BESCHWERDE GEMÄß ARTIKEL 77(1), 80(1) DSGVO

***noyb* Fall-Nr. C043**

eingebracht von

1. XXX (**Beschwerdeführer**)

gegen

2. **Clearview AI, Inc**, 214 W 29th St, Fl 2, New York City, New York, 10001, United States, (privacy@clearview.ai) (**Clearview**).

1. VERTRETUNG

3. *noyb* - European Centre for Digital Rights, Goldschlagstraße 172/4/2, 1140 Wien, Österreich, ZVR: 1354838270 (***noyb***), ist eine Organisation ohne Gewinnerzielungsabsicht, die im Bereich des Datenschutzes (Vereinsstatuten, **Beilage 1**) tätig ist.

4. Der Beschwerdeführer hat *noyb* gemäß Artikel 80(1) DSGVO beauftragt, ihn zu vertreten (**Beilage 2**).

COMPLAINT UNDER ARTICLE 77(1), 80(1) GDPR

***noyb* Case-No: C043**

filed by

1. XXX ("**Complainant**")

against

2. **Clearview AI, Inc**, 214 W 29th St, Fl 2, New York City, New York, 10001, United States, (privacy@clearview.ai) ("**Clearview**").

1. REPRESENTATION

3. *noyb* - European Centre for Digital Rights is a non-profit organisation with its registered office at Goldschlagstraße 172/4/2, 1140 Wien, Austria, and with registration number ZVR: 1354838270 (hereinafter "***noyb***") (articles of association, **Attachment 1**).

4. Pursuant to Article 80(1) GDPR, the Complainant is represented by *noyb* (**Attachment 2**).

2. SACHVERHALT

2.1. Clearview

5. Clearview AI, Inc. ist ein Unternehmen mit Sitz in den USA, gegründet 2017. Das einzige Produkt des Unternehmens ist eine Gesichtserkennungsplattform, die es Nutzern ermöglicht, Fotos von Personen mit online gefundenen Bildern von ihnen abzugleichen. Seine Plattform „*umfasst die größte bekannte Datenbank mit mehr als 3 Milliarden Gesichtsbildern, die aus öffentlich zugänglichen Webquellen stammen, darunter Nachrichtenmedien, Mugshot-Websites, öffentliche soziale Medien und andere offene Quellen*" ('Overview', Clearview AI, via https://clearview.ai/overview): Hinweis: sämtliche Zitate sind eigene Übersetzungen aus der Englisch-sprachigen Quelle, sofern nicht anders gekennzeichnet).

6. Im Jahr 2020 hatte Clearview rund 2.900 aktive Benutzer. Obwohl das gesamte öffentlich zugängliche Marketingmaterial an Strafverfolgungsbehörden gerichtet war, reichten die Kunden von Clearview Berichten zufolge von „*Sicherheitsabteilungen von Colleges bis hin zu Generalstaatsanwaltschaften*" und umfassten „*eine erschreckende Anzahl privater Unternehmen in Branchen wie Unterhaltung (Madison Square Garden und Eventbrite), Glücksspiel (Las Vegas Sands und Pechanga Resort Casino), Sport (die NBA), Fitness (Equinox) und sogar Kryptowährung (Coinbase)*" (BuzzFeed News, 'Clearview's Facial Recognition App Has Been Used by The Justice Department, ICE, Macy's, Walmart, And the NBA', 27. Februar 2020, via https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement). Quellen weisen auch darauf hin, dass Privatpersonen die Plattform von Clearview genutzt haben und angeblich „*die App bei Dates und auf Partys verwenden - und um die*

2. FACTUAL BACKGROUND

2.1. Clearview

5. Clearview AI, Inc. is a company based in the US, founded in 2017. Its sole product is a facial recognition platform allowing users to match photos of individuals to images of them found online. Its platform "*includes the largest known database of 3+ billion facial images sourced from public-only web sources, including news media, mugshot websites, public social media, and other open sources*" ('Overview', Clearview AI, available at https://clearview.ai/overview).

