Datenschutz-Folgenabschätzung (DSFA)

„JKU Face Recognition Experiment“: Automatisierte Türentsperrung

I. Vorprüfung, ob die Durchführung einer DSFA erforderlich ist

1. Whitelist/Blacklist

Tatbestände der **Whitelist** gemäß Art 35 Abs. 5 DSGVO iVm. DSFA-AV, die ein Unterbleiben der DSFA rechtfertigen würden, sind nach Einschätzung der Verantwortlichen nicht erfüllt. Hingegen können die gegenständlichen Verarbeitungsvorgänge (siehe sogleich unten) eventuell unter Art 35 Abs. 4 DSGVO iVm. § 2 Abs. 2 DSFA-V Kriterium Ziffer 3 der **Blacklist** subsumiert werden, sodass grundsätzlich von einer Verpflichtung zur Durchführung der DSFA auszugehen ist; in § 2 Abs. 3 DSFA-V wird lediglich das Kriterium der Ziffer 4 („Verarbeitung von Daten schutzbedürftiger betroffener Personen“ hier: Arbeitnehmer*innen) erfüllt, jedoch fehlt ein weiteres Kriterium, um eine DSFA-Pflicht auch nach dieser Bestimmung auszulösen. Doch selbst, wenn sich die gegenständliche Datenverarbeitung nicht in der **Blacklist** finden würde, wäre von einer DSFA-Pflicht der Verantwortlichen – wie nachfolgend aufgezeigt - auszugehen.

2. Regelbeispiele nach Art 35 Abs. 3 DSGVO

In Bezug auf Art 35 Abs. 3 lit. c DSGVO gilt, dass sich eine „systematische umfangreiche Überwachung“ u.a. aus der Menge der personenbezogenen Daten und der Zahl der betroffenen Personen ergibt; darüber hinaus ist auch die Intensität der Datenverarbeitung ein taugliches Kriterium. Da bei der gegenständlichen Datenverarbeitung nicht ausgeschlossen werden kann, dass in Einzelfällen uU eine größere Anzahl von Personen (im Laufe des Projektes in Summe grob geschätzt einige hundert) betreffen sein könnte, kann dieser Tatbestand zumindest nicht ausgeschlossen werden, weshalb sich die Pflicht zur Durchführung der DSFA auch aus Art 35 Abs. 3 lit. c DSGVO ergibt. Da eine Auswertung der Bilder nach biometrischen Merkmalen der betroffenen Personen erfolgt, wäre u.U. auch Art 35 Abs. 3 lit. b DSGVO erfüllt.

3. Generalklausel nach Art 35 Abs. 1 DSGVO

Aufgrund der **Art** (hier: besondere Datenkategorien und Videodaten) und des **Zweckes** (hier: Videoüberwachung) der Verarbeitung würde selbst bei Verneinung der obigen Tatbestände uU eine Risikoanalyse im Vorfeld (Vorprüfung) bereits ergeben, dass durch die geplante Datenverarbeitung ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen bestehen könnte.

4. Leitlinien der Art-29-Datenschutzgruppe

Ein Rückgriff auf die Leitlinien der Art-29-Datenschutzgruppe wäre demnach nicht erforderlich, jedoch kann der Vollständigkeit halber auch darauf verwiesen werden, zumal auch dort mindestens vier Kriterien (wobei nur zwei erforderlich wären) erfüllt werden:

Kriterium 3 (Systematische Überwachung): Liegt vor, da ein größerer Bereich vor den Büros des Instituts permanent videoüberwacht wird.

Kriterium 4 (Verarbeitung besonderer Kategorien von personenbezogenen Daten, strafrechtlich relevanten Daten oder vertraulichen oder höchstpersönlichen Daten: Liegt vor, da eine Auswertung von Bildern nach biometrischen Merkmalen erfolgt.

Kriterium 5 (Datenverarbeitung in großem Umfang): Liegt, wie unter Punkt **1.** dargetan, vor bzw. kann dieses Kriterium nicht ausgeschlossen werden.

Kriterium 7 (Daten von schutzbedürftigen Personen): Liegt vor, da Daten insbesondere von Mitarbeiter*innen der Verantwortlichen verarbeitet werden; von diesem Kriterium sind grundsätzlich alle Personengruppen erfasst, wo ein Machtungleichgewicht zwischen der betroffenen Person und dem Verantwortlichen festgestellt werden kann.

Kriterium 8 (Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen): Liegt vor, da die automatische Türentsperrung eine neue Anwendung darstellt und auch organisatorische Aspekte umfasst.

5. Fazit

Im Ergebnis kann daher festgehalten werden, dass die Verantwortliche zur Durchführung einer DSFA im Rahmen des obigen Forschungsprojektes verpflichtet ist.

II. Systematische Beschreibung der Verarbeitungsvorgänge und ihrer Zwecke (Art 35 Abs. 7 lit. a DSGVO)

1. Betroffene Personengruppen

Bei den Mitwirkenden handelt es sich um Mitarbeiter*innen des Instituts für Netzwerke und Sicherheit, welche freiwillig am Projekt teilnehmen. Von diesen werden spezifische Daten für diese Verarbeitungen erhoben und gespeichert.

Sonstige Betroffene sind alle Personen, welche sich in dem (öffentlich zugänglichen) Bereich aufhalten bzw. diesen betreten, in dem die Videoüberwachung stattfindet. Hier ist eine Eingrenzung der Personen nicht möglich. Entsprechende Hinweisschilder werden angebracht.

