zu strafrechtlichen Verfolgungen und Sanktionen denkbar (§ 3 Abs. 4 lit. a IDG) – dürfen bearbeitet werden, wenn ein Gesetz (nicht bloss eine Verordnung) ausdrücklich dazu ermächtigt oder verpflichtet (unmittelbare gesetzliche Grundlage) oder wenn die Datenbearbeitung für eine in einem Gesetz klar umschriebene Aufgabe zwingend notwendig ist (mittelbare gesetzliche Grundlage) (§ 9 Abs. 2 IDG). Die entsprechende gesetzliche Grundlage findet sich in den jeweiligen Sachgesetzen, hier unter Umständen im Polizei- und im Personalrecht. Jedes Bearbeiten von Personendaten muss ausserdem verhältnismässig sein (d.h. zur Erreichung des Zwecks [= zur Erfüllung der gesetzlichen Aufgabe] geeignet, zur Erreichung des Zwecks [= zur Erfüllung der gesetzlichen Aufgabe] erforderlich und der betroffenen Person zumutbar).

Werden Personendaten an Dritte (z.B. an die Herstellerin oder an andere Empfänger) bekannt gegeben, so gelten nach § 21 IDG praktisch identische Voraussetzungen in Bezug auf die Gesetzmässigkeit und die Verhältnismässigkeit. Als Bekanntgabe gilt nach § 3 Abs. 6 IDG jedes Zugänglichmachen von Informationen wie das Einsichtgewähren, Weitergeben oder Veröffentlichen.

Die inhaltlichen Vorgaben zur Rechtmässigkeit ergeben sich im Kanton Basel-Stadt primär aus folgenden Rechtserlassen:

Rechtliche Grundlagen	Fundstelle
Gesetz vom 9. Juni 2010 über die Information und den Datenschutz (IDG)	SG 153.260
Verordnung vom 9. August 2011 über die Information und den Datenschutz (IDV)	SG 153.270
Gesetz vom 13. November 1996 betreffend die Kantonspolizei des Kantons Basel-Stadt (Polizeigesetz, PolG)	SG 510.100
Personalgesetz vom 17. November 1999	SG 162.100

3.5 Empfehlungen des Datenschutzbeauftragten

Der Datenschutzbeauftragte kann zum Umgang mit Informationen Empfehlungen abgeben (§ 46 IDG).

Nach § 46 Abs. 2 IDG hat das öffentliche Organ, an welches die Empfehlungen gerichtet sind, gegenüber dem Datenschutzbeauftragten zu erklären, ob es den Empfehlungen folgen will.

3.6 Weiteres Vorgehen

Die Umsetzung der Empfehlungen des Datenschutzbeauftragten obliegt dem verantwortlichen öffentlichen Organ (hier also: der Kantonspolizei).

Das öffentliche Organ wird deshalb gebeten, dem Datenschutzbeauftragten zeitnah nach Zustellung dieses Berichts bezüglich jeder einzelnen Empfehlung mitzuteilen:

- ob es der Empfehlung folgen will,
- bis wann sie umgesetzt werden soll, beziehungsweise
- warum sie nicht umgesetzt werden soll.

4 Prüfgebiete und Feststellungen

4.1 Videodaten (Erhebung und Bekanntgabe von Personendaten)

Vorgaben

Personendaten dürfen von der Kantonspolizei unter Beachtung von § 9 IDG bearbeitet werden: Vorhandensein einer unmittelbaren oder mittelbaren gesetzlichen Grundlage, Beachtung der Verhältnismässigkeit (vgl. vorne Ziff. 3.4). Die Verantwortung für den Umgang mit Informationen trägt dasjenige öffentliche Organ, das die Informationen zur Erfüllung seiner gesetzlichen Aufgaben bearbeitet (§ 6 IDG) oder bearbeiten lässt (§ 7 IDG). Es muss dabei die Informationen mit angemessenen organisatorischen und technischen Massnahmen schützen und insbesondere deren Vertraulichkeit gewährleisten (§ 8 IDG).

Bekannt gegeben werden dürfen Personendaten von der Kantonspolizei unter Beachtung von § 21 IDG: Vorhandensein einer unmittelbaren oder mittelbaren gesetzlichen Grundlage oder einer ausdrücklichen Einwilligung der betroffenen Person im Einzelfall, Beachtung der Verhältnismässigkeit (vgl. vorne Ziff. 3.4).

