External

Anlage 7 zum DSFA-Bericht:

Vorbericht zur Anpassung der DSFA-Risikomatrizen (Anlage 3 – 5 zum DSFA-Bericht) für die Version 1.5

A. Inhalt

B. Vorwort

Der guten fachlichen Praxis folgend, wonach eine DSFA kontinuierlich überprüft und regelmäßig erneuert werden sollte, wurden in der als besonders kritisch betrachteten Anfangsphase vom DSFA-Team der SAP/T überprüft, ob weitere Datenschutzrisiken identifiziert werden können und müssen bzw. eine Neubewertung vorzunehmen ist oder Gegenmaßnahmen anzupassen sind.

Betrachtet wird der Zeitraum vom Go-Life der CWA-App bis zum 15. Oktober 2020. Die Ergebnisse wurden für die Version 1.5 vorgelegt, die Risikomatrizen wurden – soweit erforderlich – ergänzt und angepasst.

Dieser Vorbericht dient zum einen der Dokumentation, der bis zum 15. Oktober 2020 durchgeführten Maßnahmen. Zum anderen wird aufgezeigt, wie die Risikomatrizen angepasst wurden, um eine Nachvollziehbarkeit zu ermöglichen. Die Erkenntnisse aus diesem Bericht sind bereits in den Risikomatrizen umgesetzt.

C. Prüfung der DSFA

I. Betroffenengruppen

Die Risikoanalyse berücksichtigt nicht nur potentielle Schäden für CWA-Nutzer, vielmehr auch Nutzer einer anderen nationalen Corona-App, Personen im Umfeld (Haushaltsangehörige, z.B.), aber auch weitere Personen, die von Falschmeldungen betroffen sein können und sich etwa freiwillig in Quarantäne begeben oder nicht von ihren Grundfreiheiten Gebrauch machen.

In Spalte F der Risikomatrizen ist angelegt, dass die Risiken, für verschiedene Betroffenengruppen differenziert betrachtet und unterschiedliche Gegenmaßnahmen abgeleitet werden können.

Soweit in der Spalte F keine Einträge erfolgten, wurden sämtliche Betroffenengruppen in die Analyse einbezogen.

In den hier beschriebenen Folgenabschätzungen wurde auf eine Differenzierung nach Betroffenengruppen verzichtet.

II. Informationsbeschaffung/Informationsquellen

Um mögliche weitere Datenschutzrisiken zu identifizieren, wurden etwa Kommentare auf Github.com, öffentliche Äußerungen von Betroffenen sowie Stellungnahmen von interessierten Organisationen, (insbesondere die Stellungnahme der FifF) und Erkenntnisse aus dem IT-Sicherheits-Stream, den stattgefundenen Threat Modelling - Workshops bzw. aus den Abstimmungen mit CISPA [1] an das DSFA-Team adressiert und dort diskutiert. Auch wurde analysiert, ob sich durch die im Netz verfügbaren BigData-Analysen Datenschutzrisiken ergeben.

Die Pressemitteilung des LfDI Baden-Württemberg vom 09.10.2020 zum Thema „Contact-Tracing-Apps: Google späht Anwender aus!“ (https://www.baden-wuerttemberg.datenschutz.de/contact-tracing-apps-google-spaeht-anwender-aus/) wurde zum Anlass genommen, die mit dem ENF bzw. den Providern Google/ Apple zusammenhängenden Risiken zu überprüfen und eine Erklärung von Google einzuholen.

III. Prüfung potenzieller Datenschutzrisiken

1. Berichtszeitraum 15.06.2020 bis 23.07.2020

Im Berichtszeitraum bis zum 23.07.2020 wurden folgende Ereignisse auf ihr Bedrohungspotential hin geprüft:

- ENF-Nachbau
  - Re-Identifizierung durch Auswertung der Positivschlüsselpakete (nach Maßnahmen) mithilfe von Einzel-Apps
  - Re-Identifizierung durch Auswertung der Positivschlüsselpakete (nach Maßnahmen) mithilfe von Mashed Apps

[1] Das CISPA Helmholtz-Zentrum für Informationssicherheit ist eine nationale Forschungseinrichtung des Bundes innerhalb der Helmholtz-Gemeinschaft (LINK zu CISPA: https://cispa.de/de).