2. Datenkategorien und Art der Verarbeitung

2.1. An personenbezogenen Daten werden *erhoben*:

a. Bilddaten, Identität und biometrische Merkmale der Mitwirkenden am Forschungsprojekt: Von den Personen, welche durch die Kameras erkannt werden sollen, wird ihre Mitarbeiternummer abgefragt, sowie das Aussehen (Gesicht) erfasst und biometrische Merkmale daraus extrahiert.
b. Bilddaten und biometrische Merkmale der Betroffenen: Sowohl von registrierten Personen (= Mitwirkende am Forschungsprojekt) als auch Dritten (welche mit den bekannten Personen verglichen werden, die aber ansonsten nicht identifiziert werden) werden Bilder aufgenommen und aus diesen biometrische Merkmale zum sofort anschließenden Vergleich extrahiert.

c. Ort, Datum und Zeit der Erhebung: Dies ist u.U. für die Erkennung der Intention der Person erforderlich.
d. Rolle der Mitwirkenden: Zugangsberechtigt für bestimmte Türen oder nicht.
e. Absicht der Mitwirkenden: Ob und ggf. welche Tür als Ziel erkannt wurde oder „Unbekannt“

2.2. An personenbezogenen Daten werden *gespeichert*:

a. Bilddaten, Identität, biometrische Merkmale sowie Rolle (=Zugangsberechtigungen) der Mitwirkenden am Forschungsprojekt (siehe oben). Speicherdauer: 1 Jahr nach Projektende

b. Für jede *als Mitwirkende* erkannte Person mit dem Ziel einer „überwachten“ Tür:

• Bilddaten: 5-Sekunden-Film zum Erkennungszeitpunkt und Standbild. Speicherdauer: Auswertung bzw maximal 2 Monate (mit Ausnahme ausgewählter Exemplare für Publikationen)

• Ort, Datum und Zeit des Erkennungszeitpunktes: Speicherdauer 1 Jahr nach Projektende

• Identität (=Mitarbeiternummer): Speicherdauer 1 Jahr nach Projektende.

• Erkannte Bewegungsintention: Speicherdauer 1 Jahr nach Projektende

c. Für jede *als Mitwirkende* erkannte Person ohne dem Ziel einer „überwachten“ Tür bzw. ohne Erkennung des Ziels: Es erfolgt keine Speicherung, sondern die Daten werden unmittelbar nach dem (negativen) Intentionsergebnis gelöscht.

d. Für alle Personen, deren Daten erhoben wurden (siehe oben), die jedoch *nicht als Mitwirkende* erkannt wurden: Es erfolgt keine Speicherung, sondern die Daten werden unmittelbar nach dem (negativen) biometrischen Vergleich gelöscht.

3. Datenquellen

Die Daten werden einerseits durch Videokameras erhoben (Mitwirkende und sonstige Betroffene), andererseits direkt bei den Mitwirkenden durch deren Registrierung.

Zur Lage der Kameras siehe die Skizzen im Anhang.

4. Datenempfänger

Die werden nicht an Dritte weitergegeben, sondern werden nur den für die entsprechende Abwicklung notwendigen Mitarbeiter*innen des Instituts für Netzwerke und Sicherheit zugänglich gemacht.

5. Rechtsgrundlage

Rechtsgrundlage für die konkrete Verarbeitung der personenbezogenen Daten ist Art. 6 Abs. 1 lit. e und Abs. 2 sowie Art 9 Abs. 2 lit. j DSGVO iVm. § 7 Abs. 3 DSG.

Die Verarbeitung der personenbezogenen Daten zu nachstehendem Zwecken wurde gemäß § 7 Abs. 3 DSG mit Bescheid der Datenschutzbehörde vom 28.4.2021, DSB D202.282 2021-0.286.289 im für das Forschungsprojekt notwendigen Ausmaß und unter Erteilung von Auflagen genehmigt.

6. Zweck

Zweck des Projekts ist die Feststellung der Zuverlässigkeit von Gesichtserkennung und einer sicheren Integration mit einem Schließsystem auf eine datenschutzfreundliche Weise, d.h. mittels persönlicher Agenten unter der Kontrolle der jeweiligen Person anstatt eines zentralen Servers. Weiters wird versucht zu erkennen, ob die Person lediglich vorbeigehen wird (oder einen anderen Raum betritt) oder tatsächlich den betroffenen Raum betreten möchte (Intentionserkennung). Schlussendlich soll festgestellt werden, ob/wie ein sicherer Nachweis der tatsächlichen Verarbeitungsvorgänge der personenbezogenen Daten allgemein zur Verfügung gestellt werden kann (Web-Anwendung/App, Zugriff typ. per Smartphone).

7. Verarbeitungsanlagen

7.1. Ein Ziel des Projektes ist es, die Verarbeitung der Daten möglichst nahe an den Kameras durchzuführen: Eine zentrale und physisch sehr stark abgesicherte Verarbeitung ist daher prinzipiell unmöglich. Dennoch werden angemessene Sicherheitsmaßnahmen getroffen, indem die Mini-PCs zur Bildverarbeitung mit Festplattenverschlüsselung und starken elektronischen Sicherheitsmaßnahmen ausgestattet werden (Passwörter, Host-basierte Firewalls etc.). Weiters sind diese Geräte in einem separaten virtuellen Subnetz (VLAN) untergebracht, sodass ein Zugriff von „normalen“ Geräten (bzw. offenen Netzwerk-Steckdosen) nicht möglich ist, sofern diese nicht explizit und individuell freigeschaltet werden – was ausschließlich für die Arbeitsplätze der für die Auswertung zuständigen Personen erfolgt. Da die Daten auf diesen Geräten ohnehin nur eine minimale Zeit lang gespeichert sind, wird dies als ausreichend angesehen.

7.2. Zusätzlich hierzu erfolgt die Speicherung der Videoaufzeichnungen/Standbilder/Protokolle (von erkannten Personen mit relevantem Ziel). Dies erfolgt auf einem virtuellen Server in demselben Subnetz, wobei die Videos automatisch auf sichere Weise (verschlüsselt) zur Speicherung dorthin übermittelt werden. Auch hier besitzen nur die damit befassten Personen Zugriffsrechte und können die Videos für die tatsächlichen Auswertungen auf ihre lokalen Arbeitsplatzgeräte herunterladen. Durch Richtlinien und Anweisungen ist sichergestellt, dass die Daten dort nur für tatsächliche Auswertung gelagert werden dürfen, nicht jedoch als separate Kopien. Letzteres dient insbesondere dazu sicherzustellen, dass die Löschung wie vorgesehen erfolgt.

8. Dienstleister und Mitverantwortliche

Die Einbindung von Dienstleistern oder weiteren Verantwortlichen ist nicht vorgesehen.

9. Übermittlung in Drittländer oder zu internationalen Organisationen

Dies ist nicht vorgesehen.

III. Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck (Art 35 Abs. 7 lit. b DSGVO)

1. Nähere Ausführungen zum Zweck

1.1. Festgelegter Zweck: Eine genauere Festlegung der Verarbeitungsvorgänge im Vorhinein ist im Hinblick darauf, dass es sich um ein Forschungsprojekt handelt, nicht möglich. Alle Verarbeitungen beschränken sich jedoch auf obigen Zweck, welcher im Laufe des Projektes nicht verändert, z.B. erweitert, werden soll.

