EINSCHREIBEN
Österreichische Datenschutzbehörde
Barichgasse 40-42
1030 Wien

Gebührenbefreit gemäß § 2 Z 3 GebG 1957

Antragstellerin: **JKU - Johannes Kepler Universität Linz**
Institut für Netzwerke und Sicherheit
Altenbergerstraße 69, 4040 Linz

wegen: Videoüberwachung und Auswertung zu Forschungszwecken an der JKU

Antrag auf Erteilung einer Genehmigung gemäß § 7 Abs 2 Z 3 iVm Abs 3 DSG

1-fach
Beilagen erwähnt

1. Darstellung des Projektes und Forschungszweck

Das Institut für Netzwerke und Sicherheit plant folgendes Forschungsprojekt im Rahmen des Christian-Doppler-Labors für private digitale Authentifizierung in der physischen Welt sowie seines Sicherheitsschwerpunktes: Mehrere Kameras sollen (an unterschiedlichen Orten/Konstellationen: 3 Szenarien; siehe Anhang) positioniert werden, welche permanent jeweils den Gangbereich bzw (Szenario 1) eine Tür von Innen aufnehmen. Eine Tonaufnahme erfolgt nicht. Die Kameras sind nicht beweglich, sondern nehmen nur den voreingestellten Bereich wahr (siehe Skizzen). Dieses Digitalbild wird live ausgewertet, ob sich eine Person dort befindet oder sich nähert (Erkennen eines Gesichts als solches). In diesem Fall wird per Gesichtserkennung versucht, diese Person den bekannten und vorher registrierten zutrittsberechtigten Personen (im Folgenden "Mitwirkende"; geschätzte Anzahl: 10-15) zuzuordnen. Zusätzlich wird (in den beiden Gang-Szenarien) versucht, die Intention der Person festzustellen, dh ob bzw zu welcher Tür sie sich hinbewegt. Das Ziel ist es, diese Tür dann automatisch zu entsperren, sodass keine manuelle Interaktion mehr erforderlich ist. Fernziel ist zB der Einsatz eines solchen Systems in Krankenhäusern, um sicheres aber berührungsloses Öffnen von Türen zu ermöglichen, selbst wenn beide Hände „belegt" sind (zB Eingang zu Operationssälen, wo eine Berührung der Türe/Schalter/Chipkarte etc vermieden werden sollte, um Keimübertragungen zu verhindern, bzw wenn ein Tablett mit Medikamenten oÄ getragen wird und daher keine Hand frei ist). Im Rahmen des Forschungsprojektes wird lediglich das Faktum der Erkennung der Person bzw die abgeleitete Intention gespeichert sowie automatisch die Verriegelung der Türe gelöst (mittels des Sperrsystems der Universität), sodass keine manuelle Autorisierung mittels der Keplercard (NFC – ist an das Türschloss zu halten; Ausweiskarte für MitarbeiterInnen) mehr erfolgen muss und der Raum direkt betreten werden kann. Die hiervon betroffenen Türen sind in den Skizzen markiert. Im Szenario 1 (Forensiklabor) wird die Tür nicht kontrolliert, da sich die Kamera im Inneren befindet. Dieses Szenario dient als Vergleich, da die Personen den Raum an exakt definierter Stelle betreten und daher das Gesicht an einem bestimmten Ort in bestimmter Größe „auftaucht". Die Türen beinhalten im Szenario 2 (Netzwerklabor) keine Büros sondern nur allgemeine Räume, zu welchen nur wenige Personen Zutritt besitzen und welche ausnahmslos Instituts-MitarbeiterInnen sind. Im Szenario 3 betrifft dies uA Büros mit Publikumsverkehr, dh Studierende und allgemeine Öffentlichkeit, sodass eine bessere Überprüfung der Identifizierung möglich ist (bzw bei weniger sicherer Erkennung und mehreren Personen ein Entsperren vermieden werden kann, um Unbefugten keinen Missbrauch zu ermöglichen, zB durch hinterhergehen).