1.1. ENF-Nachbau

1.1.1 Beschreibung des Risikos

Die freie und transparente Verfügbarkeit der Positivschlüssel (Tagesschlüssel der infizierten Benutzer) erlaubt jeder Person das Herunterladen und die Analyse der Schlüssel. Aufgrund der "Tracing"- und nicht "Tracking"-Funktionalität der CWA, enthalten die Positivschlüssel keine Standortdaten und auch das CWA Backend verarbeitet keinerlei Ortungsinformationen aus dem Smartphone/der App.

Es ist möglich, außerhalb der App aus den Positivschlüsseln (die aller 10 Minuten geändert und) gesendeten kurzlebigen Zufalls-IDs (RPI) abzuleiten. Dadurch, dass die RPIs über die Bluetooth-Schnittstelle gesendet werden und damit im öffentlichen Raum empfangen werden können, ist es möglich diese abzuhören und mithilfe anderer Informationen aus anderen Quellen (z.B. Ortungsinformationen oder Videoaufnahmen) anzureichern und zu speichern.

Der letzte Schritt besteht darin, die Positivschlüssel aus dem Backend herunterzuladen und die abgeleiteten RPIs mit den abgefangenen, gespeicherten RPIs zu vergleichen. Mithilfe der angereicherten Informationen, ist ein Angreifer in der Lage, weitere Informationen über den Infizierten abzuleiten (z.B. den tatsächlichen Kontaktort mit der infizierten Person oder eine vollständige De-Anonymisierung des Infizierten).

Das Risiko wird in zwei verschiedene Subrisiken aufgeteilt und betrachtet: Nachbau des ENF mit Einzel-App oder mit "Mashed up" App:

- Einzel App (nur lokaler Einsatz): Der Angreifer hat ein Bluetooth-Sniffer und kann die empfangenen RPIs mit Ortungsinformationen anreichern. Damit sind einzelne Angreifer in der Lage, zu sehen wo und um wieviel Uhr Kontakt mit einer infizierten Person stattgefunden hat. Eine andere Variante besteht daraus, ein Bluetooth-Sniffer und eine Kamera an der Haustür zu verstecken. So könnte man erraten, welche von den Nachbarn oder Hausbesuchern infiziert wurde.

- Mashed up (flächendeckender Einsatz): In diesem Fall wird davon ausgegangen, dass ein flächendeckendes Überwachungssystem eingesetzt wird, um die Bevölkerung auszuspionieren, das mindestens aus Bluetooth-Sniffern und Kameras besteht. So könnte jeder Positivschlüssel nachträglich einer Person zugeordnet werden.

1.1.2 Risikoerfassung und Bewertung

In den Zeilen 52, 53 der Risikomatrix VT_1_2_4 werden diese Risiken neu erfasst. In einem Termin am 17.07.2020 hat das DSFA – Team unter Beteiligung von Fachleuten aus dem Bereich der Entwicklung Eintrittswahrscheinlichkeit und Schadenshöhe bewertet.

1.1.3 Risikobehandlung/mögliche Gegenmaßnahmen/Restrisikobewertung

Im Termin am 17.07.2020 wurden die Eintrittswahrscheinlichkeit, mögliche Gegenmaßnahmen und die Bewertung des Restrisikos diskutiert.

Die Eintrittswahrscheinlichkeit für die Variante „Mashed up“ wurde durch das DSFA-Team als „gering/vernachlässigbar“ eingestuft. Der Aufwand des flächendeckenden Einsatzes von Bluetooth-Sniffern unter der gleichzeitigen Anwendung von Kameras und der Ortungserfassung ist sehr hoch. Über die entsprechenden Mittel verfügen nur sehr wenige Staaten, Organisationen oder Firmen.

Die Eintrittswahrscheinlichkeit für die Variante „Einzel App“ (für den lokalen Einsatz) ist nach der Einschätzung des DSFA-Teams „hoch/wesentlich“, weil der ENF Nachbau durch den auf Github veröffentlichten Programmcode schon für einen durchschnittlichen Informatiker möglich ist. Der Einsatz einer solcher App würde sich insbesondere auf die Schutzziele Datenminimierung und Nichtverkettung wesentlich auswirken. In der Praxis hatte sich diese Gefahr bereits durch die sog. „Späher App“ realisiert. Jedoch wurde die App von Google zeitnah aus dem Play Store entfernt. Es ist davon auszugehen, dass Google auch zukünftig entsprechende Gegenmaßnahmen treffen wird. Das Apple App Store lässt schon aufgrund seiner Nutzungsbedingungen keine sog. Sniffer-Apps zu (Apps, die Bluetooth-Signale sniffen). Eine weitere Gegenmaßnahme wäre, den Zugriff auf die Positivschlüssel auf autorisierte Geräte zu beschränken. Wenn der Zugriff auf die Positivschlüssel auf autorisierte Geräte beschränkt wäre, müsste allerdings für die Autorisierung auf Google- und Apple-Dienste wie Safety Net Attestation oder Device Check zurückgegriffen werden. Diese Dienste sind noch nicht ausgereift und würden die Komplexität der App erhöhen. Zudem bestünde eine noch höhere Abhängigkeit gegenüber Google und Apple.

