44. Geschlossene Sitzung der Global Privacy Assembly

Oktober 2022

Entschließung über Grundsätze und Erwartungen für die angemessene Nutzung personenbezogener Daten in der Gesichtserkennungstechnologie

Diese Entschließung wird von den Sponsoren im Namen der International Enforcement Cooperation Working Group und der Data Protection in Artificial Intelligence Working Group eingereicht.

SPONSOREN:

- Europäischer Datenschutzbeauftragter, Europäische Union
- Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter, Schweiz
- Information and Privacy Commissioner, Ontario (Kanada)
- Information Commissioner's Office, Vereinigtes Königreich
- Office of the Australian Information Commissioner, Australien
- Office of the Privacy Commissioner, Kanada
- Personal Information Protection Commissioner, Japan

CO-SPONSOREN:

- Katalanische Datenschutzbehörde, Katalonien
- Commission for Informatics and Liberties, Burkina Faso
- Data Protection Authority, Niederlande
- Data Protection Authority, Norwegen
- Gibraltar Regulatory Authority, Gibraltar
- Information Access Commission, Quebec (Kanada)
- Jersey Office of the Information Commissioner, Jersey
- National Access to Public Information Agency (Argentinien)
- Commission Nationale de l'Informatique et des Libertés, Frankreich
- National Privacy Commission, Philippinen
- Office of the Information and Privacy Commissioner, Neufundland und Labrador (Kanada)
- Office of the Information and Privacy Commissioner, Nova Scotia (Kanada)

- Office of the Privacy Commissioner, Neuseeland
- Personal Information Protection Commission, Korea
- Superintendence of Industry and Commerce, Kolumbien
- Regulatory and Control Unit of Personal Data, Uruguay.

Die 44. jährliche geschlossene Sitzung der Global Privacy Assembly:

Unter Hinweis auf die Entschließung zur Technologie zur Gesichtserkennung (FRT), die auf der 42. geschlossenen Sitzung der Global Privacy Assembly (GPA) im Oktober 2020 angenommen wurde, in der die Datenschutzrisiken der FRT hervorgehoben und die International Enforcement Cooperation Working Group (IEWG) und die Data Protection in Artificial Intelligence Working Group (AIWG) beauftragt wurden, eine Reihe vereinbarter Grundsätze und Erwartungen für die angemessene Verwendung personenbezogener Daten in FRT zu entwickeln und zu unterstützen;

In Anerkennung der Einsetzung einer Subgroup von IEWG- und AIWG-Mitgliedern und ihrer Bemühungen um die Erfüllung des in der Entschließung zur FRT festgelegten Mandats durch: Durchführung von Forschungsarbeiten; Durchführung einer Literaturrecherche; Einbeziehung der GPA-Mitgliedschaft; Konsultation mit relevanten globalen Interessenträgern; Entwicklung der Grundsätze und Erwartungen;

In Anerkennung der im Oktober 2020 angenommenen Entschließung zur FRT, in der bestätigt wird, dass öffentliche und private Einrichtungen in einer Vielzahl von Umgebungen live und retrospektive FRT weiterentwickeln und einsetzen, wie z. B.: öffentliche Räume; Arbeitsplätze; Geschäfte; Bildungseinrichtungen; Online; und in Kriegsgebieten,

Unter Berücksichtigung der laufenden globalen Debatte über FRT unter verschiedenen Interessenträgern (einschließlich Regulierungsbehörden, Gesetzgebern, Entwicklern, Nutzern, Wissenschaft und Zivilgesellschaft) und ihren jeweiligen Sichtweisen auf die Vorteile und Risiken der FRT, die in Untersuchungsergebnissen, Weißbüchern, Positionspapieren, Stellungnahmen, Blogs, Zeitschriftenartikeln und anderen öffentlichen Kommunikationen dargelegt sind;

In Anerkennung der wichtigen Beiträge der Datenschutzbehörden und internationaler Gremien zur globalen Debatte durch die Veröffentlichung von Strategie- und Leitfäden, einschließlich, aber nicht beschränkt auf:

- die Leitlinien des Europäischen Datenschutzausschusses für den Einsatz von Gesichtserkennungstechnologie im Strafverfolgungsbereich und die Gemeinsame Stellungnahme des EDSA und des EDSB zum Vorschlag des EU-Gesetzes über künstliche Intelligenz;
- die Datenschutzrichtlinien der kanadischen Bundes-, Provinz- und territorialen Datenschutzbeauftragten zur Gesichtserkennung für Polizeibehörden;
- der Empfohlene Rechtsrahmen der kanadischen Bundes-, Provinz- und territorialen Datenschutzbeauftragten für die Verwendung von Gesichtserkennung durch Polizeibehörden;
- die Stellungnahme des UK Information Commissioner's Office zum Einsatz von Gesichtserkennungstechnologie an öffentlichen Orten und zum Einsatz von

Technologien zur Live-Gesichtserkennung durch Strafverfolgungsbehörden an öffentlichen Orten;

- die Leitlinien des Europarates zur Gesichtserkennung; und
- die Empfehlung der Organisation der Vereinten Nationen für Bildung, Wissenschaft und Kultur (UNESCO) zur Ethik der künstlichen Intelligenz.

Unter Hervorhebung der formellen regulatorischen Eingriffe und Durchsetzungsmaßnahmen der Datenschutzbehörden, einschließlich der Durchführung von Ermittlungen und der Verhängung von Geldbußen, Unterlassungsanordnungen, Durchsetzungsbescheiden, und Empfehlungen in Bezug auf den Einsatz von FRT in vielen Situationen durch den Privatsektor, den öffentlichen Sektor und die Strafverfolgungsbehörden.