Eine Übermittlung von Daten an das Sperrsystem erfolgt nur insoweit, als dass „eine bestimmte Tür zu entsperren ist", dh ohne Übermittlung der Identität, welche Person dies ausgelöst hat. Die Berechtigungsprüfung wird daher vom Schließsystem in das Forschungsprojekt hineinverlegt. Sollte eine betroffene Person nicht am Projekt mitwirken wollen (zB allgemeines Personal, deren Büros im Szenario 3 ebenso betroffen sind), so stellt dies kein Problem dar: die Entsperrung erfolgt weiterhin manuell und diese Personen werden von der Videoüberwachung nicht identifiziert und damit als „Unbekannte sonstige Person" eingestuft. Dies ist sogar datensparsamer als der derzeitige Zustand, bei dem die Zutrittskarte an das Türschloss zu halten ist (NFC) und die Universität daher die Identität der Karte (=Person) speichert. In umgekehrter Richtung (aus dem Schließsystem an das Forschungssystem, zB zur Überprüfung der Identität oder Verifizierung des Bewegungsziels einer Person) werden keine Daten übermittelt.

Der technische Ablauf ist wie folgt: Wird per Video ein Objekt als Person erkannt so wird versucht, die Identität dieser Person festzustellen. Dies erfolgt mittels persönlicher Agenten. Hierbei handelt es sich um Software, die auf einem vom Betroffenen selbst bestimmten Server ausgeführt wird und unter dessen Kontrolle steht. Dieser besitzt die Kontrolle über diverse personenbezogene Daten seines „Eigentümers", im konkreten Fall auch biometrische Informationen. Über sichere Kommunikation weist die Kamera diesem Agenten nach, welche Arten von Verarbeitung unter welchen Sicherheitsmaßnahmen, in welchen Fällen etc sie durchführt. Wenn dies dem Agenten aufgrund seiner

Konfiguration ausreichend erscheint (was bei Mitwirkenden vorausgesetzt wird), werden die biometrischen Merkmale an die Kamera übertragen und dort gespeichert. Damit wird eine lokale Überprüfung der von der Kamera aufgenommenen Bilder anhand der enthaltenen biometrischen Merkmale ermöglicht, welche bei unbekannten Personen - oder wo der Agent dies (aus welchen Gründen auch immer) verweigerte (zB bei MitarbeiterInnen die nicht am Projekt teilnehmen) - fehlschlägt. Dies bedeutet, dass mangels Vergleichsdaten auch nur der Versuch der Identifikation unmöglich ist, sofern der Betroffene (im Wege seines/ihres Software-Agenten) dem nicht vorher zustimmte. Auf Mitteilung des Mitwirkenden hin (evtl via Agenten) werden die gespeicherten Daten gelöscht (=Ausscheiden aus dem Projekt, Rückzug der Einwilligung etc).

War die Identifikation erfolgreich, wird für eine etwaige spätere manuelle Überprüfung ein Standbild sowie ein kurzer (5 Sekunden) Film gespeichert. Dies bedeutet, dass potentiell weitere Personen im Hintergrund bzw Handlungen Dritter/der Person mitabgebildet sein können. Es erfolgt jedoch keine Auswertung nach diesen Personen oder Aktivitäten. Die Speicherung lediglich eines Standbilds des Gesichts wäre nicht ausreichend, da nur mittels des gesamten Bilds überprüft werden kann, ob das „richtige“ Gesicht von potentiell mehreren erkannt wurde, bzw ohne kurzen Film eine Analyse/Überprüfung der Intention unmöglich ist.

War die Identifikation nicht erfolgreich, werden überhaupt keine Daten gespeichert, dh nicht einmal dass eine unbekannte Person sich zu einem bestimmten Zeitpunkt an einem gewissen Ort befand (und welche Dritte mit Zusatzwissen uU identifizieren könnten).