6. In 2020, Clearview had about 2,900 active users. Despite directing all its publicly available marketing materials to law enforcement agencies, Clearview's clients reportedly ranged from "*college security departments to attorneys general offices*" and included "*a startling number of private companies in industries like entertainment (Madison Square Garden and Eventbrite), gaming (Las Vegas Sands and Pechanga Resort Casino), sports (the NBA), fitness (Equinox), and even cryptocurrency (Coinbase)*" (BuzzFeed News, 'Clearview's Facial Recognition App Has Been Used by The Justice Department, ICE, Macy's, Walmart, And the NBA', 27 February 2020, available at https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement). Sources also indicate private individuals have used Clearview's platform, reportedly using "*the app on dates and at parties – and to spy on the public*" (Kashmir Hill, 'Before Clearview

Öffentlichkeit auszuspionieren" (Kashmir Hill, 'Before Clearview Became a Police Tool, It Was a Secret Plaything of the Rich', The New York Times, 5. März 2020, via https://www.nytimes.com/2020/03/05/technology/clearview-investors.html).

2.1.1. Technische Beschreibung der Bilddatenbank und des Produkts von Clearview

7. Nach unserer Untersuchung und der Analyse öffentlich zugänglicher Quellen (Office of the Privacy Commissioner of Canada (OPCC), PIPEDA Report of Findings #2021-001, 2. Februar 2021, via https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/; Clearview AI, 'Law Enforcement', Clearview AI Website, via https://clearview.ai/law-enforcement; Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Letter to Clearview AI Inc. - Consultation prior to an order pursuant to Article 58(2)(g) GDPR, 27. Januar 2021, via https://noyb.eu/sites/default/files/2021-01/545_2020_Anh%C3%B6rung_CVAI_ENG_Redacted.PDF) sowie unserer eigenen technischen Expertise gehen wir davon aus, dass die von Clearview für seine Gesichtserkennungsplattform erstellte Bilddatenbank in vier Schritten befüllt wird:

   i. **Automatischer Bildscraper -** ein automatisches Tool durchsucht öffentliche Webseiten und sammelt (speichert) alle Bilder, die es als menschliche Gesichter beinhaltend erkennt. Zusammen mit diesen Bildern sammelt der Scraper auch

Became a Police Tool, It Was a Secret Plaything of the Rich', The New York Times, 5 March 2020, available at https://www.nytimes.com/2020/03/05/technology/clearview-investors.html).

2.1.1. Technical description of Clearview's image database and product

7. According to our investigation and analysis of publicly available sources (Office of the Privacy Commissioner of Canada (OPCC), PIPEDA Report of Findings #2021-001, 2 February 2021, available at: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/; Clearview AI, 'Law Enforcement', Clearview AI Website, available at https://clearview.ai/law-enforcement; Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Letter to Clearview AI Inc. - Consultation prior to an order pursuant to Article 58(2)(g) GDPR, 27 January 2021, available at https://noyb.eu/sites/default/files/2021-01/545_2020_Anh%C3%B6rung_CVAI_ENG_Redacted.PDF), and our own technical expertise, we understand that the image database created by Clearview for its facial recognition platform is populated in four steps:

   i. **Automated image scraper** – an automated tool searches public webpages and collects any images that it detects as containing human faces. Along with these images, the scraper also collects metadata associated with these images, such as the image or webpage title, and its source link.

Metadaten, die mit diesen Bildern verbunden sind, wie z. B. den Bild- oder Webseitentitel und den Quelllink.

ii. **Speichern von Bildern und Metadaten** - Die während des Scraping-Prozesses gesammelten Bilder und Metadaten werden auf den Servern von Clearview gespeichert. Diese werden auf unbestimmte Zeit gespeichert, d.h. auch nachdem ein zuvor gesammeltes Foto oder eine Hosting-Webseite entfernt oder privat gemacht wurde.

iii. **Extraktion von Gesichtsmerkmalen durch bildverarbeitende neuronale Netzwerke** - für jedes gesammelte Bild wird jedes im Bild enthaltene Gesicht gescannt und verarbeitet, um seine eindeutig identifizierenden Gesichtsmerkmale zu extrahieren. Die Gesichter werden in numerische Darstellungen übersetzt, die wir als „Vektoren" bezeichnen. Diese Vektoren bestehen aus 512 Datenpunkten, die die verschiedenen einzigartigen Linien darstellen, aus denen ein Gesicht besteht. In diesem Schritt werden Gesichter von menschlich erkennbaren Bildern in maschinenlesbare eindeutige biometrische numerische Bezeichner umgewandelt.