1.2. Eindeutig: Eine Verarbeitung, die über die Identitätsfeststellung bzw. die Erkennung des Bewegungsziels hinausgeht, erfolgt keinesfalls. Der Zweck ist klar definiert und allgemein verständlich, sodass der dieser als „eindeutig“ anzusehen ist.

1.3. Legitimität: Ziel ist Erforschung einer „besseren“ Art der Gesichtserkennung; dies wurde auch bereits von der Datenschutzbehörde als im wichtigen öffentlichen Interesse liegend anerkannt.

1.4. Angemessenheit: Im Hinblick auf die für Dritte potentiell entstehenden Gefahren (unmittelbare Löschung; nur bei doppelt fehlerhafter Erkennung wird gespeichert und später manuell aussortiert; öffentlicher Bereich) liegt die Angemessenheit des Zweckes im Hinblick auf die Verarbeitung der Daten von Betroffenen und Mitwirkenden vor.

2. Erhebung von Daten

2.1. Bilddaten der Mitwirkenden: Ohne die Erhebung der Bilddaten ist eine Extraktion der biometrischen Merkmale für die Erkennung nicht möglich. Dies ist daher unabdingbar.

2.2. Identität der Mitwirkenden: Da je nach Person nur bestimmte Türen entsperrt werden dürfen, ist die Identität der Person erforderlich.

2.3. Biometrische Merkmale der Mitwirkenden: Diese werden aus den Bilddaten extrahiert und dienen dazu, die Person später wiederzuerkennen. Dies ist erforderlich, da Videoaufnahmen nie identisch sind, und daher ansonsten eine Wiedererkennung von Personen unmöglich ist.

2.4. Rolle der Mitwirkenden: Da an das Schließsystem nur weitergegeben wird, eine bestimmte Tür zu entsperren, ist die Liste der Türen, für welche eine Person berechtigt ist und die sich aufgrund ihrer Rolle ergibt, innerhalb des Systems notwendig.

2.5. Bilddaten sonstige Betroffener: Ohne der Aufnahme von Bildern ist kein Versuch, diese Personen zu erkennen, durchführbar.

2.6. Biometrische Merkmale sonstiger Betroffener: Wie erläutert, ist ein direkter Vergleich von Bildern nicht möglich, sodass zuerst die biometrischen Daten aus diesen extrahiert werden müssen, bevor ein Vergleich mit den Daten der Mitwirkenden stattfindet.

2.7. Ort, Datum und Zeit der Erhebung: Diese ergeben sich automatisch zusammen mit der Videoaufnahme, da die Bilder in einer bestimmten Kamera zu einem bestimmten Zeitpunkt entstehen. Diese Daten werden auch für die Protokollierung der Entsperrung benötigt.

2.8. Absicht der Mitwirkenden: Da nicht jedes Mal alle Türen, für welche eine Person berechtigt ist, entsperrt werden sollen, ist es notwendig festzustellen, welche Tür vermutlich das Ziel der Person ist, um diese gezielt zu entsperren.

3. Speicherung von Daten

3.1. Bilddaten der Mitwirkenden: Um verschiedene Algorithmen der Extraktion biometrischer Merkmale testen zu können, müssen auch die Basisdaten dieser Extraktion gespeichert werden.

3.2. Identität der Mitwirkenden: Das Projekt muss wissen, welche Personen Mitwirkende sind, und welche nicht. Dies ist auch für die Protokollierung der Entsperrung erforderlich.

3.3. Biometrische Merkmale der Mitwirkenden: Es ist nicht sinnvoll, diese jedes Mal zu berechnen, insbesondere, da dies bedeuten würde, den Kameras die tatsächlichen Bilder zu übermitteln. Dies ist eine Verbesserung des Datenschutzes, da sich zwar aus den Bildern die Merkmale berechnen lassen, nicht aber umgekehrt.

3.4. Rolle der Mitwirkenden: Um nur bestimmte Türen zu entsperren, sind die Berechtigungen der Personen hierfür zu speichern.

3.5. Videostream (5 Sekunden) bei Zielerkennung von Mitwirkenden: Dies ist erforderlich, um nachträglich die Qualität des Algorithmus überprüfen zu können, bzw um einen Vergleich mit einem anderen biometrischen Algorithmus zu ermöglichen. 5 Sekunden wird hier als verhältnismäßiger Zeitabschnitt gewählt, da ein Standbild uU nicht reicht (zB Drehungen des Kopfes), andererseits entspricht dies ungefähr der Dauer, welche eine Person bei normaler Gehgeschwindigkeit im Aufnahmebereich verbringt. Damit wird es sehr unwahrscheinlich, unnötigerweise sonstige Personen bzw Aktivitäten außerhalb des gewünschten und ausgeschilderten Bereichs aufzunehmen. Ein Film anstatt mehrere Standbilder ist erforderlich, um die Algorithmen für die Zielerkennung prüfen zu können

3.6. Standbild bei Zielerkennung von Mitwirkenden: Für die Protokollierung und die Auswertung der biometrischen Algorithmen wird das Bild gespeichert, das für die biometrische Auswertung herangezogen wurde. Dies dient wiederum dem Vergleich verschiedener Algorithmen, sowie der Überprüfung von Falscherkennungen. Dies stellt kein zusätzliches datenschutzrechtliches Problem dar, da es sich um ein Standbild aus dem 5-Sekunden Film handelt.

3.7. Ort, Datum und Zeitpunkt der Zielerkennung von Mitwirkenden: Dies dient der Protokollierung der Aufsperrvorgänge sowie der Positionierung des Standbildes innerhalb des 5-Sekunden Films und ist daher notwendig.

3.8. Identität des Mitwirkenden bei Zielerkennung: Wird eine Person und zusätzlich ein Ziel erkannt, so muss dieses Faktum sowie die erfolgte Türentsperrung protokolliert werden. Die Identität ergibt sich aus den biometrischen Daten, könnte also aus dem Film/Standbild bzw. menschlicher Beobachtung jederzeit wiederhergestellt werden. Diese dient nur dem Vergleich und dem Entsperrprotokoll; eine Auswertung wer wann wo welche Räume betrat erfolgt nicht.