Die Gesichtserkennung soll hierbei möglichst nahe (uU direkt in) der Kamera, ansonsten auf einem unmittelbar damit verbundenen dedizierten Klein-Rechner in räumlicher Nähe erfolgen, um die Datensicherheit besonders stark auszugestalten. Zusätzlich ist geplant, dies für Dritte nachweisbar zu machen: Jeder (dh nicht nur die registrierten Personen!) kann mittels einer Anwendung und eines Smartphones überprüfen, dass eine bestimmte Kamera die Auswertung tatsächlich „lokal“ durchführt und keine Videodaten speichert bzw weitergibt. Dies soll insb dazu dienen, das Vertrauen in solche Systeme zu erhöhen. Denn damit ist auch eine nachträgliche Auswertung von Personen unmöglich – ohne Speicherung der „Unbekannten“ können diese selbst bei späterer Verfügbarkeit biometrischer Daten nicht identifiziert werden. Für die Forschung werden während des Projektes einzelne Bilder bzw kurze Sequenzen erkannter Personen sehr wohl gespeichert – was über die Anwendung (Web-App oder dedizierte Smartphone-App) daher auch klar erkennbar ist (nur das Faktum, nicht die Bilder/Videos, auch nicht eigene). Dies schließt nicht aus, dass es sich hierbei dennoch um eine Verarbeitung personenbezogener Daten handelt, da bereits die bloße Aufnahme dem Datenschutz unterliegt, selbst wenn der Verantwortliche nie Zugriff darauf erlangt (BVwG 3.9.2019, W214 2219944-1). Im Rahmen des Forschungsprojektes besteht – anders als bei den Produktivszenarien – für die Projektmitarbeiter jedoch klarerweise Zugang zu den Daten, sowohl biometrischen wie auch den Bildern/Aufnahmen. Doch auch für Nicht-Mitwirkende Betroffene ist daher eine Verarbeitung gegeben.

Die Verwendung von Bildern in Publikationen, sofern erforderlich, erfolgt ausschließlich in anonymisierter Form oder mit expliziter zusätzlicher Zustimmung der betreffenden Person. Die gilt auch für Mitwirkenden (=separate zusätzliche Zustimmung). Eine Weitergabe der Daten an Dritte erfolgt, abgesehen von Publikationen, ausschließlich in anonymisiert Form.

Da es sich um Videoaufnahmen handelt, sind daraus uU Rasse/Hautfarbe/Gesundheitseinschränkungen erkennbar, sodass es sich um besondere Kategorien von Daten handelt. Eine Auswertung nach diesen Kriterien erfolgt nicht, sondern ausschließlich im Hinblick auf eine biometrische Identifizierung des Gesichtes sowie die Bewegungsintention.

Hinweisschilder für die Kameras werden wie in den Skizzen im Anhang dargestellt angebracht. Eine Beschreibung des Projekts erfolgt auf der Homepage des Institutes, wobei ein Hinweis auf diese (URL/QR-Code) auf den Hinweisschildern enthalten ist. Dort sind auch Hinweise zum Zugriff auf die

überprüfbaren Informationen mittels Smartphone-Anwendung (Web-App oder dedizierte Smartphone-App) zu finden. Damit werden die Betroffenen über die Datenverarbeitung unterrichtet und können bei Bedarf weitere Informationen einholen (Vergleiche DSB Bescheid vom 27.5.2014, DSB-202.135/0002-DSB/2014; die dort noch als Auflage erwähnte DVR-Nummer existiert nach Wegfall des Datenverarbeitungsregisters nicht mehr).

Zweck des Projekts ist die Feststellung der Zuverlässigkeit von Gesichtserkennung und einer sicheren Integration mit einem Schließsystem auf eine datenschutzfreundliche Weise, dh mittels persönlicher Agenten unter 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 ist festzustellen, ob/wie ein sicherer Nachweis der tatsächlichen Verarbeitungsvorgänge der personenbezogenen Daten allgemein zur Verfügung gestellt werden kann (Web-Anwendung/App, Zugriff typ. per Smartphone).

Die Daten (siehe unten) sollen bis zum Projektabschluss (Ende des CD-Labors voraussichtlich zum Jahr 2026) aufbewahrt werden, sowie bis zur endgültigen Projektabnahme danach (für Rückfragen, Evaluierung des Abschlussberichts etc; vergleiche Bescheid der DSK vom 10.4.2013, K202.120/0002/DSK/2013). Dies gilt *nicht* für die Bilddaten selbst, welche (mit Ausnahme ausgewählter Daten für Publikationen) nach der Überprüfung/Auswertung, spätestens jedoch nach zwei Monaten, gelöscht werden. Eine längere Aufbewahrung ist erforderlich, da zu Forschungszwecken verschiedene Algorithmen und Verfahren getestet werden müssen um festzustellen, welche davon die besten Ergebnisse liefern. Hierzu ist mit jedem Algorithmus die Historie zu bearbeiten, um einen Vergleich zu ermöglichen.