Unter Hinweis auf die bestehenden Rechtsvorschriften und rechtlichen Entwicklungen, die die Nutzung von FRT betreffen, einschließlich: der Illinois Biometric Information Privacy Act, das von der Europäischen Union vorgeschlagene Gesetz über künstliche Intelligenz und Kanadas vorgeschlagenes Gesetz über künstliche Intelligenz und Daten;

Unter Würdigung des Beitrags der GPA-Mitglieder für die Arbeit der FRT-Subgroup, indem ihre Sicht auf die wichtigsten Datenschutzrisiken im Zusammenhang mit den speziellen Anwendungen von FRT dargelegt wird;

Unter Begrüßung des Beitrags von FRT-Nutzern, Entwicklern, Gesetzgebern und Organisationen der Zivilgesellschaft für die Arbeit der FRT-Untergruppe zur Weiterentwicklung des Anwendungsbereichs, der Terminologie, der Klarheit, des Anwendungsbereichs und der Nutzbarkeit der Grundsätze und Erwartungen für die angemessene Verwendung personenbezogener Daten;

Unter Betonung, dass die Einhaltung der Datenschutzstandards für die verantwortungsvolle und vertrauenswürdige Entwicklung und den Einsatz von FRT überall auf der Welt von entscheidender Bedeutung ist;

In Bekräftigung der Zusagen im Strategischen Plan 2021-23 der GPA , die Stimme der Versammlung in der digitalen Politik zu stärken, die Zusammenarbeit in Regulierungsfragen auszubauen und auf ein Regelungsumfeld mit hohen Datenschutzstandards hinzuarbeiten, die weltweit klar und konsequent angewandt werden;

In der Erkenntnis, dass die Notwendigkeit klarer und kohärenter globaler Datenschutzstandards im Zusammenhang mit komplexen, risikoreichen und technologischen Innovationen wie FRT, bei denen Vorteile erzielt werden können, besonders wichtig ist und Unterschiede in der Regulierung zu Unsicherheiten für die Interessenträger führen können;

Die 44. Global Privacy Assembly befürwortet daher die Grundsätze und Erwartungen für die angemessene Nutzung personenbezogener Daten in der Gesichtserkennungstechnologie, die hier zusammengefasst und vollständig im Anhang enthalten sind:

1. **RECHTSGRUNDLAGE**: Organisationen, die Gesichtserkennung verwenden, sollten eine klare rechtmäßige Grundlage für die Erhebung und Nutzung biometrischer Daten haben.

2. **ANGEMESSENHEIT, NOTWENDIGKEIT UND VERHÄLTNISMÄSSIGKEIT:** Organisationen sollten die Angemessenheit, Notwendigkeit und Verhältnismäßigkeit ihres Einsatzes der Gesichtserkennungstechnologie begründen und nachweisen können.

3. **SCHUTZ DER MENSCHENRECHTE:** Organisationen sollten insbesondere rechtswidrige oder willkürliche Eingriffe in die Privatsphäre und andere Menschenrechte prüfen und die Menschen davor schützen.

4. **TRANSPARENZ:** Die Nutzung der Gesichtserkennung sollte für betroffene Personen und Gruppen transparent sein.

5. **RECHENSCHAFTSPFLICHT:** Die Anwendung der Gesichtserkennung sollte klare und wirksame Mechanismen zur Rechenschaftspflicht umfassen.

6. **DATENSCHUTZGRUNDSÄTZE:** Bei der Anwendung der Gesichtserkennung sollten alle Datenschutzgrundsätze, einschließlich der oben genannten Grundsätze, beachtet werden.

Die 44. Global Privacy Assembly beschließt, 2022-23 zusammenzuarbeiten, um folgendes zu erreichen:

1. Die weitere Erfüllung des Mandats in der Entschließung des Jahres 2020 der GPA zu FRT durch Ausarbeitung und Umsetzung eines Einsatzplans zur

    a. Förderung der Grundsätze mit einer Reihe wichtiger externer Interessengruppen; und

    b. Bewertung und Überprüfung der realen Anwendung der Prinzipien durch Entwickler und Nutzer von FRT.

2. Die Forderung, dass die IEWG und die AIWG weiterhin zusammenarbeiten, um diese Tätigkeit zu leisten, und der 45. geschlossenen Sitzung der Global Privacy Assembly über ihre Fortschritte Bericht erstatten.

Anhang:

Grundsätze und Erwartungen für die angemessene Nutzung personenbezogener Daten in der Gesichtserkennungstechnologie

Global Privacy Assembly

Einführung

Auf der 42. geschlossenen Sitzung der Global Privacy Assembly (GPA) im Oktober 2020 verabschiedeten die GPA-Mitglieder eine Entschließung zur Gesichtserkennungstechnologie (die Entschließung).

In der Entschließung wurde anerkannt, dass potenzielle Anwendungen der Gesichtserkennungstechnologie Vorteile für die öffentliche Sicherheit bieten könnten, betonte aber auch, dass die Technologie in der Lage ist, eine willkürliche oder rechtswidrige Überwachung zu ermöglichen und das Potenzial hat, stark in die Privatsphäre einzugreifen, voreingenommene Ergebnisse zu liefern und den Datenschutz, den Schutz der Privatsphäre und die Menschenrechte zu untergraben.

Öffentliche Einrichtungen, private Organisationen und die Zivilgesellschaft haben ihre Besorgnis darüber zum Ausdruck gebracht, dass die Technologie der Gesichtserkennung datenschutzrechtliche, rechtliche und ethische Herausforderungen mit sich bringt, die angegangen werden müssen. Gleichzeitig hat die GPA zuvor festgestellt, dass es notwendig ist, auf globale Richtlinien, Standards und Modelle für Angelegenheiten mit erheblichen Auswirkungen auf den Datenschutz hinzuarbeiten. Dies ermöglicht ein größeres Maß an regulatorischer Zusammenarbeit, verbessert die effiziente Prävention, Aufdeckung und Behebung von Datenschutzfragen und sorgt für Kohärenz und Klarheit im Aufsichtssystem für die digitale Wirtschaft.