3.9. Erkanntes Ziel des Mitwirkenden bei Zielerkennung: Es muss protokolliert werden, wann welche Tür entsperrt wurde, was darauf beruht, welche Tür als Ziel der Bewegung erkannt werden konnte. Dies ist verglichen mit dem „normalen“ System sogar datenschutzfreundlicher, da das Türsystem hier nur den Entsperrbefehl erhält, aber keine Identität wie bei normaler Entsperrung mittels Keplercard. Weiters ergibt sich das Ziel typischerweise auch aus dem kurzen Video. „Besondere“ Türen, wie z.B.

Toiletten, werden nicht überwacht, sodass sich auch aus dem Ziel selbst keine besondere Information ergibt. Diese Daten werden auch nicht im Hinblick auf Arbeitszeiten ausgewertet oder an andere Stellen der Universität weitergegeben.

3.10. Alternative Methoden: Solche stehen nicht zur Verfügung, da gerade die Auswertung von biometrischen Daten auf datenschutzfreundliche Weise das Ziel der Forschung ist, und daher eine solche auch durchgeführt werden muss. Simulierte oder synthetische Bilder sind nicht geeignet, da diese die Realität in ihrer Vielfalt nicht ausreichend abbilden können und selbst in dieser eingeschränkten Version nur mit sehr hohem Aufwand herstellbar wären.

4. Speicherdauer

Die Speicherdauer kann nicht verkürzt werden, da zur Auswertung grundlegende Daten bis nach der Abrechnung der Förderungen zum Nachweis der durchgeführten Arbeiten erforderlich sind. Potentiell besonders problematische Daten, die Videoaufzeichnungen, sind davon jedoch nicht betroffen (Forschungsinhalte) und werden dementsprechend nur kürzer gespeichert. Da verschiedene Algorithmen ausprobiert werden müssen und dies nur bei einem längeren Zeitraum einen sinnvollen Vergleich zwischen diesen erlaubt, ist eine Verkürzung der Speicherung nicht möglich. Diese ist ohnehin bereits mit der Durchführung dieser Auswertungen begrenzt (wobei zusätzlich eine absolute Obergrenze von 2 Monaten festgelegt wurde: Urlaub/Ferien verhindern u.U. eine sofortige Bearbeitung).

IV. Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen (Art 35 Abs. 7 lit. c DSGVO)

1. Identifizierte Risiken für Mitwirkende bzw. sonstige Betroffene

1.1. Für Mitwirkende ergibt sich das potentielle Risiko, dass nicht nur die Universität nachvollziehen kann, wann sie welche Tür entsperrten, sondern dass dies auch Personen direkt am eigenen Institut, bzw. dem Vorgesetzten zugänglich wird. Da jedoch die meisten Mitwirkenden ohnehin einer Pflicht zur Aufzeichnung der Arbeitszeiten unterliegen, ist dies nur ein sehr geringes Risiko bzw. sind die Auswirkungen sehr gering: die Arbeitszeit (im Sinne physischer Anwesenheit im Büro) könnte genauer überwacht werden. Dies ist auch nicht das Ziel des Projektes und entsprechende Auswertungen sind nicht vorgesehen.

1.2. Der Eingang zur Damentoilette ist in einem kleinen Teil der Tür (im Bereich der Türangeln) im Blickfeld der Kamera des Szenarios 1 (Hintergrund – durch die geöffnete Türe). Da die Kamera nur dann eine Person aufnehmen kann, wenn die Tür zum Forensiklabor geöffnet wird und jemand eintritt, verdeckt diese Person teilweise den Toiletteneingang zusätzlich; allerdings nimmt die Kamera auch das Bild auf, wenn jemand den Raum betritt und die Tür geöffnet bleibt. Sollte daher währenddessen jemand die Toilette verlassen, wäre eine Falscherkennung zumindest möglich (kleines Gesicht im Hintergrund). Auch beim Betreten ist eine Erkennung möglich, indem die Person im Vorbeigehen erkannt wird und dann aus der Öffnung der Toilettentür auf das Betreten geschlossen wird (das eigentliche Eintreten ist nicht sichtbar). Eine Schwärzung ist in

diesem Szenario nicht möglich, da sich das Gesicht der zu erkennenden Person genau davor befinden kann. Aus der Größe/Position der Person ist jedoch eindeutig erkennbar, ob die Person in der Forensiklabor-Tür steht oder mehrere Meter weiter hinten. Eine Falscherkennung ist daher äußerst unwahrscheinlich und wird bei Entdeckung sofort mit allen Daten gelöscht. Eine Auswertung falscher Erkennungen erfolgt in keinem Fall. Daraus ließe sich uU herausfinden, ob eine Mitarbeiterin schwanger ist, bevor sie dies dem Arbeitgeber meldet.

1.3. Der Eingang zur Damentoilette ist potentiell im Blickfeld der Kamera des Szenarios 2. Der unmittelbare Bereich davon wird durch Schwärzung des Bildes in der Kamera unkenntlich gemacht. Da nicht zu erwarten ist, dass Damen ausschließlich knapp an der Wand im verdeckten Bereich entlangschleichen, um diese aufzusuchen, werden sie dennoch aufgenommen; aus dem Nicht-Betreten anderer Räume ist weiters das Ziel wahrscheinlich (könnte auch der Seminarraum sein) erschließbar, auch wenn das eigentliche Betreten nicht aufgenommen wird (aber ihr „verschwinden“). Daten nicht mitwirkender Personen werden ohnehin nicht gespeichert, sodass sich hier keine Probleme stellen, insbesondere, da eine Falsch-Identifizierung äußerst unwahrscheinlich ist. Allerdings werden sich unter den Mitwirkenden voraussichtlich auch Frauen befinden. Hier soll das Problem durch die Erkennung der Intention gelöst werden: Welche Tür wird „angesteuert“? Wird als Ziel die Toilette erkannt, so erfolgt keine Speicherung des Ereignisses (da keine überwachte Tür). Tatsächlich problematisch sind daher lediglich die Fälle, dass eine Person (fälschlicherweise) als Mitwirkende erkannt wird und (zusätzlich) die Intention fälschlicherweise als auf die entgegengesetzte Gangseite verweisend interpretiert wird (alle im Projekt überwachten Türen sind von der Kamera aus auf der linken Gangseite zu finden, die Damentoilette hingegen rechts). Der Gang ist zwar eine Sackgasse, doch kann nicht ausgeschlossen werden, dass sich Personen aus dem Seminarraum zur Toilette begeben. Aus der Position (=“nach“ der Tür) ist deshalb eine Erkennung des Ziels in diesem Fall voraussichtlich nicht möglich, doch da es keine Kamera in Richtung der Seminarraum-Tür gibt (die geplante zeigt von dieser weg; siehe Skizze), ist eine Personenerkennung fast ausgeschlossen. Dann verbliebe immer noch die Erkennung der Ziel-Seite des Gangs. Sollte trotz allem eine fehlerhafte Erkennung erfolgen, wird der Vorgang bei Entdeckung sofort mit allen Daten gelöscht. Eine Auswertung nach dieser Tür erfolgt in keinem Fall. Zu möglichen Auswirkungen siehe oben.