An personenbezogenen Daten sollen *erhoben* werden:

1. 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.
2. 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.
3. Ort, Datum und Zeit der Erhebung: Dies ist uU für die Erkennung des Ziels der Person erforderlich.
4. Rolle der Mitwirkenden: Zugangsberechtigt für bestimmte Türen oder nicht.
5. Absicht der Mitwirkenden: Welche Tür als Ziel erkannt wurde oder „Unbekannt“

An personenbezogenen Daten sollen *gespeichert* werden:

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

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

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

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

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

d. Erkannte Bewegungsintention. Speicherdauer: 1 Jahr nach Projektende

3. 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.

4. Für jede Person, 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.

2. Über die Antragstellerin

Die Antragstellerin verfolgt wissenschaftliche Forschungszwecke iSd Art 89 Abs 1 DSGVO und ist demzufolge eine wissenschaftliche Einrichtungen iSd § 2b Z 12 FOG. Zudem geht die Antragstellerin, da es sich bei ihr um eine Universität im Sinne des § 6 Universitätsgesetz 2002 (UG) handelt davon aus, dass in § 3 UG keine datenschutzrechtliche Rechtsgrundlage für die Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken begründet liegt, die im Wege der Öffnungsklausel des Art 9 Abs 2 lit j DSGVO in Anspruch genommen werden könnte.

Ebenso geht die Antragstellerin davon aus, dass sie selbst datenschutzrechtlich Verantwortliche im Sinne des Art 4 Z 7 DSGVO ist, und nicht die konkret mit dem wissenschaftlichen Forschungsprojekt betrauten Forscherinnen und Forscher, die allesamt in einem Dienstverhältnis zur Antragstellerin stehen und das Forschungsprojekt in Erfüllung ihrer dienstlichen Pflichten durchführen.

3. Potentielle Problembereiche

Bei den Bildaufnahmen treten uU besondere rechtliche Probleme auf, welche hier mitsamt den ergriffenen Gegenmaßnahmen dargestellt werden.

- 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 offen 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 Forensiklabortür 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.
- 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, insb 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.

- 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 (zB Rechtsberatung) handelt. Zusätzlich kann dieser Raum auch von der anderen Seite des Gebäudes, dh 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 stellen sich daher keine Probleme.
- Der Eingang zum Netzwerklabor ist eine überwachte Tür, dh 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 InstitutsmitarbeiterInnen zu festgelegten Zeitpunkten statt, wobei eine Anwesenheitsliste geführt wird. Durch Information der TeilnehmerInnen (uA die Hinweisschilder), dem Fehlen einer Kamera im Laborinneren, sowie der Auswertung und Speicherung ausschließlich von Mitwirkenden bestehen hier keine Probleme.
- Andere geeignete Orte für Kameras bzw zu überwachende Türen stehen nicht zur Verfügung. An der Universität ist immer mit Publikumsverkehr zu rechnen und dieser ist für das Projekt auch erforderlich. Ebenso müssen Türen betroffen sein, zu welchen nur ein eingeschränkter Teil der Mitwirkenden Zugang besitzt (weshalb zB die Institutsbibliothek, welche von allen InstitutsmitarbeiterInnen betreten werden darf, kein gutes Studienobjekt wäre). Da auch im realen Leben damit zu rechnen ist, dass besonders geschützte Bereich betroffen sein können (hier zB die Damentoilette), müssen die Möglichkeiten, diese zuverlässig aus der Verarbeitung auszunehmen, ebenso erforscht und getestet werden.
- Datensicherheitsmaßnahmen werden getroffen, indem sich die Kamera zwar (Szenarios 2 und 3) im öffentlich zugänglichen Raum befinden, die zugehörigen Rechner mit den biometrischen Daten sich jedoch in angrenzenden Büros befinden. Ein Zugriff auf diese durch die Allgemeinheit ist daher nicht möglich (bzw nur über die vorgesehenen Anwendungen zum Nachweis der Verarbeitungen). Die elektronischen Zugangskennungen (Passwörter etc) besitzen nur direkt am Projekt beteiligte Personen (vergleiche Bescheid der DSK vom

13.12.2013, K202.128/0004-DSK/2013). Weitere Datensicherheitsmaßnahmen orientieren sich am Stand der Technik.