Daher beschloss die GPA, eine Reihe abgestimmter Grundsätze und Erwartungen für die angemessene Nutzung personenbezogener Daten in der Gesichtserkennungstechnologie zu entwickeln, einschließlich der Empfehlung, wie Risiken gemindert werden können. Dieses Dokument dient diesem Zweck.

Über die Gesichtserkennung

Gesichtserkennung ist ein Verfahren, bei dem Software-Tools ein digitales Bild des Gesichts einer Person analysieren, ihre verschiedenen Merkmale in eine biometrische Vorlage extrahieren und diese Vorlage mit einer oder mehreren vorab extrahierten biometrischen Vorlagen vergleichen. Dies kann zum Zweck der **Verifizierun**g (z. B. ein One-to One-Vergleich zur Überprüfung einer von einer Person behaupteten Identität) oder der **Identifizierung** (z. B. ein One-to-Many Vergleich oder ein Many-to-Many-Vergleich eines Bildes einer unbekannten Person mit einer Datenbank biometrischer Referenzen) erfolgen. Dies kann in verschiedenen Modi geschehen, einschließlich **Live**- oder **Near-Live**-Anwendungen (z. B. Echtzeitvergleich eines oder mehrerer Gesichter mit einer Überwachungsliste) und **retrospektive**n Anwendungen (z. B. Vergleich eines zuvor aufgenommenen Bildes einer unbekannten Person mit einer Datenbank biometrischer Referenzen, wie bei einer polizeilichen Untersuchung).

Wie in der Entschließung anerkannt, stützt sich die Gesichtserkennungstechnologie auf sensible biometrische Informationen, die für den Einzelnen einzigartig und schwer zu verändern sind. Entscheidungen, die über Personen durch Nutzung dieser Identifikatoren getroffen werden, oft ohne ihr Wissen oder ihre Zustimmung, können zu nachteiligen Folgen führen, ohne dass angemessene Rechtsmittel zur Verfügung stehen. Neben den Auswirkungen auf die Privatsphäre kann die weit verbreitete Nutzung von Gesichtserkennung auch zu diskriminierenden Auswirkungen führen und die Fähigkeit zur Ausübung anderer grundlegender Menschenrechte wie der Meinungs-, Bewegungs- und Vereinigungsfreiheit beeinträchtigen.

Geltung der Grundsätze

Diese Grundsätze gelten für alle Arten und Nutzungen der Gesichtserkennung durch Organisationen des privaten und öffentlichen Sektors (einschließlich Strafverfolgungsbehörden). Auch wenn wir der Einfachheit halber den Begriff „Gesichtserkennung“ in diesem Dokument verwendet haben, gelten die nachstehenden Grundsätze gleichermaßen für jede biometrische Analyse von Gesichtsbildern und biometrischen Vorlagen (wie Rückschlüsse auf demografische Merkmale, emotionale Zustände usw.). Die Grundsätze sollen für Anwender, Entwickler und Anbieter von Gesichtserkennungssystemen gelten.

Wichtig ist, dass die nachstehend aufgeführten Grundsätze von gleichwertiger Bedeutung sind und ganzheitlich betrachtet werden sollten.

Schließlich erkennen wir an, dass Regierungen und Datenschutzbehörden eine wichtige Rolle bei der Gesichtserkennungstechnologie spielen, insbesondere im Hinblick auf die Schaffung und Durchsetzung geeigneter regulatorischer Rahmenbedingungen. Dies würde jedoch den Rahmen dieses Dokuments sprengen.

Terminologie

In diesem Dokument haben wir die folgenden Begriffe verwendet:

Biometrisches Merkmal: Ein biometrisches Merkmal ist die Messung eines physiologischen Merkmals (z. B. Fingerabdruck, Iris, Gesicht oder Handgeometrie einer Person) oder eines Verhaltensmerkmals (z. B. Gangart oder Tastendruckmuster) einer Person. Diese Merkmale sind meist beständig, einzigartig für die Person und schwer oder gar nicht zu ändern (d. h. die Änderung eines biometrischen Merkmals erfordert eine Änderung der physischen Person). Als solche sollten sie als sensibel angesehen werden.

Biometrisches Template: Eine digitale oder mathematische Darstellung der biometrischen Daten eines Individuums. Obwohl das spezifische Vorlagenformat veränderbar ist, stellt es ein Merkmal dar, das einzigartig, schwer zu ändern und untrennbar mit einer Person verbunden ist; als solches sollte es als sensibel behandelt werden.

Biometrische Probe: Ein biometrisches Template, das aus einem Bild einer unbekannten oder nicht verifizierten Person extrahiert wird, das mit einer biometrischen Referenz (im Falle einer Verifizierung) oder einer Referenzdatenbank (im Falle der Identifizierung) verglichen wird.

Biometrische Referenz: Ein biometrisches Template, das aus einem Bild extrahiert wird, das einer bekannten Identität zugeordnet ist, und mit dem eine biometrische Probe verglichen wird.

Referenzdatenbank: Eine Liste oder Datenbank biometrischer Referenzen, mit denen jeweils eine biometrische Probe verglichen wird.

Rechtliche Überlegungen

Die nachstehenden Grundsätze werden als Empfehlungen formuliert (unter Verwendung des Begriffs „sollte“). Viele von ihnen sind jedoch in den Rechtsordnungen der Mitglieder ausdrücklich gesetzlich vorgeschrieben oder können von Gerichten und Datenschutzbehörden so ausgelegt werden. Es obliegt jeder Organisation, die Gesichtserkennungstechnologie einsetzen möchte, sich über die geltenden rechtlichen Anforderungen in ihrer Rechtsordnung zu informieren.