1.4. Der Eingang zum Seminarraum ist in Szenario 2 im Erkennungsbereich enthalten. Dieser wird sowohl für Besprechungen mehrerer Institute genützt, wie auch (je nach Corona-Lage) für Lehrveranstaltungen. Es ist daher mit einer Vielzahl an Personen zu rechnen, welche keine Mitwirkenden des Projektes sind. Dies stellt jedoch kein Problem dar, da es sich um keinen besonderen Raum und keine ungewöhnlichen Tätigkeiten (z.B. Rechtsberatung) handelt. Zusätzlich kann dieser Raum auch von der anderen Seite des Gebäudes, d.h. von einem anderen Gang ohne jegliche Videoüberwachung, aus betreten werden. Ähnliche Szenarien gelten für den Besprechungsraum, der auf den Skizzen nicht dargestellt ist, da er außerhalb des Bereichs liegt (Szenario 2: auf der Gangseite von

Seminarraum und Damentoilette, aber hinter einem Quergang gelegen in ca. doppelter Entfernung; Szenario 3: deutlich rechts von der Bibliothek und damit hinter der näher liegenden Kamera bzw wiederum sehr weit von der in diese Richtung zeigenden Kamera). Er wird zwar von den Kameras noch erfasst, aber Personen dort können aufgrund der geringen Bildgröße nicht mehr erkannt werden. Bei diesem ergeben sich daher keine Probleme. Eine potentielle Suwirkung wäre, dass die Universität feststellen könnte, wer wann mit wem eine Besprechung abgehalten hat, bzw im Falle von Studierenden, wer an einer LVA teilgenommen hat, bzw verspätet erschien oder früher ging. Dies wäre jedoch für den LVA-Leiter ebenfalls jederzeit erkennbar.

1.5. Der Eingang zum Netzwerklabor ist eine überwachte Tür, d.h. Mitwirkende werden dabei erkannt. Gleichzeitig handelt es sich hierbei um einen Raum, in dem Lehrveranstaltungen stattfinden. Studierende sind voraussichtlich keine Mitwirkenden, doch könnte eine derartige „Überwachung“ Befürchtungen hervorrufen, dass die Lehrveranstaltungs-Teilnahme visuell überwacht wird. Da es sich um ein Labor mit teurer Ausrüstung handelt, finden Lehrveranstaltungen ausschließlich in Anwesenheit von Institutsmitarbeiter*innen zu festgelegten Zeitpunkten statt, wobei eine Anwesenheitsliste geführt wird. Durch Information der Teilnehmer*innen (u.A. die Hinweisschilder), dem Fehlen einer Kamera im Laborinneren, sowie der Auswertung und Speicherung ausschließlich von Mitwirkenden bestehen hier keine Probleme. Auch hier wäre als Auswirkung möglich, die Teilnahme bzw -Anwesenheitsdauer von Studierenden zu überwachen.

2. Spezifische Risiken

2.1. Vertraulichkeit: Die Videoaufnahmen könnten öffentlich werden, sowohl als Live-Übertragung wie auch als Aufzeichnung (ebenso wie die 5-Sekunden Kurzaufzeichnungen). Direkter Zugriff auf die Kameras besteht nicht; diese sind unmittelbar mit dem Auswertungs-Computer verbunden, sodass von außen auf diese nicht zugegriffen werden kann. Die Auswertungs-Computer sind orientiert am Stand der Technik abgesichert, sodass ein Fremdzugriff darauf sehr unwahrscheinlich ist. Die 5-Sekunden Aufzeichnungen werden zentral auf einem gut abgesicherten virtuellen Server gespeichert. Alle Geräte sind in einem separaten VLAN untergebracht, welches durch eine Firewall vom restlichen Universitätsnetz bzw. dem Internet getrennt ist. Daraus könnte uU ein öffentliches peinliches Verhalten in größerem Umfang bekannt werden und dauerhaft zum Abruf im Internet bereitstehen. Da es sich um einen öffentlichen Raum handelt, ist aber gleicherweise damit zu rechnen, dass Personen mit einem Handy mitfilmen. Da es sich nur um sehr kurze Ausschnitte handelt und diese bei Betroffenen gar nicht gespeichert werden, ist das Bekanntwerden der Aufzeichnungen keine große Gefahr. Fremder Zugriff auf die Kameras, und damit Zugang zu den Videodaten, welche ansonsten nicht gespeichert werden, könnte eine Überwachung in größerem Ausmaß erlauben, sodass sowohl wieder eine Anwesenheitskontrolle (auch für nicht am Projekt Mitwirkende, welche in diesem Bereich ihr Büro haben), als auch für Dritte eingeschränkt möglich wäre.