iv. **Speichern der Gesichtsmerkmale und Indizierung/Hashing** - Clearview speichert alle diese Bezeichner in einer Datenbank, wo sie mit den Bildern und anderen auf dem Clearview-Server gespeicherten Informationen verknüpft werden. Diese Vektoren werden dann gehasht (Hashing besteht aus der Umwandlung eines Vektors durch eine mathematische Funktion in einen kürzeren Wert oder Schlüssel mit fester Länge, der den ursprünglichen Vektor repräsentiert). Jeder Hash wird dazu verwendet, die Datenbank zu indizieren und auch, wie im nächsten Schritt erklärt, um die Gesichter miteinander abzugleichen. Jedem

ii. **Image and metadata storing** – the images and metadata collected through the scraping process are stored on Clearview's servers. These are stored indefinitely, i.e. even after a previously collected photograph or hosting webpage has been removed or made private.

iii. **Extraction of facial features through image processing neural networks** – for each image collected, every face contained in the image is scanned and processed in order to extract its uniquely identifying facial features. Faces are translated into numerical representations which we refer to as "vectors". These vectors consist of 512 data points that represent the various unique lines that make up a face. At this step, faces are converted from human recognisable images to machine-readable unique biometric numerical identifiers.

iv. **Facial features storing and indexing/hashing** – Clearview stores all these identifiers in a database where they are associated with the images and other scraped information stored on Clearview's server. These vectors are then hashed (hashing consists of the transformation of a vector, through a mathematical function, into a shorter fixed-length value or key that represents the original vector). Each hash is used to index the database and also, as explained in the next step, to match faces to each other. Every photo of a face in the database has a different vector and respective hashed value associated with it.

Photo eines Gesichts in der Datenbank ist ein anderer Vektor und ein entsprechender Hash-Wert zugeordnet.

8. Der fünfte und letzte Schritt im Produktlebenszyklus von Clearview ist der **Abgleich**. Dieser Schritt erfolgt nach der soeben beschriebenen vierstufigen Befüllung der Datenbank in vier Schritten. Er wird durchgeführt, wenn ein Benutzer von Clearview eine Person identifizieren möchte, und dazu ein Bild seiner Zielperson hochlädt und eine Suche durchführt. Clearview analysiert dann das Bild und extrahiert einen Vektor des Zielgesichts, der dann gehasht und mit allen zuvor in seiner Datenbank gespeicherten gehashten Vektoren verglichen wird. Abschließend zieht das Clearview-Tool alle übereinstimmenden Bilder aus der Vektordatenbank und zeigt sie dem Benutzer als Suchergebnisse an, zusammen mit allen zugehörigen Metadaten, so dass der Benutzer die ursprüngliche Quellseite der übereinstimmenden Bilder sehen kann.

2.1.2. Die Clearview „Enthüllungen" und das anschließende Interesse der Aufsichtsbehörden

9. Am 18. Januar 2020 enthüllte ein Artikel der *New York Times* mit dem Titel „*The Secretive Company That Might End Privacy as We Know It*" die Existenz von Clearview (Kashmir Hill, 'The Secretive Company That Might End Privacy as We Know It', The New York Times, 18 Januar 2020, via https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html). Vor diesem Artikel hatte Clearview mit bewusster Geheimhaltung operiert, während es sein Produkt „*mehr als 600 Strafverfolgungsbehörden*" und „*mindestens einer Handvoll Unternehmen zu Sicherheitszwecken*" anbot. Nach diesen

8. The fifth and last step in Clearview's product lifecycle is **matching,** which happens after the database has been populated according to the just described four steps. It is performed when a user of Clearview wishes to identify an individual, and for this uploads an image of their target and runs a search. Clearview then analyses the image and extracts a vector from the target face, which is then hashed and compared against all hashed vectors previously stored in its database. Finally, the Clearview tool pulls any matching images from the vector database and shows them to the user as search results, along with any associated metadata, such as the URL, the file name, but also any embedded geolocation data.