- Ein Verstoß gegen § 12 Abs 4 Z4 DSG liegt nicht vor, da zwar die Bilddaten nach biometrischen Kriterien zur Personenidentifikation ausgewertet werden (Art 9 Abs 1 DSGVO), aber keine Auswahl der Bildaufnahmen danach erfolgt. Weiters ist das Ziel dieses Paragraphen, eine Diskriminierung von Personen zu verhindern – dies erfolgt hier jedoch in keinster Weise. Die biometrischen Daten sind gerade nicht das Ziel der Auswertung, sondern lediglich das Mittel um auf eine Zutrittsberechtigung bzw das intendierte Bewegungsziel einer Person zu schließen – alles keine besonderen Kategorien an Daten. Darüber hinaus wurde von allen identifizierten Personen, i.e. den Mitwirkenden, im Vorhinein die ausdrückliche Zustimmung eingeholt. Von allen anderen Betroffenen werden alle Daten unmittelbar vollständig gelöscht. Insb bei biometrischen Daten kann dieser Paragraph weiters nicht wörtlich angewendet werden, da ansonsten selbst das Entsperren des eigenen Mobiltelefons oder Laptops mittels Bildaufnahme des eigenen Gesichts unzulässig wäre. In diesen Fällen erfolgt das gleiche wie im geplanten Forschungsprojekt: auch dort können andere Personen vor die Kamera gelangen, sie werden nicht identifiziert, und die Daten anschließend sofort verworfen.

4. Beabsichtigte Datenverarbeitungen, Umfang des Antrags

Details zu den geplanten Verarbeitungen sind in der Erläuterungen zu finden.

- Live-Aufnahme von Bilddaten im Gebäudeinneren der Universität
- Auswertung der Live-Bilder nach vorhandenen Personen und Vergleich dieser mit biometrischen Merkmalen mit vorher festgestellten Profilen von Mitwirkenden
- Speicherung von Standbildern und Kurzfilmen, sofern eine mitwirkende Person mit dem Ziel einer kontrollierten Türe erkannt wurde und sofortige Löschung aller anderen Daten

Der Antrag richtet sich ausschließlich auf Betroffene, die *nicht* gleichzeitig Mitwirkende sind, da bei Letzteren ihre freiwillige Einwilligung als Rechtsgrundlage dient.

5. Antrag auf Genehmigung der Verarbeitungen nach § 7 DSG

Mit diesem Antrag wird die Genehmigung dieser Verarbeitungen nach Maßgabe des § 7 Abs 2 Z 3 iVm Abs 3 DSG beantragt.

Gemäß § 7 Abs 2 Z 3 iVm § 7 Abs 3 DSG dürfen bei Datenverarbeitungen für im öffentlichen Interesse liegende wissenschaftliche Forschungszwecke, die nicht unter Abs. 1 fallen (i.e. personenbezogene Ergebnisse zum Ziel haben), personenbezogene Daten nur mit Genehmigung der Datenschutzbehörde verarbeitet werden.

Die Genehmigung ist zu erteilen, wenn die Einholung der Einwilligung der betroffenen Person mangels ihrer Erreichbarkeit unmöglich ist oder sonst einen unverhältnismäßigen Aufwand bedeutet, ein öffentliches Interesse an der beantragten Verarbeitung besteht und die fachliche Eignung des Verantwortlichen glaubhaft gemacht wird. Sollen besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) ermittelt werden, muss ein wichtiges öffentliches Interesse an der Untersuchung vorliegen; weiters muss gewährleistet sein, dass die personenbezogenen Daten beim Verantwortlichen der Untersuchung nur von Personen verarbeitet werden, die hinsichtlich des Gegenstandes der Untersuchung einer gesetzlichen Verschwiegenheitspflicht unterliegen oder deren diesbezügliche Verlässlichkeit sonst glaubhaft ist.

5.1. <u>Einholung der Einwilligung unmöglich / unverhältnismäßiger Aufwand</u>

Eine Zumutbarkeit der Einholung einer Einwilligung ist aufgrund der nachfolgenden Gründe unmöglich bzw würde für die Verantwortlichen einen unverhältnismäßigen Aufwand bedeuten:

- Die Mitarbeiter des Instituts (Szenario 1: Kamera im Rauminneren) sind ohne weiteres erreichbar, ebenso die Studierenden (Szenario 2: Kamera am Gangende), welche aufgrund der Lehrveranstaltungsanmeldung bekannt und damit erreichbar sind.