GRUNDSÄTZE

1. RECHTSGRUNDLAGE: Organisationen, die Gesichtserkennung verwenden, sollten eine klare rechtmäßige Grundlage für die Erhebung und Nutzung biometrischer Daten haben.

1.1. Organisationen sollten die Rechtmäßigkeit ihrer Nutzung biometrischer Daten für die Gesichtserkennung dokumentieren und aufzeigen. Dies umfasst sowohl die rechtmäßige Grundlage für die Erfassung eines Bildes einer Person zur Erstellung einer biometrischen Probe

als auch für die Erstellung, den Zugriff auf oder die Änderung einer Referenzdatenbank, die verwendet wird oder werden soll. Dies sollte regelmäßig neu bewertet werden, um Änderungen des Gesetzes oder seiner Auslegung Rechnung zu tragen.

1.2. Wenn sie in einer Rechtsordnung tätig sind, die mehrere rechtmäßige Grundlagen für die Verarbeitung anerkennt, sollten Organisationen prüfen, ob eine andere Grundlage geeigneter ist als die Einwilligung. In vielen Anwendungen, einschließlich der Nutzung von Gesichtserkennung in öffentlich zugänglichen Räumen und Beschäftigungskontexten, kann es für eine Organisation schwierig sein, nachzuweisen, dass sie eine aussagekräftige Einwilligung einer Person erhalten hat.

1.3. Wenn die Einwilligung die Grundlage für die Verarbeitung ist, sollten Organisationen sicherstellen und nachweisen können, dass die Einwilligung aussagekräftig ist. Dies bedeutet, dass sie in Kenntnis der Sachlage erteilt wurde, dass sie spezifisch, aktuell, freiwillig gegeben und eindeutig ist. Dazu gehört auch die Berücksichtigung der Fähigkeit einer Person, eine aussagekräftige Einwilligung zu erteilen (z. B. bei Jugendlichen oder schutzbedürftigen Personen).

> 1.3.1. Einer ausdrücklichen Einwilligung wird der Vorzug gegeben. Organisationen sollten sich bewusst sein, dass die stillschweigende Einwilligung in vielen Rechtsordnungen nicht den Standard für die Zustimmung erfüllen würde und im Allgemeinen nicht für die Erhebung sensibler personenbezogener Daten herangezogen werden sollte. Sollte sich jedoch eine Situation ergeben, in der eine Organisation der Auffassung ist, dass sie sich auf die stillschweigende Einwilligung in die Gesichtserkennung berufen kann, sollte sie in der Lage sein, nachzuweisen, dass dies i) unter den Umständen angemessen ist, und ii) unter den gegebenen Umständen vernünftigerweise davon ausgegangen werden kann, dass eine Person ihre Einwilligung erteilt hat.

1.4. Unternehmen sollten sich darüber im Klaren sein, dass in vielen Rechtsordnungen das Auslesen von Bildern aus öffentlich zugänglichen Online-Plattformen (einschließlich sozialer Netzwerke) zur Erstellung einer Gesichtserkennungs-Referenzdatenbank nicht als rechtmäßig oder fair angesehen wird und auch nicht als transparentes Verfahren gilt.

2. ANGEMESSENHEIT, NOTWENDIGKEIT UND VERHÄLTNISMÄSSIGKEIT: Organisationen sollten die Angemessenheit, Notwendigkeit und Verhältnismäßigkeit ihrer Nutzung der Gesichtserkennungstechnologie begründen und nachweisen können.

2.1. Organisationen sollten die Notwendigkeit der Nutzung von Gesichtserkennungstechnologie begründen. Angesichts der Sensibilität der betreffenden Informationen ist der Schwellenwert für die Feststellung der Notwendigkeit hoch. Sie erfordert eine eindeutige Bestimmung des Zwecks, dass die Gesichtserkennungstechnologie bei der Erreichung dieses Zwecks wirksam sein kann und dass der Zweck vernünftigerweise nicht mit weniger in die Privatsphäre eingreifenden Mitteln erreicht werden kann. Bequemlichkeit oder Erwünschtheit sollte nicht als Begründung für die Notwendigkeit herangezogen werden.

2.2. Organisationen sollten die Verhältnismäßigkeit ihrer Nutzung der Gesichtserkennungstechnologie begründen und nachweisen können. Auch hier ist der Schwellenwert für die Feststellung der Verhältnismäßigkeit hoch. Die Vorteile der Anwendung

der Gesichtserkennung sollten das Risiko eines Schadens, den sie für die Privatsphäre und andere Menschenrechte des Einzelnen darstellt, deutlich überwiegen. Zur Begründung der Verhältnismäßigkeit sollten die Organisationen folgendermaßen vorgehen:

2.2.1. Organisationen sollten die von der Nutzung der Gesichtserkennungstechnologie erwarteten Vorteile dokumentieren und nachweisen können. Die Organisationen sollten auch klar festlegen, wie sie messen werden, ob das System diese Erwartungen erfüllt hat, und wie hoch der Nutzen ist, unterhalb dessen der Einsatz der Gesichtserkennung eingestellt würde.

2.2.2. Organisationen sollten dokumentieren und nachweisen können, dass sie potenzielle oder bekannte Schadensrisiken bewertet haben, die durch ihre vorgeschlagene Nutzung der Gesichtserkennung entstehen. Dies sollte auch die Berücksichtigung der Schadensrisiken für Einzelpersonen und Gruppen umfassen. Die Organisationen sollten auch klar dokumentieren, welche Maßnahmen sie zur Minderung festgestellter Risiken ergriffen haben.