2.1.2. The Clearview 'revelations' and subsequent actions by regulators

9. On 18 January 2020, a *New York Times* article entitled "The Secretive Company That Might End Privacy as We Know It" revealed Clearview's existence to the world (Kashmir Hill, 'The Secretive Company That Might End Privacy as We Know It', The New York Times, 18 January 2020, available at https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html). Prior to this article, Clearview had operated with intentional secrecy, while offering its product to "*more than 600 law enforcement agencies*" and "*at least a handful of companies for security purposes*". Following these "revelations", organisations and

„Enthüllungen" begannen Organisationen und Aufsichtsbehörden in den USA und im Ausland, die Praktiken von Clearview zu überprüfen.

10. In den USA wurden „*innerhalb von Tagen nach Veröffentlichung des Times-Artikels acht mutmaßliche Klagen eingereicht, weitere folgten*" (Sam Jungyun Choi et al, '*Clearview AI revelations spark action on use of facial recognition*', Privacy Laws & Business International Report, August 2020, via https://www.cov.com/-/media/files/corporate/publications/2020/08/clearview-ai-revelations-spark-action-on-use-of-facial-recognition.pdf). Da es in den USA kein Bundesdatenschutzgesetz gibt, werden diese Klagen in den einzelnen Bundesstaaten nach den Gesetzen der jeweiligen Bundesstaaten erhoben. Eine davon wurde im Mai 2020 von der American Civil Liberties Union (ACLU) in Illinois eingereicht (ACLU, '*ACLU sues Clearview AI*', 28. Mai 2020, via https://www.aclu.org/press-releases/aclu-sues-clearview-ai), unter dem bundesstaatlichen *Biometric Information Privacy Act* (BIPA), der die Sammlung und Verwendung biometrischer Daten regelt. Eine weitere Klage wurde im Februar 2021 in Kalifornien von Bürgerrechtsaktivisten und Gruppen für die Rechte von Einwanderern eingereicht, die behaupten, dass die Praktiken von Clearview gegen die verschiedenen lokalen Verbote der staatlichen Nutzung von Gesichtserkennungstechnologie verstoßen (CNN Business, '*Clearview AI sued in California by immigrant rights groups, activists*', 10. März 2021, via https://edition.cnn.com/2021/03/09/tech/clearview-ai-mijente-lawsuit/index.html).

11. In Kanada hat das *Office of the Privacy Commissioner of Canada* (**OPCC**) zusammen mit den Datenschutzbehörden der Provinzen im Februar 2020 eine Untersuchung der Praktiken von Clearview eingeleitet. Es

regulators in the United States (US) and abroad started scrutinising Clearview's practices.

10. In the US, "*eight putative actions were filed within days of publication of the Times article, and more have followed*" (Sam Jungyun Choi et al, 'Clearview AI revelations spark action on use of facial recognition', Privacy Laws & Business International Report, August 2020, available at https://www.cov.com/-/media/files/corporate/publications/2020/08/clearview-ai-revelations-spark-action-on-use-of-facial-recognition.pdf). Due to the lack of a federal privacy law in the US, these actions are taken in individual states under state legislation. One of these was filed in May 2020 by the ACLU in Illinois (ACLU, 'ACLU sues Clearview AI', 28 May 2020, available at https://www.aclu.org/press-releases/aclu-sues-clearview-ai), under the state's Biometric Information Privacy Act (BIPA), which regulates the collection and use of biometric information. Another was filed in February 2021 in California by civil liberties activists and immigrants' rights groups, claiming that Clearview's practices violate the various local bans on government use of facial recognition technology (CNN Business, 'Clearview AI sued in California by immigrant rights groups, activists', 10 March 2021, available at https://edition.cnn.com/2021/03/09/tech/clearview-ai-mijente-lawsuit/index.html).

11. In Canada, the Office of the Privacy Commissioner of Canada ("**OPCC**"), together with provincial privacy regulators, opened an investigation into Clearview's practices in February 2020. It published its report of findings on 2 February 2021, recommending that Clearview cease

veröffentlichte seinen Ergebnisbericht am 2. Februar 2021 und empfahl, dass Clearview seine Dienste in Kanada nicht mehr anbietet, die Sammlung, Verwendung und Weitergabe von Bildern und biometrischen Gesichtsdaten von Personen in Kanada einstellt und die Bilder und biometrischen Gesichtsdaten von Kanadiern in seinem Besitz löscht ((Office of the Privacy Commissioner of Canada (OPCC), PIPEDA Report of Findings #2021-001, 2. Februar 2021, via https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/).