Aus diesen Gründen verbleibt für die Variante „Mashed up“ das Restrisiko „3“ (grün) und für die Variante „Einzel App“ das Restrisiko „9“ (gelb).

1.2 Re-Identifizierung durch Auswertung der Positivschlüsselpakete

Das RKI hatte vorgegeben, dass die Größe der Positiv-Schlüsselpakete mindestens 140 Keys enthalten muss. Damit sollte erreicht werden, dass die Keys von 10 Personen übermittelt werden, um eine Re-Identifizierung zu erschweren. Diese Größe konnte in der Anfangszeit (14 Tage nach Go-Live) nicht erreicht werden. Um die Größe der Positiv-Schlüsselpakete zu erreichen, wurde nach Durchführung eines Threat-Modelling Workshops entschieden, dass die Pakete im CWA-Server mit fingierten Positivschlüsseln (sog. Dummyschlüssel) aufgefüllt werden. Jeder erfolgreich hochgeladene Positivschlüssel wird zusätzlich N-1 mal dupliziert. Für die Kopien werden dieselben Metadaten (Transmission Risk Level, Rolling Start Interval Number, Rolling Period) verwendet. Nur die Key Data, die zufällig generiert wird, wird ausgetauscht. Damit geht jeder einzelne Key in einer Menge von N Keys unter (1 echter Positivschlüssel + N-1 Positivschlüssel). Der eine echte Key unter den N Keys lässt sich nicht identifizieren, da das einzige Unterscheidungsmerkmal die Key Data ist, welche bereits inhärent zufällig ist. Der Parameter N ist konfigurierbar und kann über die Zeit der aktuellen Situation angepasst werden. Siehe auch die DSK_CWA_Server_v1.5, Kap. 5.3.10, Tabelle 22: Dummyschlüssel Erzeugung).

Bei der Umsetzung, insbesondere den folgenden, veröffentlichten statistischen Auswertungen, zeigte sich, dass die Methode eine Re-Identifizierung nicht verhindern kann.

Das entsprechende Risiko ist in Zeile 47 dokumentiert. Das Restrisiko für die Rechte der Betroffenen in Folge Re-Identifizierung nach Auswertung wird mit „gelb“ bewertet. In der Folgezeit wurde die Entwicklung weiter beobachtet. Auch wurde seitens SAP/ T eingeschätzt, dass das Risiko durch den zusätzlichen Parameter Symptombeginn noch steigen könnte, weil dieser eine Gruppierung der Nutzer ermöglicht. Daher wurde eine Empfehlung an das RKI erarbeitet, auf die Dummy-Schlüssel-Erzeugung

zukünftig zu verzichten. Darüber hinaus ist die Anzahl der CWA-Diagnoseschlüssel gestiegen und steigt vermutlich durch die Anbindung des European Federation Gateway Service (EFGS) weiter an.

Daher wurde durch das RKI folgende Entscheidung getroffen und in der CWA umgesetzt:

Aktuell werden keine Dummyschlüssel erzeugt. Der Konfigurationsparameter ist daher aktuell auf den Wert 1 gesetzt worden. In Abhängigkeit vom Infektionsgeschehen kann diese Konfiguration aber geändert werden.

Damit wurden die Risiken der Re-Identifizierung durch SAP/ T auf „grün“ gesenkt (siehe Zeilen 48, 49) der Risikomatrix.

1.3 Review von Risiken

Im Termin am 17.07.2020 wurden weitere Bedrohungen der Risikomatrix VT_1_2_4 einem Review unterzogen, die Teilaspekte des o.g. Angriffs durch einen ENF – Nachbau betreffen.