2.2.3. Im Falle der Identifizierung sollte eine Organisation ein eindeutiges öffentliches Interesse an der Nutzung der Technologie nachweisen. Im Allgemeinen wird ein kommerzieller Gewinn an sich nicht als eindeutiges öffentliches Interesse angesehen.

2.2.4. Der Schwellenwert für die Verhältnismäßigkeit kann bei der Nutzung der Gesichtserkennungstechnologie zur Überprüfung leichter erreicht werden, wenn die Organisation nachweisen kann, dass Einzelpersonen ihre aussagekräftige Einwilligung in die Nutzung des Systems gemäß Grundsatz 1.3 erteilt haben.

2.3. Organisationen sollten die Angemessenheit ihrer Nutzung von Gesichtserkennungstechnologie begründen. Der Schwellenwert für die Begründung der Angemessenheit ist hoch. Was angemessen ist, ist eine Frage des Einzelfalls. Die Angemessenheit kann sowohl durch die Erwartungen der Gemeinschaft als auch durch aktuelle Standards und Praktiken der Gesichtserkennungstechnologie beeinflusst werden.

2.4. Um zu vermeiden, dass Entscheidungen durch versunkene Kosten oder Verpflichtungen beeinflusst werden, sollte die Bewertung der Angemessenheit, der Notwendigkeit und der Verhältnismäßigkeit vor dem Kauf, der Entwicklung oder dem Einsatz eines Gesichtserkennungssystems erfolgen.

2.5. Organisationen sollten sich der Feststellung ihrer jeweiligen Datenschutzbehörden bewusst sein, dass die bekannten oder potenziellen Schäden bestimmter Anwendung(en) der Gesichtserkennung so erheblich sind, dass sie in keinem Verhältnis zu den beabsichtigten Vorteilen stehen können.

2.5.1. Insbesondere sollten sich die Organisationen bewusst sein, dass der potenzielle Schaden, der mit der Erkennung menschlicher Merkmale in öffentlich zugänglichen Räumen (auch durch Gesichtserkennung) verbunden ist, dazu geführt hat, dass mehrere nationale, regionale und lokale Datenschutzbehörden, einschließlich aller Datenschutzbehörden des EWR, Verbote der Praxis vorschlagen.

2.5.2. Organisationen sollten sich auch bewusst sein, dass viele Datenschutzbehörden ein Verbot anderer Formen der Gesichtsanalyse gefordert haben, die nicht mit der

Verifizierung und Identifizierung in Zusammenhang stehen, wie z. B. der Rückschluss auf den Gemütszustand.

2.6. Die Bewertung der Angemessenheit, Notwendigkeit und Verhältnismäßigkeit durch eine Organisation sollte regelmäßig überprüft werden. Dabei sollte unter anderem geprüft werden, ob der Bedarf noch besteht; ob die an den Einsatz der Gesichtserkennung gestellten Erwartungen erfüllt wurden; und ob zuvor nicht identifizierte Schäden entstanden sind oder festgestellte Schäden schlimmer waren als erwartet, so dass diese Schäden nun die Vorteile überwiegen.

3. SCHUTZ DER MENSCHENRECHTE: Organisationen sollten insbesondere rechtswidrige oder willkürliche Eingriffe in die Privatsphäre und andere Menschenrechte prüfen und die Menschen davor schützen.

3.1. Im Allgemeinen sollten Organisationen davon ausgehen, dass der Einsatz der Gesichtserkennungstechnologie zu Unrecht in die Datenschutzrechte von Einzelpersonen eingreifen kann.

3.1.1. Dieser Eingriff ist in der Regel am größten, wenn diese Technologien in einem öffentlich zugänglichen Raum eingesetzt werden. Organisationen sollten insbesondere beachten, dass die Anwesenheit einer Person an einem öffentlichen Ort nicht unbedingt bedeutet, dass sie die berechtigte Erwartung an den Schutz der Privatsphäre oder der Kontrolle über personenbezogene Daten abgelegt hat. Nach Grundsatz 2.5.1 haben mehrere Datenschutzbehörden ein Verbot solcher Nutzungen vorgeschlagen.

3.1.2. Eingriffe werden auch durch die Nutzung von Gesichtserkennung erhöht, durch die Bewegungen, Handlungen oder Verhaltensweisen einer Person im Laufe der Zeit verfolgt werden (an den gleichen oder mehreren Orten und insbesondere an Orten, die sensible Informationen über eine Person offenbaren können).

3.2. Organisationen sollten nicht davon ausgehen, dass Bilder von Personen, die öffentlich im Internet zugänglich sind (einschließlich auf Social-Media-Seiten), gesammelt und umgewandelt werden können, um sie als biometrische Proben oder biometrische Referenzen zu verwenden oder um ein Gesichtserkennungssystem zu trainieren, ohne das Wissen und die Zustimmung dieser Personen oder eine andere rechtmäßige Grundlage für eine solche Sammlung und Verwendung.

3.3. Bei der Ermittlung potenzieller Auswirkungen auf das Recht auf Datenschutz und den Schutz der Privatsphäre sollten Organisation folgendermaßen vorgehen:

3.3.1. Durchführung geeigneter Folgenabschätzungen (z. B. eine Folgenabschätzung für die Privatsphäre, eine Datenschutz-Folgenabschätzung oder eine Folgenabschätzung für die Menschenrechte).

3.3.1.1. Organisationen sollten bezüglich der Bewertung und Minderung von Datenschutzrisiken allen potenziell betroffenen Personen gegenüber transparent sein.