4.1.1 Videodaten generell

Feststellungen

Nach Auskunft der Herstellerin ist das Alarmpikettfahrzeug Tesla Modell X mit acht nicht hochauflösenden Kameras ausgestattet. Die Kameras und Sensoren überwachen den Aussenraum des Fahrzeugs. Die Kameras und Sensoren seien nur in Betrieb, wenn das Fahrzeug eingeschaltet ist. Im Fahrzeuginnern befinden sich gemäss Angaben der Herstellerin keine Bildaufnahmegeräte. Die Funktion der Kameras und Sensoren liegt in der Unterstützung des Fahrers und der Sicherheitssysteme des Fahrzeuges. Zusätzlich erlaubt die Rückfahrkamera einen aktuellen Blick auf den Bereich hinter dem Fahrzeug. Eine der Frontkameras offeriert zusätzlich die Möglichkeit der Einrichtung einer «Dashcam», also einer frontal aufzeichnenden Videokamera. Die Dashcam muss vom Fahrzeughalter speziell eingerichtet werden und ist nicht ab Werk betriebsbereit.

Nach den Angaben der Herstellerin speichern die **Kameras** – ausser der Dashcam (siehe dazu weiter unten) – nicht laufend Bilder. Bildaufnahmen werden zwar unverschlüsselt, aber nur temporär auf einem internen flüchtigen Speicher (im sog. Autopilot Board) festgehalten. Im Falle eines sicherheitsrelevanten Vorfalles («safety relevant incident») werden kurze Aufnahmen vor dem Ereignis auf einem fest eingebauten Speicher im Fahrzeug festgehalten (im Autopilot Board). Sicherheitsrelevante Vorfälle sind einerseits die Auslösung des Airbags und andererseits die Fast-Auslösung des Airbags, also eine ungewöhnliche Geschwindigkeitsveränderung unterhalb des Schwellenwertes, bei dem der Airbag ausgelöst wird («A ‹near-deployment› is a circumstance where the vehicle experiences a sudden change in velocity sufficient to reach the regulatorily-defined threshold to start recording data related to

a collision to the vehicle's event data recorder, but the change in velocity is below the regulatorily-defined threshold for airbag deployment.»). Gemäss Angaben der Herstellerin verlangen die Bildaufnahmen eine weitere Bearbeitung mit spezifischer, hersteller-eigener Software, um sie in gängige Bildformate zu transformieren. Die Daten werden zwar unverschlüsselt abgelegt, ein Zugriff darauf innerhalb des Fahrzeugs sei jedoch nicht möglich ohne Zerstörung des Autopilot Boards. Diese im Fahrzeug gespeicherten Aufnahmen stehen der Herstellerin zur Auswertung zur Verfügung, nicht aber dem Fahrzeughalter.

Die Aufnahmen aus sicherheitsrelevanten Vorfällen werden nach Herstellerangaben verschlüsselt an die Herstellerin übermittelt (über WLAN, über das Mobilfunknetz oder durch Auslesen im Servicecenter) und nach erfolgreicher Übermittlung vom Fahrzeugspeicher gelöscht. Sie werden von der Herstellerin für die Verbesserung der Fahrzeugsicherheit genutzt und nach deren Angaben gelöscht, wenn sie für die Zweckerfüllung nicht mehr benötigt werden. Die Herstellerin gibt an, dass die Datenübermittlung an sie vom Servicecenter ausgeschaltet werden kann, ohne dass die Betriebssicherheit des Fahrzeugs beeinträchtigt wird. Die Datenübertragung kann dann nur wieder im Servicecenter eingerichtet werden (nicht über einen Fernzugriff auf das System).

Bilddaten weisen mindestens das Potenzial eines Personenbezugs auf. Natürliche Personen können u.a. über die Erkennung ihres Gesichtes, die Halterinnen und Halter von Fahrzeugen über deren Kontrollschilder oder anderen Kennzeichnungen bestimmbar werden. Die Aufzeichnungen aus den Kameras können also Personendaten enthalten.