- Andere Studierende (zB Aufsuchen des Sekretariats oder von MitarbeiterInnen) oder sonstige Universitätsbedienstete (zB Postverteilung), sind jedoch nicht im Vorhinein bekannt. Diese müssen auch nicht notwendigerweise das die Forschung durchführende Institut besuchen (zB Besprechungsraum). Eine Einholung der Einwilligung alles Studierender der Antragstellerin (ca. 20.000 Studien belegt) sowie jeglicher Universitätsbediensteter (ca. 3300) ist jedoch effektiv unmöglich (zB aufgrund nachträglicher Immatrikulation, laufendes Personalwechsels etc). Entsprechend dem Bescheid der DSB vom 9.4.2018, DSB-D202.201/0003-DSB/2018 ist dies als eine äußerst hohe Anzahl an potentiell zu kontaktierenden Personen anzusehen (dort: 1.600 werden als „sehr hoch“ bezeichnet).

- Das Gebäude selbst unterliegt keiner Zugangsbeschränkung, sodass dieses auch von sonstigen Personen ohne (direkte) Vertragsbeziehung zur Universität betreten wird: Putzpersonal, Handwerker, Angehörige/Bekannte von Studierenden bei Besorgungen, prospektive Studierende (zB um sich bezüglich des Studiums zu informieren), sowie die allgemeine Öffentlichkeit (zB um Erkundigungen/Auskünfte einzuholen). Diese sind nicht einmal theoretisch im Vorhinein identifizierbar und kontaktierbar. Ein Verbot für solche Personen, das gesamte Gebäude oder auch nur das relevante Stockwerk zu betreten ohne vorher eine (wegen etwaigen Nachweises schriftlich erforderliche) Einwilligungserklärung abzugeben ist mit dem Selbstverständnis und den Aufgaben einer Universität nicht vereinbar und auch praktisch undurchführbar. Dies würde weiters dem Zweck des Forschungsprojekts - auch unbekannte Personen bei diversesten Motivationen/Zielen/Verhalten/… zu untersuchen – entgegenlaufen (siehe ähnlich Bescheid der DSB 10.8.2015, DSB-D202.152/0002-DSB/2015).

Daher geht die Antragstellerin von einer Unzumutbarkeit der Einholung sämtlicher Einwilligungserklärungen allenfalls betroffener Personen aus.

5.2. Wichtiges öffentliches Interesse an der Verarbeitung

Die Erkennung von Personen basierend auf Bildaufnahmen ist international weit verbreitet und gut erforscht. Dies erfolgt jedoch auf wenig datenschutzfreundliche Art. Zweck dieses Projektes ist es daher, die gleichen Funktionen bereitzustellen, aber hierbei den Datenschutz zu verbessern und die Autonomie der Betroffenen zu verstärken: Es muss nicht mehr darauf vertraut werden, dass zB der Arbeitgeber später die biometrischen Daten löschen wird, sondern es kann (über den selbst kontrollierten Software-Agenten) dies selbst veranlasst, sowie die vorgenommenen Verarbeitungen überprüft, werden. Da ein Verzicht auf Gesichtserkennung unrealistisch erscheint, ist es daher für die Allgemeinheit sehr wichtig, diese möglichst datenschutzfreundlich auszugestalten. Ansätze hierzu bestehen, aber deren Funktion, Praktikabilität etc ist erst zu erforschen und testen, wozu dieses Projekt dient. Dies bedeutet auch eine Ausweitung des Stands der Technik (praktische Erprobung), sodass bei zukünftigen Projekten in allen Bereichen entsprechende Technologien wenn auch vielleicht nicht umgesetzt, so doch zumindest evaluiert werden müssen.

Gerade in Zeiten großer allgemeiner Gesundheitsgefahren ist das konkrete Szenario automatischer Türöffnung in Verbindung mit sicherer Identifizierung, jedoch ohne Berührungsnotwendigkeit, ein herausragend wichtiges Ziel.

5.3. Fachliche Eignung der Verantwortlichen

Da es sich bei der Antragstellerin um eine juristische Person des öffentlichen Rechts handelt, ist auf die tatsächlich verarbeitenden Personen innerhalb ihrer Organisationsstruktur abzustellen. Im konkreten Falle sind dies:

Projektleitung: Univ.Prof. DI Dr. René Mayrhofer (Institutsvorstand; Leiter des CD-Labors)

Projektmitarbeiter: Dr. Michael Roland, MSc (Post-Doc; Stv. Leiter des CD-Labor)

Sämtliche Personen, die eine Verarbeitung von Daten im Rahmen und Umfang des Antrags vornehmen, unterliegen entweder einer gesetzlichen Verschwiegenheitspflicht nach Maßgabe der einschlägigen berufsrechtlichen Bestimmungen oder sind aufgrund ihrer Vita glaubhaft verlässlich und unbescholten (Curricula Vitae der mit der Verarbeitung betrauten Personen im Anhang; siehe auch deren Veröffentlichungen).