Der Review führte nur in Zeile 105 zu einer Anpassung der Eintrittswahrscheinlichkeit. Die Eintrittswahrscheinlichkeit wurde von „2“ auf „3“ erhöht.

2. Berichtszeitraum 24.07.2020 – 12.10.2020

2.1 Risiken durch Laboranbindung

2.1.1 Hintergrund

Bisher ist die Übertragung der Testergebnisse nur über das BS Labortool Gateway möglich, wofür die Labore proprietäre Software benötigen.

Ergänzt wird das Labortool Gateway mit einer REST[2]-Schnittstelle (CWA Rest Service). Der CWA REST Service dient Laboren, die Coronatests durchführen, als Schnittstelle zum Test Result Server der Corona Warn App.

Dazu stell das REST-Service eine standardisierte Schnittstelle zur einfachen Anbindung von Laboren ohne proprietärer Laborsoftware zur Verfügung. Sie übertragen gehashte GUIDs mit den entsprechenden Testergebnissen an das CWA REST-Service, dieses leitet es über das Gateway weiter, welcher diese wiederum an den Test Result Server der Corona Warn App sendet.

2.1.2 Risikobewertung

In einem Workshop am 01.10.2020 wurden Risiken betrachtet, die mit der Anbindung einer solchen Schnittstelle verbunden sind. Durch das DSFA-Team wurden IT-Sicherheitsmaßnahmen nicht geprüft, vielmehr wurde auf die Aussagen und Dokumentationen zur Systembeschreibung der Schnittstelle vertraut. Ein Penetrationstest wurde durchgeführt, um die IT-Sicherheit der Schnittstelle und der Laboranbindung zu prüfen. Das Ergebnis liegt aktuell noch nicht vor.

[2] REST: Representational State Transfer

Die untersuchten Risiken, deren Bewertung und ergriffene Gegenmaßnahmen sind in der Risikomatrix VT_3 (Testing_inkl. Laborschnittstelle) dokumentiert. Es handelt sich um die Zeilen 11, 16, 24, 25, 31, 34, 35, 37, 38, 40, 42, 43, 44, 45, 48.

Neue „Hohe Restrisiken“ wurden nicht ermittelt.

Ein „gelbes“ Restrisiko wird aktuell insbesondere für Denial of Service Angriffe gesehen, durch ungesicherten Einsatz der Schnittstelle in den einzelnen Laboren, die unbefugten Dritten Zugang erlaubt und ermöglicht, unrichtige Daten an das Gateway zu übertragen (Zeile 43). Dieses Restrisiko kann nicht durch technische Maßnahmen seitens des Service Providers minimiert werden, vielmehr benötigt es hier die verantwortungsvolle und wachsame Nutzung seitens der Labore.

2.2 Review von Risiken im Zeitraum 07.10.2020 – 12.10.2020

Im genannten Zeitraum wurden die Risikomatrizen einem Review unterzogen.

2.1.1 Anforderung des RKI

Auf Anforderung des RKI wurden in der 41. KW die im DSFA – Bericht beschriebenen Risiko (cluster) überprüft. Im Ergebnis der Prüfung wurden die Risikoeinschätzungen nicht verändert, insbesondere nicht reduziert. Auch wenn sich die Risiken für die von der Datenverarbeitung Betroffen seit GoLive der App noch nicht realisiert haben, wird nicht davon ausgegangen, dass dies bereits ein hinreichender Zeitraum ist, um Eintrittswahrscheinlichkeiten zu senken. Üblicherweise wird hierfür ein Referenzrahmen von einem Jahr betrachtet. Sollten sich die Risiken innerhalb eines Jahres nicht verwirklichen, könnte eine Reduzierung aufgrund von belastbaren Erfahrungswerten erfolgen.

2.1.2 Überprüfung anhand der Dokumentation von dokumentierten Risiken im DSK Rahmenkonzept V 1.3

Eine Gegenüberstellung mit den im DSK Rahmenkonzept Version 1.3 beschriebenen Risiken und Restrisiken führte zu folgenden Anpassungen:

a. Risikomatrix VT_1_2_4 (VT 1: App-seitige Verarbeitung Kontaktereignisse/ VT2: Kontaktfall/ VT: 4: Infektfall)

- teilweise Anpassungen in Spalte T (etablierte Maßnahmen) und Aufnahme von Verweisen auf die jeweiligen Kapitel des DSK Rahmenkonzeptes v1.3,

- in Zeile 134 (neu) wurde das Risiko durch technische Grenzen des ENF spezifiziert. Technische Grenzen des ENF bzgl. Backup und Restore werden in Zeile 135 (neu) extra betrachtet.