Die cnlab security AG hat die Datenübermittlung vom Fahrzeug an die Herstellerin technisch überprüft. Der Datenverkehr zwischen dem Fahrzeug und dem Internet wurde über die WLAN-Strecke gemessen. Während der Messung wurde das Fahrzeug in verschiedene Situationen gebracht (fahrend, abgestellt, geparkt und abgeschlossen, ladend). Da die Datenübertragung an die Herstellerin verschlüsselt erfolgt, konnten keine Aussagen zum Inhalt der Datenübertragung gemacht werden. Anhand der übermittelten Datenvolumina konnten zumindest die Angaben der Herstellerin plausibilisiert werden. Dabei sind keine Auffälligkeiten festgestellt worden, die in Widerspruch zu den von der Herstellerin gemachten Angaben stehen. Insbesondere die Übertagung von Bilddateien wäre aufgrund ihres Volumens in der technischen Prüfung aufgefallen. Es bestehen somit keine Hinweise, dass eine laufende Übermittlung von Bildaufnahmen an die Herstellerin stattfindet.

Die Datenübertragung konnte selbstverständlich nur in gewissen Fahrzeugsituationen geprüft werden; insbesondere die künstliche Herbeiführung einer Situation die zur Auslösung der Bildaufnahmen bei sicherheitsrelevanten Vorfällen geführt hätten, konnte unter Laborbedingungen nicht hergestellt werden. Es wird aber von der cnlab security AG in ihrem Bericht festgehalten, dass die technischen Prüfungen keine Anzeichen ergeben haben, die den Angaben der Herstellerin widersprechen würden. Eine analoge Messung des Datenverkehrs zwischen Fahrzeug und Internet über die Mobilfunk-Verbindung (via den Mobilfunk-Provider) konnte noch nicht durchgeführt werden, da der Zugang zum Mobildatenverkehr aus regulatorischen Gründen noch

nicht gewährt wurde. Führen die Ergebnisse dieser Messung zu einer abweichenden Beurteilung, wird dies in einem Nachtrag zum vorliegenden Bericht festgehalten.

Drei Spezialfälle sind im Folgenden gesondert zu betrachten: die Aufnahmen der Rückfahrkamera, die Speicherung und Übermittlung von Bilddaten bei sicherheitsrelevanten Vorfällen und beim Einsatz der Dashcam.

Zu den Spezialfällen:

- Die Bilder der **Rückfahrkamera** werden nach Herstellerangaben nur als Hilfe für die Fahrerin oder den Fahrer angezeigt und nur im flüchtigen Speicher aufgezeichnet; diese Rückfahrhilfe wird bei einer Mehrzahl von heute verkauften Fahrzeugen angeboten und ist damit nicht fahrzeugspezifisch. Die reine Anzeige der Rückfahrkamera erscheint, selbst wenn in Einzelfällen allenfalls Personen identifizierbar sein könnten, zum sicheren Betrieb des Fahrzeuges erforderlich und damit datenschutzkonform. Damit erübrigt sich eine Empfehlung.

- Bei **sicherheitsrelevanten Vorfällen** werden die Bilddaten von wenigen Sekunden vor dem Vorfall abgespeichert und an die Herstellerin übermittelt. Nach erfolgreicher Übermittlung der Daten an die Herstellerin werden sie auf dem lokalen Speicher im Fahrzeug gelöscht. Für die Herstellerin dienen diese Aufnahmen zur Verbesserung der Sicherheit (und wohl auch zum Beweis, dass nicht ein Mangel am Fahrzeug z.B. Unfallursache war). Die Herstellerin macht keine über ihre Datenschutzrichtlinie hinausgehende Zusicherung betreffend die Datennutzung. Allerdings wird während der Lebensdauer eines Fahrzeuge eine solche Datenübermittlung statistisch gesehen wohl zwischen niemals und ein paar wenigen Malen geschehen. In diesen Fällen ist es dann ausserdem auch durchaus möglich, dass die Daten für die Herstellerin überhaupt nicht auf eine bestimmbare Person bezogen werden können. Das Risiko einer Persönlichkeitsverletzung erscheint deshalb als sehr gering. Trotzdem sollte die Kantonspolizei, um die Gefahr der Identifikation gänzlich auszuschliessen, prüfen, ob sie diese automatische Übermittlung deaktivieren lassen will.

- Zu Videodaten aus dem Betrieb der Dashcam siehe sogleich unten (Ziff. 4.1.2).

Empfehlungen

Der Datenschutzbeauftragte empfiehlt:

E1 die Deaktivierung der automatischen Übermittlung von Bilddaten bei sicherheitsrelevanten Vorfällen zu prüfen.