Soweit die Verantwortlichen bzw die verarbeitenden Personen auf sonstige wissenschaftliche Mitarbeiter zurückgreifen, wird deren fachliche Eignung von den Verantwortlichen entsprechend geprüft; diese sind den Verantwortlichen bzw den verarbeitenden Personen gegenüber auch weisungsunterworfen. Zusätzlich werden diese im Rahmen von entsprechenden Erklärungen zur Verschwiegenheit verpflichtet.

6. Urkundenvorlage und Anträge

Unter Vorlage von Skizzen zu

- Örtlicher Gegebenheit
- Position der Kameras
- Erfassungsbereich der Kameras
- Anbringung der Hinweisschilder

stellt die Antragstellerin den

ANTRAG,

die Österreichische Datenschutzbehörde möge die beabsichtigten Verarbeitungen gemäß § 7 Abs 2 Z 3 iVm Abs 3 DSG genehmigen.

Linz, am ……

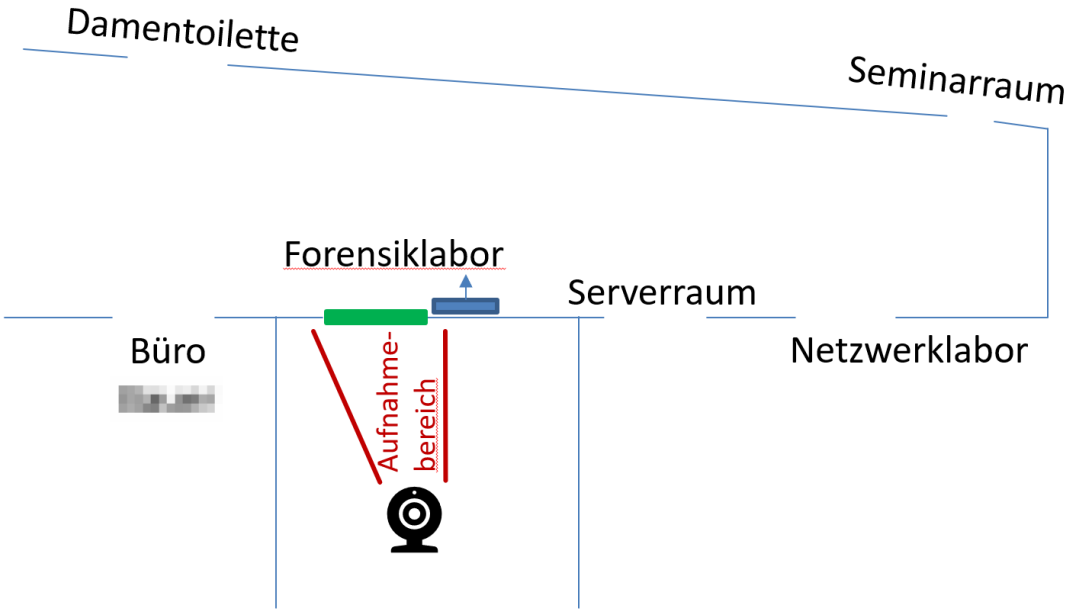
…….

JKU - Johannes Kepler Universität Linz,
vertreten durch Vizerektorin Univ.-Prof.in Dr.in Alberta Bonanni,