12. In UK und Australien leiteten die Datenschutzbehörden im Juli 2020 eine gemeinsame Untersuchung der „*Praktiken zum Umgang mit personenbezogenen Daten*" von Clearview ein (Information Commissioner's Office, 'The Office of the Australian Information Commissioner and the UK's Information Commissioner's Office open joint investigation into Clearview AI Inc.', 9. Juli 2020, via https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/07/oaic-and-ico-open-joint-investigation-into-clearview-ai-inc).

13. In der EU wurden in verschiedenen Ländern unterschiedliche Maßnahmen ergriffen. In Deutschland sah der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (**HmbBfDI**) eine Anordnung vor, Clearview zu verpflichten, den Hashwert des dortigen Beschwerdeführers zu löschen (*noyb*, 'Clearview AIs biometrische Fotodatenbank in der EU illegal, aber nur begrenze Löschungsanordnung', 28. Januar 2021, via https://noyb.eu/de/clearview-ai-der-eu-illegal). Die vorgesehene Anordnung beschränkte sich auf den jeweiligen Einzelfall und

offering its services in Canada, cease the collection, use and disclosure of images and biometric facial arrays collected from individuals in Canada, and delete the images and biometric facial arrays of Canadians in its possession (Office of the Privacy Commissioner of Canada (OPCC), PIPEDA Report of Findings #2021-001, 2 February 2021, available at: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/).

12. In the UK and Australia, data protection regulators opened a joint investigation into the "*personal information handling practices*" of Clearview in July 2020 (Information Commissioner's Office, 'The Office of the Australian Information Commissioner and the UK's Information Commissioner's Office open joint investigation into Clearview AI Inc.', 9 July 2020, available at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/07/oaic-and-ico-open-joint-investigation-into-clearview-ai-inc).

13. In the EU, disparate actions were taken in various countries. In Germany, the Hamburg Data Protection Authority was looking into an order requiring Clearview to delete the hash value associated with an individual's facial images (*noyb*, 'Clearview AI's biometric photo database deemed illegal in the EU, but only partial deletion ordered', 28 January 2021, available at https://noyb.eu/en/clearview-ai-deemed-illegal-eu). The envisaged decision was limited to the individual case in issue and fell short of requiring the cessation of Clearview's activities in the jurisdiction. In Sweden, the Swedish

verlangte nicht die Einstellung der Aktivitäten von Clearview in dem Jurisdiktion. In Schweden stellte die schwedische Aufsichtsbehörde im Februar 2021 fest, dass die schwedische Polizeibehörde die Dienste von Clearview rechtswidrig genutzt und personenbezogene Daten unter Verstoß gegen das schwedische Strafdatengesetz, die Durchführungsbestimmungen der Strafverfolgungsrichtlinie (2016/680), verarbeitet hatte (**LED**) (Integritetsskydds myndigheten, '*Police unlawfully used facial recognition app*', 11. Februar 2021, via https://www.imy.se/nyheter/police-unlawfully-used-facial-recognition-app/). Verschiedene andere Länder wie Italien haben Untersuchungen zu Clearview-Praktiken eingeleitet (Wired, '*Il Garante italiano della privacy indaga sulla più controversa società di riconoscimento facciale al mondo*', 15. April 2021, via https://www.wired.it/attualita/tech/2021/04/15/riconoscimento-facciale-garante-privacy-clearview-ai/).

14. Der Europäische Datenschutzausschuss (**EDSA**) gab auf Fragen von Mitgliedern des Europäischen Parlaments, die Bedenken hinsichtlich Clearview äußerten, am 10. Juni 2020 eine vorläufige Bewertung ab (EDPB, *Letter to Members of the European Parliament*, Ref: OUT2020-0052, 10. Juni 2020, via https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-response-meps-sophie-t-veld-moritz-korner-michal-simecka_en). Diese Bewertung konzentrierte sich auf „*die Rechtkonformheit und Rechtmäßigkeit der Verarbeitung, die sich aus der möglichen Nutzung eines Dienstes durch die EU-Strafverfolgungsbehörden ergibt, wie er von Clearview AI angeboten wird*", und äußerte ernsthafte Zweifel.