2.2. Integrität: Die Integrität der Daten wird durch strikte Zugriffsregeln gesichert. Konkrete Probleme könnten jedoch durch nachträgliche Modifikationen entstehen: Da die Videos nur eine kurze Zeit gespeichert werden, könnte später die Identität einer Person, welche einen Raum betreten hat, unerkannt verändert werden. Dies erscheint wenig wahrscheinlich und relevant, weil es nur Personen betreffen kann, die ohnehin Zutritt zu diesem Raum besitzen, da ansonsten keine Entsperrung erfolgt worden wäre. Im Extremfall könnte damit ein Diebstahl in einem Büro einem anderen Mitarbeiter „unterschoben" werden, ohne dass zuvor die Keplercard gestohlen werden müsste. Ein anderer möglicher Angriff wäre es, z.B. sich selbst Entsperr-Rechte für Räume zu geben, welche man normalerweise nicht betreten darf. Im betroffenen Bereich befindet sich jedoch kein strikt abzusichernder Raum, sondern lediglich normale Arbeits-Büros bzw. allgemeine Räume (Beispiel Forensik-Labor: Instituts-Drucker). Das Büro von Prof. Mayrhofer ist z.B. auch über das Sekretariat betretbar, welches alle Mitarbeiter*innen betreten dürfen. Einzig relevant ist der Server-Raum, zu dem nur eine eingeschränkte Gruppe Zutritt besitzt. Doch selbst hier dürfte ein unbefugter Zutritt von Institutsmitarbeiter*innen (und nur solche sind Mitwirkende) keine wirkliche Gefahr darstellen. Dennoch wird jede Änderung der Zugriffsregeln protokolliert, sodass dies zumindest nachvollziehbar ist. Um Dritte von Änderungen abzuhalten werden Zugriffsberechtigungen und generelle Sicherheitsmaßnahmen gegen Hacking eingesetzt. Dies betrifft jedoch ausschließlich Mitwirkende am Projekt und keine der hier relevanten Betroffenen, da deren Daten nicht gespeichert werden und daher Veränderungen nicht vorkommen können.

2.3. Verfügbarkeit: Beschädigungen der Kameras bzw. Mini-PCs können nicht vermieden werden, da sich diese an öffentlichen Orten befinden. Ein vorübergehender Verlust stellt kein großes Problem dar, da die Türen weiterhin normal geöffnet werden können, und dann lediglich eine Zeit lang keine Daten für die Forschung vorhanden sind – durchgehende Vollständigkeit ist aber für diese kein Erfordernis. Bezüglich der sonstigen Daten wird auf übliche Backup-Strategien gesetzt, um diese zu erhalten. Dies hat keine Auswirkungen auf Betroffene, da keine Daten von diesen gespeichert werden.

2.4. Belastbarkeit: Die Computer hinter den Kameras sind so ausgelegt, dass sie die Bilder in Echtzeit verarbeiten können. Zusätzlich sind diese Systeme vom Rest des Instituts-Netzwerks (bzw. dem öffentlichen Internet) abgetrennt. Dies erhöht nicht nur die Sicherheit, sondern reduziert auch die Möglichkeiten für DoS Angriffe.

2.5. Datenminimierung: Dies wurde bereits oben dargestellt. Es werden keine Daten verarbeitet, die nicht für den Zweck erforderlich sind. Aufgrund der restriktiven Zugriffsberechtigungen und der Richtlinien und Vorgaben wäre es auch für Projektmitarbeiter*innen äußerst schwierig, heimlich zusätzliche Daten zu erheben oder speichern.

2.6. Nichtverkettung: Da keine Rohdaten an Dritte herausgegeben oder an andere Stellen der Universität weitergegeben werden, weder Videoaufnahmen noch biometrische Merkmale oder Erkennungs-/Entsperr-Logs, ist eine Verknüpfung mit anderen Daten nicht möglich. Für das Sperrsystem der Universität ist allerdings erkennbar, dass eine Tür von

„sonst jemandem“ entsperrt wurde. Es besitzt also weniger Informationen als sonst (wo die genaue Identität bekannt ist). Aufgrund häufiger Vorkommnisse in einem Büro kann damit jedoch identifiziert werden, dass eine bestimmte Person am Projekt mitwirkt, da diese ihr Büro häufig „visuell“ entsperrt. Die Daten des Sperrsystems sind allerdings nur für sehr wenige Personen zugänglich und diese gehören der Universität an. Das Faktum der Mitwirkung am Projekt ist aber der Universität – wenn auch nicht unbedingt denselben Personen – bereits bekannt. Darüber hinaus ist dies für Mitwirkende kein problematisches Faktum mit besonderem Geheimhaltungsbedarf.

3. Ausübung von Betroffenenrechten

Die Betroffenenrechte können durch individuelle Bearbeitung jederzeit gewährleistet werden. Hierbei ist zu berücksichtigen, dass mangels Speicherung von Daten *sonstiger Betroffener* fast alle Rechte ohnehin leerlaufen (z.B. die Löschung: wo nichts gespeichert ist, kann nichts gelöscht werden). Für *Mitwirkende* am Projekt werden die Rechte im Bedarfsfall individuell durch Auswertungen der gespeicherten Daten durchgeführt. Einzig potentiell problematisch ist die Löschung der Daten bei Rückzug der Einwilligung. In einem solchen Fall müssen die Aufzeichnungen – soweit sie noch existieren – nach der erkannten Person durchsucht und anschließend gelöscht werden. Dies ist mit einem etwas höheren Aufwand verbunden, aber technisch ohne weiteres durchführbar.

4. Informationspflicht

Es ist jederzeit klar, wo sich Kameras befinden, und wer auf diese bzw. deren Daten Zugriff besitzt. Diese Informationen sind aufgrund der Ausschilderung und der Webseite für sonstige Betroffene jederzeit verfügbar. Eine Entfernung der Schilder würde von den Mitwirkenden rasch bemerkt. Für Mitwirkende basiert die Verarbeitung auf einer Einwilligung, welche bereits die erforderlichen Informationen enthält.

URL der Website: **https://www.digidow.eu/experiments/face-recognition-on-campus/**

5. Mögliche Auswirkungen und ihre Eintrittswahrscheinlichkeit

5.1. Veränderung des Verhaltens aufgrund der sichtbaren Kameras: Dies wird durch die Informationsschilder zumindest stark reduziert. Eine vollständige Verhinderung ist nicht möglich, sofern die Kameras nicht unsichtbar angebracht werden. Dies erscheint jedoch weniger nutzerfreundlich (und wäre kaum legal); wenn eine Beobachtung durch Kameras erfolgt, dann sollte dies (und auch die Kameras) für Betroffene erkennbar sein. Für Mitwirkende ist keine Änderung zu erwarten; diese erhalten einen zusätzlichen Service, der ihnen den Alltag erleichtert (kein manuelles Entsperren notwendig), ohne dass sie dadurch beeinträchtigt werden. Insbesondere wird nur der „öffentliche“ Bereich gefilmt, aber z.B. nicht das Innere von Büros. Es erscheint daher unwahrscheinlich, dass das Verhalten bzgl. Betreten/Verlassen des Büros hierdurch verändert wird. Potentiell könnte dies auch dazu führen, statt dem Büro mehr Heimarbeit durchzuführen, um der Videoüberwachung zu entgehen; doch dann