als Antragstellerin

Anhang 1: Darstellung der drei Szenarien

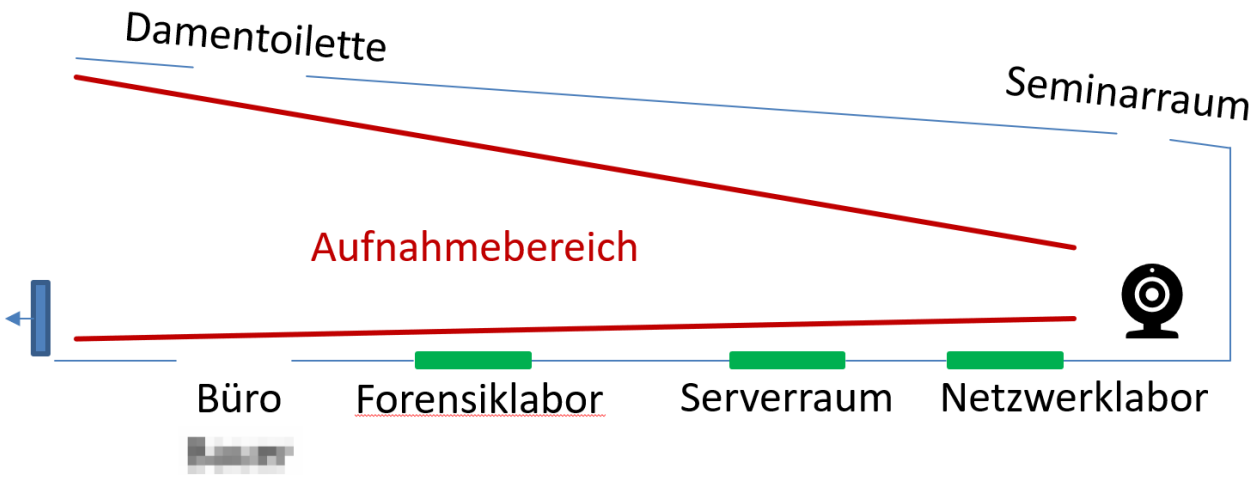
Szenario „1 - Forensiklabor“



Hinweisschild; von Kabelkanal abgehängt

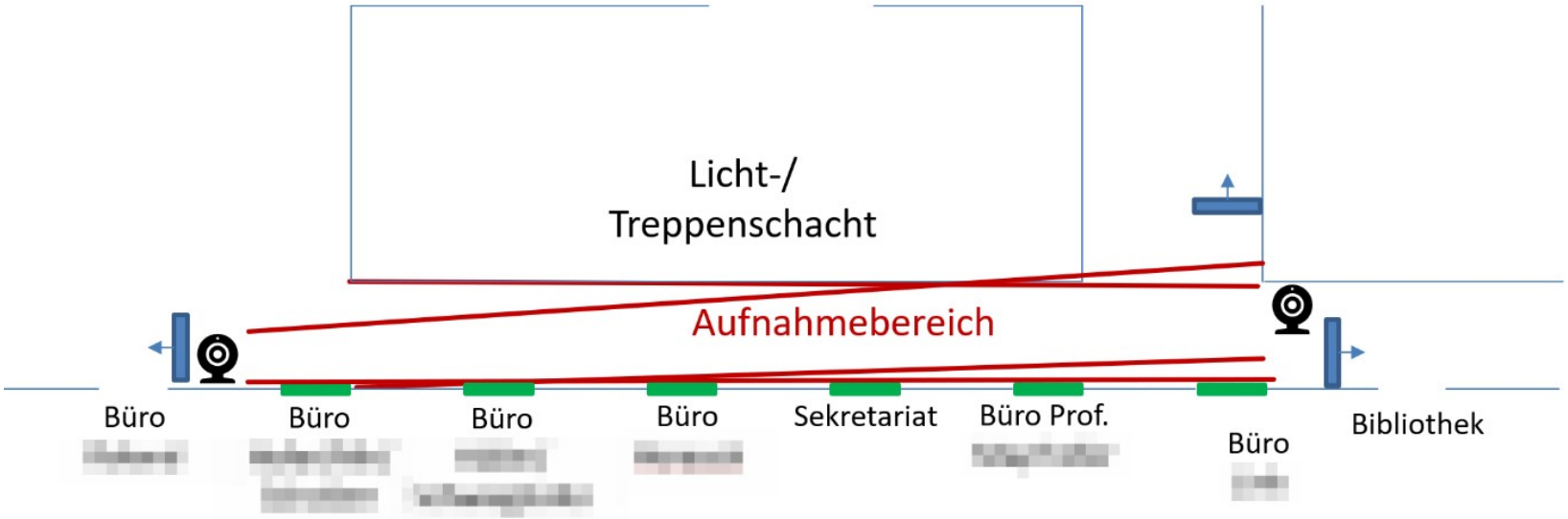
Kontrollierte Tür (hier ohne Entsperrung, da Kamera innen)

Szenario „2 - Netzwerklabor“



Hinweisschild; von Kabelkanal abgehängt

Szenario „3 - Gang“



Hinweisschild; von Kabelkanal/Decke abgehängt

Kontrollierte Tür mit Entsperrung