15. Die Anzahl der verschiedenen Fälle in Europa und anderswo zeigt, dass Einzelpersonen und Aufsichtsbehörden große und weit verbreitete

Authority for Privacy Protection found in February 2021 that the Swedish Police Authority had unlawfully used Clearview's services and processed personal data in breach of the Swedish Criminal Data Act, the implementing legislation of the Law Enforcement Directive (2016/680) ("**LED**") (Integritetsskydds myndigheten, 'Police unlawfully used facial recognition app', 11 February 2021, available at https://www.imy.se/nyheter/police-unlawfully-used-facial-recognition-app/). Various other countries opened investigations into Clearview's practices, such as Italy (Wired, 'Il Garante italiano della privacy indaga sulla più controversa società di riconoscimento facciale al mondo', 15 April 2021, available at https://www.wired.it/attualita/tech/2021/04/15/riconoscimento-facciale-garante-privacy-clearview-ai/).

14. The European Data Protection Board ("**EDPB**"), following questions from Members of the European Parliament raising concerns about Clearview, issued a preliminary assessment on 10 June 2020 (EDPB, Letter to Members of the European Parliament, Ref: OUT2020-0052, 10 June 2020, available at https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-response-meps-sophie-t-veld-moritz-korner-michal-simecka_en). This assessment focused on "*the compliance and lawfulness of processing resulting from the possible use by EU law enforcement authorities of a service such as offered by Clearview AI*", expressing serious doubts.

15. The number of different cases raised in Europe and elsewhere demonstrates keen and widespread concern from individuals and regulators about Clearview's practices. Yet, to this date, no efforts have

Bedenken über die Praktiken von Clearview haben. Bis heute wurden jedoch keine Anstrengungen unternommen, um einen koordinierten Ansatz für dieses an sich globale Problem zu verfolgen. Ein koordinierter Ansatz ist in Europa längst überfällig, da es über eines der weltweit stärksten Rahmenbedingungen für Datenschutz und den Schutz der Privatsphäre verfügt. Ein fragmentierter Ansatz würde den Wert und die Kraft der GDPR und der LED beeinträchtigen, wenn allen europäischen Bürgern das gleiche Maß an Schutz der Privatsphäre geboten wird.

2.2. Beschwerdeführer ist in der Clearview AI Datenbank

16. Der Beschwerdeführer stellte via Email (**Beilage 3**) am 28. April 2021 ein Auskunftsverlangen bei Clearview. In Übereinstimmung mit den Identifizierungs- und (fraglich ob effektiven) Authentifizierungsanforderungen von Clearview stellte er ein Profilfoto und ein geschwärztes Foto seines nationalen Personalausweises zur Verfügung (**Beilagen 3a und 3b**).

17. Am 29. April 2021 antwortete Clearview per Email (**Beilage 4**) auf das Auskunftsverlangen mit einer PDF-Datei, die fünf Suchergebnisse zum Profil des Beschwerdeführers in der Datenbank von Clearview zeigte (**Beilage 4a**).

3. DSB IST ZUSTÄNDIGE BEHÖRDE FÜR DIE BESCHWERDE

18. Clearview hat keine Hauptniederlassung in der EU im Sinne des Artikel 4(16)(a) DSGVO. Der Beschwerdeführer ist in Österreich wohnhaft. Folglich ist die DSB die gemäß Artikel 55(1) DSGVO zuständige Behörde für diese Beschwerde.

been made to adopt a coordinated approach to this intrinsically global issue. A coordinated approach is long overdue in Europe, which boasts one of the strongest privacy and data protection frameworks in the world. A fragmented approach would detract from the value and force of the GDPR and LED in bringing the same level of privacy protection to all European citizens.

2.2. Complainant is in Clearview AI's database

16. The Complainant submitted a subject access request to Clearview on April 28, 2021. In line with Clearview's identification and (questionable whether effective) authentication requirements, he provided a profile photo and a redacted photo of his national ID card (**Attachments 3a and 3b**).

17. On April 29, 2021, Clearview responded to the subject access request by email with a PDF file (**Attachment 4**) that contained five search results of the Complainant's profile in Clearview's database (**Attachment 4a**).

3. DSB IS COMPETENT TO DEAL WITH THE COMPLAINT

18. Clearview does not have a main establishment in the EU in the meaning of Article 4(16)(a) GDPR. The Complainant resides in Austria. Consequently, the DSB is the competent authority to deal with this complaint according to Article 55(1) GDPR.