3.3.2. Berücksichtigung demografischer Unterschiede (d. h. Vorurteile) sowohl in Bezug auf die Funktionsweise des Systems (z. B. relevante Leistungsunterschiede zwischen Gruppen) als auch in Bezug auf die Anwendung des Systems (z. B. Unterschiede in der Art und Weise, wie sich der Einsatz

des Systems auf Einzelpersonen oder Gruppen auswirken wird). Die Organisationen sollten auch überlegen, wie sie die unterschiedlichen Auswirkungen des Einsatzes des Gesichtserkennungssystems auf verschiedene Gruppen fortlaufend messen werden.

3.3.3. Die mögliche abschreckende Wirkung auf Rechte wie die Meinungsfreiheit und die Vereinigungsfreiheit sowie das Diskriminierungspotenzial im Zusammenhang mit der Nutzung von Gesichtserkennungssystemen in öffentlich zugänglichen Räumen sind unabhängig vom Zweck dieser Systeme zu prüfen.

3.3.4. Wenn marginalisierte Gruppen durch den Einsatz eines Systems besonders betroffen sein können, sollten sie sich mit den Vertretern dieser Gruppen über die erwarteten Auswirkungen und Strategien zur Schadensminderung beraten.

3.4. Wenn möglich, sollte bei Nutzung der Gesichtserkennung zu Kontrollzwecken eine alternative Methode zur Verfügung gestellt werden, die sich nicht auf biometrische Daten stützt, auch für Personen, die die Einwilligung ablehnen oder widerrufen. Personen sollten nicht für die Nutzung dieser Alternative bestraft werden.

4. TRANSPARENZ: Die Nutzung der Gesichtserkennung sollte für betroffene Personen und Gruppen transparent sein.

4.1. Organisationen sollten sicherstellen, dass Einzelpersonen (in einfacher, klarer Sprache) über Folgendes informiert werden:

4.1.1. Jedes Mal, wenn ihre aufgenommenen Gesichtsbilder von einem Gesichtserkennungssystem bearbeitet werden können oder werden, oder wenn ihr biometrisches Template in eine Referenzdatenbank für ein Gesichtserkennungssystem aufgenommen werden kann oder wird. Es ist wünschenswert und bewährte Praxis - und unter bestimmten Umständen gesetzlich vorgeschrieben -, dass Personen vor oder zum Zeitpunkt der Erfassung ihres Gesichtsbildes darüber informiert werden.

4.1.2. Ihre Datenrechte in Bezug auf Gesichtserkennungssysteme sowie die Ausübung dieser Rechte. Dies umfasst unter anderem die Möglichkeit, zu verlangen, dass ihr Gesichtsbild nicht einem Gesichtserkennungssystem bearbeitet wird, dass ihr biometrisches Template (falls zutreffend) aus einer Referenzdatenbank gelöscht wird oder dass Informationen über sie in einem Gesichtserkennungssystem korrigiert werden (z. B. durch Aktualisierung ihrer biometrischen Referenz).

4.1.3. Alle anderen Informationen, die den Einzelpersonen in ihrer Rechtsordnung zur Verfügung gestellt werden müssen. Dies beinhaltet, wie und wo Informationen gespeichert werden, für welche Zwecke sie verarbeitet werden, wie lange sie aufbewahrt werden und mit welchen Stellen sie geteilt werden können.

4.2. Die Organisationen sollten prüfen, wie sie sicherstellen, dass alle Personen, einschließlich Jugendlicher und schutzbedürftiger Personen, angemessen informiert werden.

4.3. Organisationen sollten sich bewusst sein, dass die alleinige Beschilderung über den Einsatz eines Gesichtserkennungssystems für die Einhaltung des Grundsatzes 4.1 in der Regel nicht ausreichen wird.

4.3.1. Wenn man sich zwecks Verarbeitung auf die Einwilligung beruft und die Beschilderung ein Teil dieses Einwilligungsverfahrens ist, sollte die Beschilderung deutlich sichtbar sein, bevor eine Person einen überwachten Bereich betritt. Diese Beschilderung sollte einen Hinweis auf alle verfügbaren Alternativen für den Zugang zum Raum enthalten. Die Beschilderung sollte auch deutlich darauf hinweisen, dass die Gesichtserkennung im Gegensatz zu einer Standard-Überwachungskamera verwendet wird.

4.3.2. Wenn Beschilderung ein wesentlicher Bestandteil der Bekanntmachungsstrategie einer Organisation ist, sollte darüber nachgedacht werden, wie Personen, die Schwierigkeiten haben, die Zeichen zu lesen oder zu verstehen, informiert werden.

4.4. Im Falle einer nachträglichen Gesichtserkennung sollten Organisationen proaktive Maßnahmen zur Sicherstellung ergreifen, dass Einzelpersonen über die Nutzung und den Zweck des Systems informiert werden. Dies beinhaltet sowohl die Veröffentlichung dieser Informationen vor dem Einsatz des Systems als auch (falls angemessen) spezielle Mitteilungen an Personen, deren Bilder von dem System verarbeitet wurden.

5. RECHENSCHAFTSPFLICHT: Die Nutzung der Gesichtserkennung sollte klare und wirksame Mechanismen zur Rechenschaftspflicht umfassen.

5.1. Organisationen sollten für alle Nutzungen der Gesichtserkennung klare Richtlinien für die Steuerung und Risikominderung festlegen und darauf vorbereitet sein, die Existenz und Wirksamkeit dieser Maßnahmen nachzuweisen.

5.1.1. Organisationen sollten ein Instrument zur Feststellung der Nichteinhaltung von Steuerungs- und Risikomanagementrichtlinien für die Gesichtserkennung (auch durch interne Akteure) und zur Feststellung von Folgen für die Nichteinhaltung einrichten und pflegen.