- Das Risiko in Zeile 135 (neu) wird als mitigiert betrachtet und dies entsprechend dokumentiert, da die CWA vom Backup ausgenommen wird (siehe auch Zeile 135, Spalte T).

b. Risikomatrix VT_3 (Testing)

- keine.

c. Risikomatrix VT_Verifikations_Hotline

- keine.

2.3 Erfassung und Bewertung von Risiken infolge der EFGS-Anbindung

2.3.1. Methode

Als Risikomatrix „Anlage 6_2020-10-15_EFGSv1.4_Risikomatrix VT_5“ steht dem Auftraggeber die Matrix zur Verfügung, die im Rahmen der, die Entwicklung des EFGS begleiteten, DSFA erstellt wurde. Dort werden die Datenschutzrisiken für CWA-Nutzer betrachtet, die durch den Betrieb und die Nutzung des EFGS entstehen.

Risiken aus dieser EFGS-Risikomatrix, die speziell bei der Anbindung der CWA an das EFGS zu betrachten sind bzw. Risiken denen (nur) mit Maßnahmen durch die nationale CWA begegnet werden kann, sind ergänzend in die „Risikomatrix VT_1_2_4“ eingeflossen und werden als neue Version mit dem Namen „Anlage 3 Risikomatrix VT 1_2_4_CWAV1.5_mit_EFGS“ zur Verfügung gestellt. Es handelt sich dabei um folgende Zeilen: 5, 7, 15, 55 – 59, 75, 92 – 97, 109, 110, 121 – 123, 137 – 141, 157, 158, 165. In der Risikomatrix werden in Spalte D (Risiko/ Bedrohung) diese Risiken mit dem Zusatz „(EFGS-Risiko)“ versehen, um die Nachvollziehbarkeit zu erleichtern.

2.3.2. Einzelne Risikobewertungen

(1) Hervorzuheben sind die in den Zeilen 55 – 59 und 109 dokumentierten (Re-Identifizierungs-)risiken im Zusammenhang mit den „Country of Interest“. Diese Risiken entstehen bei der derzeit vorgesehenen Anbindung an das EFGS nicht, da eine Auswahl durch den CWA-Nutzer, mit welchen Ländern Schlüssel geteilt werden ebenso wenig erfolgt, wie eine Angabe von Ländern, für die sich der CWA – Nutzer interessiert.

(2) Darüber hinaus wird ein weiteres hoch eingestuftes Risiko bei der Anbindung des EFGS an die CWA mitigiert, welches dadurch entstehen kann, dass andere am EFGS beteiligte Staaten keinen vergleichbaren Verifikationsprozess haben, um sicherzustellen, dass keine Daten zu „falschen Positiven“ verarbeitet werden. Dieses Risiko und die Gegenmaßnahmen sind in Zeile 121 dokumentiert; das Risiko wird dadurch „grün“, dass der CWA Server nur Positivschlüssel an die CWA Apps verteilt, denen eine Attestierung durch ein Labor oder eine Testeinrichtung zugrunde liegt.

(3) Hohe Risiken

Datenverarbeitungen ohne Rechtsgrundlage mittels EFGS: Jede Art von nochmaligem Upload durch empfangende nationale Backends auf EFGS Server. Weitere und von der ursprünglichen Datenverarbeitung zu unterscheidender Datenverarbeitung, die von Rechtsgrundlage nicht umfasst wird.

→ Risiko-Matrix VT 1, 2, 4, dort Zeile 7 (neu)

Dieses Risiko wurde aus der Risikomatrix zum EFGS übernommen. Es stellt einen Spezialfall des Risikos dar, dass ein nationales Backend eines „joint controllers“ personenbezogene Daten ohne ausreichende Rechtsgrundlage hochlädt. Der CWA Server lädt vom EFGS heruntergeladene Schlüssel nicht erneut hoch.