4.1.2 Videodaten aus der Dashcam

Feststellungen

Eine der vorwärts gerichteten Kameras kann als Dashcam genutzt werden. Dafür muss der Fahrzeughalter (hier also die Kantonspolizei Basel-Stadt) einen eigenen USB-Speicher im Fahrzeug bereitstellen. Wird die Dashcam vom Fahrzeughalter

eingerichtet, wird jeweils ein Clip von einer Minute Länge aufgezeichnet und als Aufnahme bis zu einer Stunde festgehalten. Nach einer Stunde wird der Speicher mit neuen Aufnahmen überschrieben. Diese Aufnahmen sind im Standardformat .mp4 als Videos gespeichert und abrufbar durch den Fahrzeughalter. Es findet keine Übermittlung an die Herstellerin statt.

Die Kantonspolizei hat bereits in ihrem Projektbeschrieb vom 27. Dezember 2018 mitgeteilt, dass sie auf die Einrichtung der optionalen Dashcam verzichtet. Sie hat ausserdem zugesichert, dass sie die Dashcams auch in Zukunft nicht einrichten will.

Die technische Prüfung der cnlab security AG hat bestätigt, dass die USB-Anschlüsse bei den bereits vorhandenen Fahrzeugen ausgebaut wurden. Die elektrischen Kontakte für die USB-Anschlüsse sind somit nur durch mechanische Manipulationen am Fahrzeug wieder erreichbar.

Der Datenschutzbeauftragte nimmt von der Zusicherung der Kantonspolizei Kenntnis, dass die Dashcam nicht eingerichtet ist und auch in Zukunft nicht eingerichtet werden soll.

Die cnlab security AG hat aber darauf hingewiesen, dass die Dashcam-Funktion gemäss Herstellerin in einer Beta-Phase ist und bei einer Firmware-Aktualisierung eventuell neue Funktionen eingeführt werden. Es ist somit nicht auszuschliessen, dass sich die Dashcam-Funktion in Zukunft noch ändern wird. Bei Aktualisierungen der Firmware muss deshalb sichergestellt werden, dass die Funktionen der Dashcam den Vorgaben der Kantonspolizei noch entspricht.

Empfehlungen

Falls die Kantonspolizei auf diese Zusicherung zurückkommen möchte, ist zu verlangen, dass sie dieses Vorhaben dem Datenschutzbeauftragten zur Vorabkontrolle unterbreitet und insbesondere die dafür notwendigen Rechtsgrundlagen nachweist und die zur Wahrung der Grundrechte betroffener Personen erforderlichen Schutzmassnahmen vorschlägt.

Der Datenschutzbeauftragte empfiehlt:

E2 das allfällige Vorhaben, entgegen der Zusicherung vom 27. Dezember 2018 die Dashcam in Alarmpikettfahrzeugen doch zu aktivieren, dem Datenschutzbeauftragten zur Vorabkontrolle vorzulegen;

E3 bei Aktualisierungen der Firmware sicherzustellen, dass die Funktionen der Dashcam den Vorgaben der Kantonspolizei noch entsprechen.

4.2 Audiodaten (Erhebung und Bekanntgabe von Personendaten)

Vorgaben

Zu den Vorgaben für das Bearbeiten von Personendaten vgl. oben Ziff. 4.1.

Feststellung

Das Alarmpikettfahrzeug Tesla hat gemäss Angaben der Herstellerin zwei Mikrophone im Fahrzeuginnern. Mittels Sprachsteuerung können über diese Mikrophone Anrufe auf einem via Bluetooth verbundenen Mobiltelefon getätigt werden, es kann Musik abgespielt und das Navigationsgerät genutzt werden. Zur Nutzung der Sprachbefehle können die Kontakte aus einem (persönlichen) Mobiltelefon von den Nutzenden via Bluetooth mit dem Fahrzeug synchronisiert werden. Dabei werden Kontaktdaten von Dritten im Fahrzeug gespeichert.

Die Mikrophone nehmen Geräusche und Stimmen auf, wenn sie über den Sprachbefehlsknopf am Lenkrad aktiviert werden. Die Aufnahmen können über denselben Knopf auch wieder beendet werden. Hört der Sprechende auf zu sprechen, endet die Aufnahme ebenfalls. Startet die Aufnahme, erklingt ein Signalton und eine Anzeige erscheint am Armaturenbrett. Während der Aufnahme werden die Sprachbefehle ebenfalls am Armaturenbrett angezeigt. Sprachbefehle werden nur temporär im Fahrzeug gespeichert und nach der Bearbeitung gelöscht.