könnte ebenso einfach keine Mitwirkung am Projekt erfolgen. Auch für „bekannte“ Personen, d.h. Institutsmitarbeiter*innen, welche nicht am Projekt teilnehmen, erfolgt keine Personenerkennung. Darüber hinaus erfolgt im selben Gebäude beim Eingang bereits eine Live-Videoüberwachung durch die Universität. Kameras sind daher nichts ungewöhnliches und der einzige Unterschied ist die Auswertung der Bilder. Für Nicht-Mitwirkende ergibt sich durch die sofortige Löschung ein identisches Ergebnis (mit nur wenigen Sekunden Verzögerung). Dieses Risiko erscheint daher als sehr unwahrscheinlich.

5.2. Auswertung der Daten zu anderen Zwecken: Eine Auswertung der Daten könnten z.B. zur Arbeitszeitüberwachung erfolgen, um das Betreten/Verlassen des Büros pro Tag zu prüfen. Dies ist technisch eine leichte Auswertung, leidet aber an Schwierigkeiten. An sich können die Kameras nur das Betreten erkennen, doch wäre es mit der zu erprobenden Technologie wahrscheinlich ebenso möglich, auch das Versperren einer Türe und anschließendes Weggehen zu erkennen. Dies ist jedoch kein Ziel des Projekts und aufgrund freier Zeiteinteilung besteht auch kein Bedarf an solchen Auswertungen. Dieses Risiko wird daher als sehr gering eingeschätzt.

5.3. Weitergabe von Aufzeichnungen: Die Aufzeichnungen werden nach einer kurzen Frist gelöscht, doch diese könnten vorher kopiert und sofort oder auch später weitergegeben werden. Es ist jedoch unwahrscheinlich, dass dies einen Nachteil für die Mitwirkenden darstellt, da nur ein sehr kurzer Ausschnitt zu sehen ist, in welchem sie in einem öffentlichen Bereich einen Raum betreten. Potentiell problematisch könnten daher höchstens Zusatzaspekte sein; begleitende Personen oder getragene Dinge, welche dann ebenfalls aufgezeichnet werden. Die Wahrscheinlichkeit hierfür ist sehr gering einzuschätzen, da derartiges Vorgehen an sich schon unwahrscheinlich ist, und dann auch noch die Weitergabe ebenfalls unwahrscheinlich ist. Eine andere Möglichkeit ist, wenn Dritte in den Videos mitaufgezeichnet werden, z.B. im Hintergrund. Doch auch hier erscheint die Wahrscheinlichkeit und die Gefahr gering; es handelt sich um einen öffentlichen Raum, sehr kurze Ausschnitte, seltene Ereignisse (Betreten eines Büros im Vergleich zur Zeit, die inner-/außerhalb verbracht wird), und geringe Motivation für Weitergaben.

5.4. Weitergabe biometrischer Merkmale: Die extrahierten biometrischen Merkmale könnten weitergegeben werden. Dies bedeutet jedoch keine relevante Gefahr für Personen, da diese aus normalen Fotos extrahiert werden. Das bedeutet, jeder der Zugang zu einem Foto der Person hat, kann diese Daten ohnehin extrahieren. Eine Weitergabe ist daher sehr unwahrscheinlich und stellt kaum eine Gefahrenerhöhung dar.

5.5. Integration biometrischer Merkmale aus Drittquellen: Es könnten Fotos von sonstigen Personen beschafft werden (z.B. den Team-Seiten der JKU-Homepage), um daraus biometrische Merkmale zu extrahieren und zusätzliche Personen zu erkennen. Da diese jedoch nur äußerst selten einen der überwachten Räume (versuchen zu) betreten, würden viele dieser Personen in die Kategorie „kein Ziel erkannt“ sortiert und ihre Videos würden nicht gespeichert. Dies würde daher nur dann Sinn machen, wenn die Anwendung komplett unterschiedlich programmiert würde; Erkennung aller Personen und Speicherung unabhängig von

genauem Ort, erkanntem Ziel etc. Selbst dann ist aufgrund der Position der Kameras direkt vor dem Institut eher selten von einem Treffer bei sonstigen Personen auszugehen. Dies wird daher als unwahrscheinlich eingestuft. Potentiell problematisch könnte die Integration von Fotos/Merkmalen von Instituts-MitarbeiterInnen sein, welche keine Mitwirkende am Projekt sind; von diesen sind Bilder vorhanden und sie betreten den entsprechenden Bereich/Räume häufig. Diese Gefahr wird durch entsprechende Anweisungen bzw. Kontrolle der Auswertungen ausreichend reduziert.

5.6. Speicherung von Personen ohne Erkennung: Immer wenn eine Person erkannt wird, könnten diese Videos gespeichert werden, um später mit anderen Daten oder händisch einer Erkennung durchzuführen. Auch hier ist wieder davon auszugehen, dass dies nur wenige Personen beträfe. Dies würde auch eine komplette Umprogrammierung der Auswertungs-Computer erfordern und wird daher als unwahrscheinlich eingestuft.

5.7. Kenntnisnahme bzw. Weitergabe von Tonaufnahmen: Es findet überhaupt keine Tonaufzeichnung bzw. Auswertung statt. Die Gefahr ist daher praktisch nicht existent, da eine Aufzeichnung aufgrund des zusätzlichen Speicherbedarfs wahrscheinlich auffallen würde.

5.8. Zusätzliche Aufzeichnungen: Erlangt ein Angreifer Zugriff auf die Kameras, kann das Video zusätzlich ausgewertet und ausgeleitet oder gespeichert werden. Damit wäre eine länger dauernde Überwachung möglich, insbesondere auch von Betroffenen die keine Mitwirkenden sind. Dies wird durch Zugriffsschutz der Kameras sowie das Subnetz/Firewall verhindert.