5.2. Alle Nutzer eines Gesichtserkennungssystems sollten regelmäßige Schulungen zu allen relevanten internen Datenschutzrichtlinien, den rechtlichen Anforderungen in ihrer Rechtsordnung, den Einschränkungen und potenziellen Vorurteilen von Gesichtserkennungssystemen, zur Durchführung des Gesichtsvergleichs und zur Minderung bekannter Risiken wie die von der Automatisierung induzierte Voreingenommenheit (d. h. der Tendenz für den Menschen, den Vorschlägen eines automatisierten Systems ein größeres Gewicht zu geben) durchführen.

5.3. Wo immer es angemessen ist, sollten die Schlussfolgerungen über die Identität einer Person von einem Menschen bewertet werden, der eine entsprechende Ausbildung absolviert hat. Dies ist insbesondere der Fall, wenn eine Einzelperson von einer solchen Schlussfolgerung erheblich betroffen sein wird.

5.3.1. Einzelpersonen sollten die Möglichkeit erhalten, jede Entscheidung, die auf der Grundlage einer Identifizierung mittels Gesichtserkennung getroffen wurde, anzufechten und Abhilfe zu verlangen.

5.3.2. Organisationen sollten sicherstellen, dass der Schwellenwert für eine „Übereinstimmung“ für die geplante Nutzung des Systems angemessen ist, unabhängig davon, ob dieser Schwellenwert von der Organisation selbst oder vom Entwickler des

Systems festgelegt wird.

5.3.3. Organisationen sollten Strategien zur Eindämmung von Risiken im Zusammenhang mit Nichtübereinstimmungen (sowohl falsch-positive als auch falsch-negative) und Fehlregistrierungen (d. h. Ungenauigkeiten in der Referenzdatenbank) entwickeln.

5.4. Organisationen sollten die Einschränkungen der Gesichtserkennungssysteme anerkennen und die Ergebnisse dieser Systeme entsprechend interpretieren. Im Falle eines nachträglich eingesetzten Gesichtserkennungssystems, das von Strafverfolgungsbehörden genutzt wird, sollte beispielsweise eine Übereinstimmung als ein möglicher Hinweis im Gegensatz zu schlüssigen oder zulässigen Beweismitteln betrachtet werden.

5.5. Organisationen sollten regelmäßige Nachprüfungen der Wirksamkeit des Gesichtserkennungssystems, der ergriffenen Risikominderungsmaßnahmen und der internen Einhaltung der Governance-Strategien durchführen.

5.6. Organisationen sollten alle demografischen Unterschiede in Bezug auf die Wirksamkeit ihres Einsatzes eines Gesichtserkennungssystems kontrollieren und regelmäßig bewerten.

5.7. Organisationen, die Gesichtserkennungssysteme entwickeln, sollten die Maßnahmen zur Messung und zum Schutz vor demografischen Differenzen in ihren Produkten sowie die Wirksamkeit dieser Maßnahmen (d. h. etwaige bekannte Leistungsunterschiede zwischen den demografischen Gruppen) dokumentieren.

5.8. Organisationen, die Gesichtserkennungssysteme kaufen oder anderweitig nutzen möchten, sollten folgendes unternehmen:

5.8.1. Einholung von Informationen über die Messung und den Schutz vor demografischen Differenzen, die nach Grundsatz 5.7 dokumentiert sind.

5.8.2. Einholung von Informationen über die demografischen Merkmale der Schulungs-, Test- und Bewertungsdatensätze des Produkts, um sicherzustellen, dass sie ein ausreichend vielfältiges Personenspektrum für den beabsichtigten Kontext enthalten.

5.8.3. Sicherstellung, dass das Produkt so konzipiert und getestet wurde, dass es mit dem vorgesehenen Verwendungszweck kompatibel ist. Zum Beispiel ist ein Gesichtserkennungsprodukt, das zur Überprüfung in einer gut beleuchteten, kontrollierten Umgebung entwickelt wurde, möglicherweise für die Identifizierung in einer dunklen, sehr verwinkelten oder hochdynamischen Umgebung (d. h. sich bewegende Menschenmenge) nicht ausreichend genau.

5.8.4. Wenn sich Organisationen auf einen Drittanbieter verlassen, sollen sie über ein robustes Risikomanagement-Rahmenwerk für die Bewertung der Einhaltung des Grundsatzes 5.10 verfügen, sowie über die damit verbundenen vertraglichen Schutzmaßnahmen, um die Einhaltung der Vorschriften sicherzustellen.

5.9. Organisationen sollten Verfahren und Strategien festlegen, um Datenverletzungen im Zusammenhang mit dem Gesichtserkennungssystem zu ermitteln, zu mildern, darauf zu reagieren und der zuständigen Datenschutzbehörde zu melden.

5.10. Organisationen sollten sicherstellen, dass alle von ihnen einbezogenen Dritten die in diesem Dokument festgelegten Grundsätze (soweit sie für Dritte gelten) sowie alle gesetzlichen

Anforderungen erfüllen.

6. DATENSCHUTZGRUNDSÄTZE: Bei der Nutzung der Gesichtserkennung sollten alle Datenschutzgrundsätze, einschließlich der oben genannten Grundsätze, beachtet werden.

Organisationen müssen *alle* Datenschutzgrundsätze während des gesamten Lebenszyklus eines Gesichtserkennungssystems berücksichtigen. Zusätzlich zu den oben beschriebenen gehören dazu:

6.1. Privacy by Design.

6.1.1. Bei der Entwicklung eines Gesichtserkennungssystems sollten Organisationen einen Privacy by Design-Ansatz verfolgen, um sicherzustellen, dass Schutzmaßnahmen von Anfang an in Gesichtserkennungssysteme integriert sind.