Die Sprachaufnahmen werden verschlüsselt übertragen. Sie werden in Echtzeit über die Internetverbindung an die von der Herstellerin beauftragten Drittanbieter für die Umwandlung von Sprach- zu Textbefehlen weitergeleitet. Gemäss den Angaben der Herstellerin werden keine identifizierenden Merkmale im Zusammenhang mit den Sprachbefehlen übermittelt. Die Herstellerin selber erhält nach eigenen Angaben keine Kopien von Sprachaufnahmen.

Die technische Prüfung der cnlab security AG hat den Datenverkehr zwischen dem Fahrzeug und dem Internet über die WLAN-Strecke gemessen. Unmittelbar nach der Aufnahme eines Befehls über die Sprachsteuerung konnte der Verbindungsaufbau zu Drittanbietern beobachtet werden. Obwohl eine genaue Zuordnung der einzelnen Verbindungen aufgrund der Verschlüsselung der Inhalte nicht möglich war, schien das beobachtete Aufkommen und Datenvolumen plausibel für diese Form von Dienst. Eine automatische oder ungewollte Auslösung der Sprachsteuerung konnte während der technischen Prüfung nicht beobachtet werden.

Eine analoge Messung des Datenverkehrs zwischen Fahrzeug und Internet über die Mobilfunk-Verbindung (via den Mobilfunk-Provider) ist zurzeit noch ausstehend. Führen die Ergebnisse dieser Messung zu einer abweichenden Beurteilung, wird dies in einem Nachtrag zum vorliegenden Bericht festgehalten.

Die im Rahmen der Sprachsteuerung bearbeiteten Daten können unter Umständen Personendaten darstellen. Die Daten werden aber nur flüchtig gespeichert und nach der Umwandlung zu Text gelöscht. Die Auslesung der Daten ist somit nur sehr schwierig möglich. Zudem finden die Audioaufnahmen in einem klar definierten Umfang statt und sind von den Fahrzeuginsassen einfach zu kontrollieren. Ein allfälliger Personenbezug ist im Falle der Alarmpikettfahrzeuge nicht direkt herstellbar, da Aussenstehende grundsätzlich keine Kenntnis haben, wer sich zu einem bestimmten Zeitpunkt im Fahrzeug befindet. Dieser Bezug ist zwar für die Kantonspolizei anhand der Einsatzplanung herstellbar, bei mehreren Fahrzeuginsassen müsste dann aber die sprechende Person anhand der Stimme identifiziert werden. Der Aufwand

für die Bestimmbarkeit der Person erscheint unverhältnismässig hoch und das Potential für eine persönlichkeitsverletzende Bearbeitung von Personendaten vernachlässigbar. Es werden zudem keine Daten an die Herstellerin bekanntgegeben und die Übermittlung von Sprachbefehlen an Drittanbieter scheint anhand der vorliegenden Angaben nicht auf Personen bezogen werden zu können. Eine Empfehlung zu diesem Sachverhalt erübrigt sich somit.

Die Synchronisation von Daten aus Mobiltelefonen mit dem Fahrzeug kann von der Kantonspolizei zugelassen oder untersagt werden. Falls Daten aus Mobiltelefonen (zum Beispiel Kontakte oder Kalendereinträge) mit dem Fahrzeug synchronisiert werden dürfen, muss sichergestellt werden, dass diese Daten nur so lange gespeichert werden, wie dies zur Aufgabenerfüllung notwendig ist. Danach müssen die Daten vom Fahrzeugspeicher gelöscht werden.

Empfehlung

Der Datenschutzbeauftragte empfiehlt:

E4 die Nutzung der Synchronisierungsfunktion mit Daten aus Mobiltelefonen der Fahrzeuginsassen zu regeln.

4.3 Sensordaten

4.3.1 Allgemein

Vorgaben

Zu den Vorgaben für das Bearbeiten von Personendaten vgl. oben Ziff. 4.1.