V. Geplante Abhilfemaßnahmen (Art 35 Abs. 7 lit. d DSGVO)

1. Eine Auswertung der erhobenen bzw. gespeicherten Daten für andere Zwecke, insbesondere im Hinblick auf Arbeitszeiten, erfolgt nicht. Die Auswertung erfolgt direkt durch die Projektmitarbeiter*innen, sodass Vorgesetzte erst Zugriff auf die Daten erhalten müssten, bevor diese überhaupt derartige Auswertungen durchführen könnten.
2. Datensicherheitsmaßnahmen werden getroffen, indem sich die Kameras zwar (Szenarios 2 und 3) im öffentlich zugänglichen Raum befinden, räumlich bedingt ebenso die zugehörigen Rechner, sich die biometrischen Daten jedoch auf verschlüsselten Festplatten befinden. Ein Zugriff auf diese durch die Allgemeinheit ist daher nicht möglich (bzw. nur über die vorgesehenen Anwendungen zum Nachweis der Verarbeitungen) oder bei Kenntnis der Passwörter. Die elektronischen Zugangskennungen (Passwörter etc.) besitzen nur direkt am Projekt beteiligte Personen. Der Server für die Speicherung der Aufzeichnungen setzt ein verschlüsseltes Dateisystem ein. Weitere Datensicherheitsmaßnahmen orientieren sich am Stand der Technik.
3. Werden bei manueller Durchsicht Falscherkennungen entdeckt, so werden diese nachträglich ausgeschieden und gelöscht. Eine Anonymisierung der Bilder, z.B. durch Verpixelung, erfolgt nicht, da dies die wissenschaftliche Auswertung verhindern würde. Die Videos werden jedoch umgehend gelöscht, wenn diese nicht mehr benötigt werden.
4. Da nur Räume entsperrt werden, welche die Betroffenen ohnehin betreten dürfen, ergibt sich kein Nachteil für die Mitwirkenden. Sollte das System versagen und keine automatische Entsperrung erfolgen, so ist diese

weiterhin auf dem bisher üblichen Wege mit der Keplercard möglich, sodass auch hierbei kein Nachteil gegenüber dem Zustand ohne das System entsteht.

5. Sonstige Betroffene werden durch die Videoüberwachung nicht benachteiligt, da deren Daten immer nur für eine minimale Zeit gespeichert werden. Ihre biometrischen Merkmale werden zwar extrahiert und verglichen, aber es erfolgt keine Speicherung derselben. Durch die Kennzeichnung und den Link/QR-Code werden diese Personen auch über die konkreten Zwecke ausreichend informiert, sodass evtl. Befürchtungen ausgeräumt werden.
6. Speziell die extrahierten biometrischen Merkmale werden durch technische Maßnahmen geschützt, damit diese nicht exportiert und in Verbindung mit anderen Kameras, also an anderen Orten, wiederverwendet werden. Dies ist jedoch ohnehin eine geringere Gefahr, da dies auch aus öffentlich vorhandenen Bildern der Personen möglich ist: Die Extraktion erfolgt aus einem normalen 2D-Bild, und nicht etwa durch ein besonderes Enrollment-Verfahren, 3D-Scans etc., sodass diese Daten anderweitig nicht oder nur sehr viel schwerer zugänglich wären und daher ein besonderes Angriffsziel darstellen würden.
7. Tonaufnahmen finden überhaupt nicht statt (sofern die Kameras dies überhaupt unterstützen).
8. Überprüfungen: Regelmäßige Überprüfungen der Verarbeitungen finden nicht statt, doch erfolgen diese indirekt über die Auswertungen und die darauf basierenden wissenschaftlichen Arbeiten.
9. Protokollierungen: Änderungen der Zugriffsregeln werden protokolliert, aber ansonsten findet keine automatische Aufzeichnung der Verarbeitungsvorgänge statt. Da es sich um Forschung handelt, erfolgt eine Dokumentation ohnehin durch die Aufzeichnungen der Experimente und die darauf basierenden wissenschaftlichen Arbeiten.
10. Zugangspassworte (bzw. kryptographische Schlüssel etc.) zu den Kameras, Auswertungsrechnern, bzw. dem Speicherserver erhalten ausschließlich die damit direkt befassten Mitarbeiter*innen; diese werden vor Beginn der Arbeiten noch einmal speziell über die Geheimhaltungspflichten sowie die Datenschutzvorschriften geschult.
11. Die Veröffentlichung der Forschungsergebnisse erfolgt im Hinblick auf Dritte ausschließlich in anonymisierter Form. Sollten Beispielsbilder von Mitwirkenden veröffentlicht werden sollen, z.B. im Rahmen von Publikationen, so wird eine separate Einwilligung hierfür eingeholt.

VI. Stellungnahme des Datenschutzbeauftragten (Art 35 Abs. 2 DSGVO)

Die Datenschutz-Folgeabschätzung wurde nach Maßgabe des Art 35 DSGVO sowie der Leitlinien der Art-29-Datenschutzgruppe, WP 248 unter Einbeziehung der Rechtsabteilung, des Informationsmanagements, Datenschutzbeauftragten, Instituts für Netzwerke und Sicherheit sowie des Betriebsrates durchgeführt.

Die Einholung der Standpunkte sämtlicher von der Datenverarbeitung betroffener Personen ist nicht praktikabel bzw. mit unverhältnismäßig hohem Aufwand verbunden, da der Kreis der potentiell betroffenen Personen in Einzelfällen besonders groß sein kann bzw. viele dieser Personen im Vorhinein der Verantwortlichen nicht bekannt und somit auch nicht kontaktierbar sind; ein geeigneter Vertreter im Sinne des Art 35 Abs. 2 DSGVO ist für diese Personen nicht existent.

Die von der Verantwortlichen gewählten technischen und organisatorischen Abhilfemaßnahmen sind geeignet, die Realisierung der mit der Datenverarbeitung verbundenen bzw. identifizierten und bewerteten Risiken für die Rechte und Freiheiten der betroffenen Personen weitgehend auszuschließen, sodass die geplante Datenverarbeitung stattfinden kann.

VII. Stellungnahme des Betriebsrates (Art 35 Abs. 9 DSGVO)

Als BRwiss haben wir die Interessen der wissenschaftlichen Mitarbeiter*innen zu vertreten. Da diese alle vom Projekt informiert sind und die entscheidenden Zonen entsprechend ausgeschildert sind, sehen wir keine Bedenken gegen dieses Projekt, zumal die Mitarbeiter*innen ihr Verhalten entsprechend ausrichten können und damit letztlich eine ausreichende Hoheit über ihre Daten haben.