6.1.2. Soweit dies angemessen ist, sollten Organisationen die zentrale Speicherung biometrischer Templates und biometrischer Rohdaten vermeiden. Im Falle einer Überprüfung könnte die biometrische Referenz beispielsweise auf einem Gerät oder Artefakt (wie einem Führerschein, Reisepass oder Mitarbeiteridentifikationsausweis) gespeichert werden, das sich im Besitz der zu überprüfenden Person befindet. Wenn biometrische Templates zentral gespeichert werden (wo bestimmte Zwecke dafür festgelegt werden), sollten sie durch starke und geeignete kryptografische Maßnahmen geschützt werden.

6.1.3. Organisationen, die ein Gesichtserkennungssystem nutzen, sollten sicherstellen, dass in jeder Phase des Informationslebenszyklus des Systems geeignete Schutzmaßnahmen angewandt werden.

6.2. Zweckbindung und Nutzungsbeschränkung.

6.2.1. Organisationen sollten die Zwecke, für die Gesichtserkennungssysteme verwendet werden, klar definieren und nicht von diesen Zwecken abweichen, es sei denn, dies ist gesetzlich erlaubt.

6.3. Datenminimierung, -speicherung und -löschung.

6.3.1. Organisationen sollten Aufbewahrungsfristen für biometrische Rohdaten und biometrische Templates (einschließlich solcher, die als biometrische Proben oder biometrische Referenzen verwendet oder in Referenzdatenbanken gespeichert sind) festlegen und biometrische Templates löschen, wenn deren Aufbewahrung nicht mehr erforderlich ist. Dieser Zeitraum sollte dem abnehmenden Nutzen eines biometrischen Templates im Laufe der Zeit Rechnung tragen.

6.3.2. Im Allgemeinen sollten biometrische Proben, die nicht mit einer biometrischen Referenz übereinstimmen, sofort gelöscht werden. Eine begrenzte Aufbewahrung solcher Bilder kann akzeptabel sein, wenn dies nach vernünftigem Ermessen erforderlich ist, z. B. für Systemtests, für die es eine klare Rechtsgrundlage gibt und mit dem festgelegten Zweck für die betreffende Verarbeitung im Einklang stehen, wenn eine angemessene Aufbewahrungsrichtlinie besteht. Abgeglichene biometrische Proben können für einen bestimmten Zeitraum aufbewahrt werden, sollten jedoch nur in Bezug auf diesen

Abgleich verwendet werden (d. h. zu Beweiszwecken oder um Einzelpersonen zu ermöglichen, eine über sie getroffene Entscheidung anzufechten).

6.3.3. Sofern dies nicht für einen definierten (und rechtmäßigen) Zweck erforderlich ist, sollten Organisationen vermeiden, ein Profil der Aktivitäten oder Verhaltensweisen einer Person zu erstellen, indem sie Übereinstimmungen in der Gesichtserkennung über einen längeren Zeitraum hinweg korrelieren.

6.3.4. Organisationen sollten über zugängliche Mechanismen verfügen, damit Einzelpersonen ihre biometrischen Templates aus einer Referenzdatenbank löschen lassen können, wenn sie ihrer Aufnahme nicht mehr zustimmen oder andere rechtmäßige Gründe haben, ein Ersuchen um Löschung zu stellen und wenn diesem Ersuchen stattgegeben wird. Solche Löschungen sollten zweckdienlich sein und so bald wie möglich (und innerhalb gesetzlich festgelegter Fristen) erfolgen.

6.4. Sicherheitsvorkehrungen.

6.4.1. Die Organisationen sollten Sicherheitsvorkehrungen ergreifen, die der hohen Sensibilität der Informationen in einem Gesichtserkennungssystem angemessen sind.

6.4.2. Organisationen sollten die erforderlichen Richtlinien, Verfahren, Sicherheitsstandards und -kontrollen umsetzen, um sicherzustellen, dass weder das Gesichtserkennungssystem noch die von ihm erfassten oder gespeicherten personenbezogenen Daten einem unbefugten oder unbeabsichtigten Zugriff, Missbrauch, Störungen oder Verlusten unterliegen.

6.4.3. Organisationen sollten sicherstellen, dass alle von ihnen eingesetzten Gesichtserkennungssysteme (einschließlich der von Dritten entwickelten Systeme) geeignete Maßnahmen zum Schutz biometrischer Templates umfassen und dass diese Schutzmaßnahmen angewandt werden. Diese sollten nach Möglichkeit den international anerkannten Standards für den Schutz biometrischer Informationen entsprechen.

6.4.4. Organisationen sollten ihre Sicherheitsvorkehrungen regelmäßig überprüfen, um sicherzustellen, dass sie für eine sich entwickelnde Bedrohungslandschaft ausreichend bleiben.

6.5. Datenqualität.

6.5.1. Organisationen sollten sicherstellen, dass biometrische Referenzen und alle anderen vom Gesichtserkennungssystem erhobenen, generierten und gespeicherten personenbezogenen Daten für den Zweck, für den sie genutzt werden, hinreichend genau und aktuell sind.

6.5.2. Organisationen sollten angemessene Maßnahmen ergreifen, um personenbezogene Daten zu korrigieren oder zu löschen, die in Bezug auf den Zweck, für den sie verwendet werden, ungenau sind.

6.5.3. Organisationen sollten sicherstellen, dass nur Bilder, die für die Nutzung mit Gesichtserkennungssystemen geeignet sind, in biometrische Referenzdatenbanken aufgenommen oder als biometrische Proben verwendet werden. Bei der Qualitätsbewertung sollten zumindest die Bildeigenschaften wie Pose, Beleuchtung,

Ausdruck, Bildgröße und -auflösung sowie Gesichtsverdeckung (d. h. das Vorhandensein von Brillen, Hüten, Schals oder Masken) berücksichtigt werden.