Feststellung

Die geprüften Alarmpikettfahrzeuge sind mit diversen Sensoren inner- und ausserhalb des Fahrzeugs ausgestattet. Nach den Angaben der Herstellerin erfassen diese Sensoren Informationen zum Fahrzeugzustand (inkl. Fahrverhalten) und zu den Fahrzeuginsassen auf interne Speichermedien und übermitteln sie anschliessend an die Herstellerin (zu den Standortdaten vgl. unten Ziff. 4.3.2). Gemessen wird beispielsweise der Abstand des Fahrzeugs von anderen Fahrzeugen oder Gegenständen oder ob eine Person auf dem Fahrersitz sitzt. Ziel der Sensormessungen ist es zum einen, den Fahrzeuginsassen Warnhinweise zu geben; zum andern dienen sie der Wartung und Weiterentwicklung des Fahrzeugs. Informationen von Sensoren werden lokal im Fahrzeug, unverschlüsselt auf einer Speicherkarte gespeichert. Nach Ausbau der Speicherkarte können die Daten grundsätzlich ausgelesen werden. Zudem ist der Zugriff auf die Daten für das Servicecenter wie auch für die Herstellerin möglich.

Die von den Sensoren erhobenen und gespeicherten Daten können einen Personenbezug aufweisen, wenn sie mit Angaben zu den Fahrzeuginsassen verbunden werden können. Insbesondere die Verbindung mit der Fahrzeugidentifikationsnum-

mer kann dazu beitragen, dass Personen identifizierbar sind (bei Privatfahrzeugen z.B. der registrierte Fahrzeughalter). Im Fall der Alarmpikettfahrzeuge wären diese Daten für die Herstellerin allenfalls zuordenbar, wenn die Fahrerin oder der Fahrer ihr/sein Profil (mit den Einstellungen für die Sitzposition, Spiegelstellung usw.) namentlich eingibt. Die Kantonspolizei empfiehlt ihren Mitarbeitenden aber, dies nur mit einem (selbstgewählten) Pseudonym zu tun. Die Herstellerin kann also die Personen höchstens singularisieren (also feststellen, dass es wiederum die gleiche Person ist), aber allein aufgrund der Fahrzeugidentifikationsnummer nicht bestimmen, wer die Person ist. Weitere Personen im Fahrzeug oder Personen ausserhalb des Fahrzeuges können zwar als Menschen erkannt, aber nicht identifiziert werden. Für die Herstellerin handelt es sich also nicht um Personendaten. Damit erübrigt sich diesbezüglich eine Empfehlung. Allenfalls könnte geprüft werden, ob im Servicecenter die Übermittlung von Sensordaten an die Herstellerin ausgeschaltet werden soll. Das Fahrzeug bleibt nach Herstellerangaben funktionsfähig.

Für die Kantonspolizei sind diese Daten zur Person der Fahrerin oder des Fahrers zuordenbar, weil die Kantonspolizei aufgrund der Einsatzplanung bzw. Einsatzleitung ohnehin weiss, wer ihrer Mitarbeitenden als Fahrerin oder Fahrer oder als weitere Teammitglieder eingeteilt ist. Ausserdem müssen Blaulichtfahrzeuge nach der Verordnung vom 19. Juni 1995 über die technischen Anforderungen an Strassenfahrzeuge (SR 741.41) mit einem Datenaufzeichnungsgerät ausgerüstet sein, so dass im Fall von Kollisionen auch weitere Informationen aus den 30 Sekunden vor dem Ereignis bekannt sind.

Es erscheint nicht schon als problematisch, dass die Kantonspolizei diese Daten besitzt. Problematisch kann allenfalls sein, was sie damit macht. Eine (personenbezogene) Verwendung dieser Daten muss deshalb personalrechtlich gerechtfertigt sein. Eine (verhältnismässig ausgestaltete) Anordnung erscheint im Rahmen des Weisungsrechts des Arbeitgebers zulässig. Damit soll sichergestellt werden, dass für die Mitarbeitenden transparent ist, welche Daten über sie unter welchen Voraussetzungen zu welchem Zweck wie lange bearbeitet werden, und dass die Bearbeitung rechtmässig und verhältnismässig ist.

Empfehlung

Der Datenschutzbeauftragte empfiehlt:

E5 für die Bearbeitung der durch Sensoren erhobenen Daten, die auf Mitarbeitende beziehbar sind, die notwendigen personalrechtlichen Rechtsgrundlagen (z.B. eine Dienstvorschrift) zu schaffen und

E6 durch organisatorische Massnahmen sicherzustellen, dass die Daten auch nur so bearbeitet werden, wie dies gerechtfertigt und verhältnismässig ist.

4.3.2 Insbesondere die Geolokalisierung

Vorgaben

Zu den Vorgaben für das Bearbeiten von Personendaten vgl. oben Ziff. 4.1.