Eine technische Mitigation dieses Risikos des Uploads durch andere nationale Backends könnte darin bestehen, dass der CWA Server im Rahmen der Paketierung der Diagnoseschlüssel den Parameter rolling_start_interval_number der Schlüssel überprüft und veraltete Schlüssel verwirft. Hierdurch würde das Risiko umgangen, Schlüssel zu verteilen, die nur auf Grund des Wiederhochladens noch im System nationale Backends und EFGS verarbeitet werden. Eine solche technische Lösung wurde bisher von den Verantwortlichen nicht weiter verfolgt. Vielmehr wurde von den joint controllern ein onboarding Prozess etabliert und sich gegenseitig ein gewisses Vertrauen entgegengebracht, dass eine Datenverarbeitung ohne Rechtsgrundlage nicht erfolgt. In Verfolgung des gemeinsamen Zwecks in gemeinsamer Verantwortung ist das Risiko akzeptabel.

Überlastung des mobilen Endgeräts des Nutzers auf Grund Herunterladens zu großer Datenpakete im Zusammenhang mit dem EFGS

→ Risiko-Matrix VT 1, 2, 4, dort Zeile 139 (neu)

Dieses Risiko wurde aus der Risikomatrix zum EFGS übernommen.

Die großen Volumina gehen auf eine Schätzung zu Beginn der Entwicklung des EFGS zurück. Belastbare Zahlen, die diese Schätzung korrigieren, liegen aktuell noch nicht vor. Wenn eine solche Überlastung beobachtet wird, könnte man dem mit einer europaweiten Umstellung auf das Traveller Pattern oder „Country of Interest“ (CoI) begegnen.

Das Risiko unterliegt daher einer regelmäßigen Überprüfung.

D. Weitere Anpassungen

In den Risikomatrizen wurden Rechtsschreibfehler korrigiert und die Bezugnahmen auf IDs der Designentscheidungen angepasst, soweit dies erforderlich war.

E. Änderungshistorie der Risikomatrizen

Überblicksartig werden nachfolgend die Änderungen in den Risikomatrizen für die DSFA v1.5 dargestellt.

Risikomatrix VT_1_2_4_CWAV1.5_mit_EFGS

Änderung			Beschreibung der Änderung	Freigabe des Berichts	Stadium
Nr.	Datum	Version			
1	16.06.2020	1.0	Finale Version 1.0		veröffentlicht
2	23.07.2020	1.2	Berichtigung von Rechtsschreibfehlern/ Ergänzung in Z 12, Spalte U, dass geplantes Popup – Fenster nicht in Version 1.2 .1.5 kommt/ Ersetzung der Bezeichnung (i)TEK durch Positivschlüssel/ Neuaufnahme der Risiken in Z 52, 53/	Zusammen mit Version 1.5	offen

			Farbliche Markierung (dunkelrot) der Risiken, die überprüft wurden/ Anpassung der Risikozahl in Z 115/ Übernahme von bisher fehlenden oder angepassten Bezügen zu Designentscheidungen		
3	08.10.2020	1.5	DSFA-Risikobewertung neu aufgenommener Risiken (Z 48, 49, 135)		offen
4	12.10.2020	1.5	Aus der Rikomatrix zur EFGS-DSFA übernommene Risiken (Z 5, 7, 15, 55-59, 75, 92-97, 109,110, 121-123, 137-141, 157, 158, 165)		offen
5	12.10.2020	1.5	Neuaufnahme des Risikos durch Änderung der Risikoermittlung im ENF (Z 31)		

Risikomatrix VT_3 (Testing, inklusive Laboranbindung)

Änderung			Beschreibung der Änderung	Freigabe des Berichts	Stadium
Nr.	Datum	Version			
1	16.06.2020	1.0	Finale Version		veröffentlicht
2	23.07.2020	1.2	Berichtigung von Rechtsschreibfehlern	Zusammen mit V 1.5	offen
3	08.10.2020	1.5	Neuaufnahme von Risiken durch Laboranbindung (Z 11, 16, 24, 25, 31, 34, 35, 37, 38, 40, 42, 43, 44, 45, 48)		offen

Risikomatrix VT_Verifikations_Hotline

Änderung			Beschreibung der Änderung	Freigabe des Berichts	Stadium
Nr.	Datum	Version			
1	16.06.2020	1.0	Finale Version		Veröffentlicht
2	23.07.2020	1.2	Berichtigung von Rechtsschreibfehlern// Anpassung Z 5 (Einwilligung als RG notwendig)	Zusammen mit V 1.5	
3	08.10.2020	1.5	Review der Risiken (Abgleich mit DSK_Rahmenkonzept V1.3)		