Feststellung

Das Fahrzeug bietet zum einen die Möglichkeit, dass der Fahrzeugstandort identifiziert wird. Dazu bietet die Herstellerin eine **mobile Anwendung** (App) an, die aber vom Fahrzeughalter aktiviert werden muss. Nach Angaben der Herstellerin werden Standortinformationen von ihr nicht gespeichert. Sie stellt nur die Verbindung zwischen der Anwendung und dem Fahrzeug her.

Zum andern können über das **Navigationssystem** des Fahrzeugs Routen berechnet und abgefahren werden. Dazu wird der Kartenservice von Google Maps genutzt. Nach den Angaben der Fahrzeugherstellerin erhält Google Maps beim Abruf von Kartenmaterial aber jeweils nicht die einzelne Fahrzeugidentifikation, sondern eine IP-Adresse, die sich das Fahrzeug mit andern Tesla-Fahrzeugen teilt. Somit sei eine Identifikation des Fahrzeugs und seiner Insassen durch den Dienstleistungsanbieter Google nicht möglich.

Das Fahrzeug bietet auch die Option, dass Strassenabschnittsdaten («road segment data») der Herstellerin bzw. Drittanbietern zur Verfügung gestellt werden. Damit werden in anonymisierter Form Informationen zu den Strassen- und Verkehrsverhältnissen erhoben und Anbietern zur Verfügung gestellt, die eine angepasste Navigation für Fahrzeuge zur Verfügung stellen. Diese Funktion ist für Fahrzeuge, die in der Schweiz vertrieben werden, ab Betrieb deaktiviert und kann über die Einstellung im Fahrzeug gesteuert werden. Die Strassenabschnittsdaten wären auch nicht zur Fahrzeugidentifizierungsnummer zuordenbar, sondern werden für jede Fahrt mit einem zufälligen Identifikator ausgestattet.

Diese Anwendungen sind datenschutzrechtlich nur relevant, wenn die Daten einen Personenbezug aufweisen. Das darf in Bezug auf die Herstellerin und die Dienstanbieter ausgeschlossen werden. Somit erübrigt sich diesbezüglich eine Empfehlung.

Für die Kantonspolizei sind auch die Standortdaten bestimmten Personen zuordenbar, weil sie aufgrund der Einsatzplanung bzw. Einsatzleitung weiss, wer ihrer Mitarbeitenden als Fahrerin oder Fahrer oder als weitere Teammitglieder eingeteilt ist. Den Fahrzeugstandort besitzt sie abgesehen davon schon heute, weil etwa die Position der (Alarmpikett-)Fahrzeuge in der Einsatzzentrale angezeigt wird.

Empfehlungen

Der Datenschutzbeauftragte empfiehlt:

E7 die Erfassung und Übermittlung von Strassenabschnittsdaten nicht zu aktivieren.

Für die allfällig personenbezogene Verwendung von Geolokalisierungsdaten durch die Kantonspolizei siehe Empfehlungen E5 und E6.

4.4 Wesentliche Weiterentwicklungen der Hard- und Software

Feststellungen

Die Ausführungen in diesem Bericht beziehen sich auf die Fahrzeuge in der bestehenden Konfiguration. Es ist dafür zu sorgen, dass Änderungen in der Konfiguration der Hard- und Software auf ihre datenschutzrechtliche Relevanz überprüft und gegebenenfalls dem Datenschutzbeauftragten zur Vorabkontrolle vorgelegt werden.

Empfehlungen

Der Datenschutzbeauftragte empfiehlt:

E8 wesentliche datenschutzrechtlich relevante Änderungen der Hardware-/Software-Konfiguration erneut dem Datenschutzbeauftragten zur Vorabkontrolle vorzulegen.

4.5 Weitere Alarmpikettfahrzeuge Tesla

Die Ausführungen in diesem Bericht beziehen sich auf die drei bereits ausgelieferten Fahrzeuge in der bestehenden Konfiguration. Vier der sieben bestellten Fahrzeuge werden erst nach Abschluss dieser Vorabkontrolle geliefert.

Alle Empfehlungen gelten auch für die noch zu liefernden vier weiteren Fahrzeuge.

5 Verteiler

Der vorliegende Bericht wird der Kantonspolizei in zwei Originalen zugestellt.

Datum: 26. April 2019

Unterschriften:

sig. Beat Rudin
Datenschutzbeauftragter

sig. Katja Gysin
Stellvertretende Datenschutzbeauftragte