4. BESCHWERDEGRÜNDE

19. Clearview verstößt gegen die DSGVO wie folgt und weiter ausgeführt:

    i. Fehlen einer Rechtsgrundlage gemäß Artikel 6(1) DSGVO.
    ii. Fehlen einer Rechtmäßigkeitsbedingung gemäß Artikel 9(2) DSGVO.
    iii. Verstoß gegen Artikel 5(1)(a) DSGVO, Grundsatz von Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz.
    iv. Verstoß gegen Artikel 5(1)(b) DSGVO, Grundsatz der Zweckbindung.
    v. Verstoß gegen Artikel 27(1) DSGVO, Benennen eines Vertreters in der Union.

20. Dies ist unbeschadet etwaiger anderer DSGVO-Verstöße.

21. Bevor wir die die Verstöße näher begründen werden, zeigen wir zunächst wieso

    i. die DSGVO auf Clearviews Verarbeitungstätigkeiten Anwendung findet und wieso
    ii. Clearview personenbezogene Daten und besondere Kategorien von personenbezogenen Daten verarbeitet.

4.1. Die Verarbeitung Clearviews unterfällt der DSGVO

22. Clearviews Verarbeitung unterfällt jedenfalls dem Anwendungsbereich gemäß Artikel 3(2)(b) DSGVO.

4. GROUNDS FOR THE COMPLAINT

19. Clearview violates the GDPR as follows and as further developed:

    i. Lack of lawful basis under Article 6(1) GDPR.
    ii. Lack of lawful condition under Article 9(2) GDPR.
    iii. Violation of Article 5(1)(a) GDPR, the lawfulness, fairness and transparency principle.
    iv. Violation of Article 5(1)(b) GDPR, the purpose limitation principle.
    v. Violation of Article 27(1) GDPR, appointing a representative in the Union.

20. This is without prejudice to any other GDPR violations that the competent supervisory authority may find.

21. Before presenting the violations, we will first put forward why

    i. Clearview's processing is subject to the GDPR, and why
    ii. Clearview processes personal data and special categories of personal data.

4.1. Clearview's processing is subject to the GDPR

22. Clearview's processing is at least subject to the GDPR's scope under Article 3(2)(b) GDPR.

23. Artikel 3(2)(b) DSGVO eröffnet einen weiten Anwendungsbereich. Jeder Webseitenbetreiber oder nachgelagerter Verantwortlicher (zB Data Brokers im Rahmen von Werbesystemen) weltweit, der seine europäischen Nutzer in identifizierter oder identifizierbare Weise verfolgt, ist vom Anwendungsbereich der DSGVO erfasst (vgl. Hornung in Simits/Hornung/Spiecker gen. Döhmann, Art. 3 Rn. 61 DSGVO).

24. Insbesondere erfasst die DSGVO jede Form der Verfolgung im Internet, die ihrer Intensität nach einer „Überwachung" der Betroffenen gleichkommt (Zerdick in Ehmann, Art. 3 DSGVO Rn. 19).

25. **Technologieneutrale Formulierung.** So ist anerkannt, dass das Verfolgen durch Cookies, Tags und Pixel in den Anwendungsbereich von Artikel 3(2)(b) DSGVO fällt. Erst recht eröffnet eine Verfolgung betroffener Personen im Internet durch das Abgleichen von biometrischen Daten, wie von Clearview praktiziert, den Anwendungsbereich von Artikel 3(2)(b) DSGVO. Insbesondere erfasst das Abgleichen im Zusammenhang mit Kontext-Daten (zB aus Social Media Profilen) auch das „Verhalten" des Betroffenen.

26. Artikel 3(2)(b) DSGVO differenziert nicht zwischen den technischen Wegen der Datenverarbeitung oder dem Inhalt der gesammelten Informationen. Es kann daher keinen Einfluss auf die Anwendbarkeit der DSGVO haben, ob Clearview etwa Cookie-Daten oder Bilddaten von europäischen Nutzern sammelt.

23. Article 3(2)(b) GDPR opens a wide scope of application. Any website operator or downstream controller (e.g., data brokers in the context of advertising systems) worldwide that tracks its European users in an identified or identifiable way is covered by the scope of the GDPR (see Hornung in Simits/Hornung/Spiecker gen. Döhmann, Art. 3 para 61 GDPR).

24. In particular, the GDPR covers any form of tracking on the Internet which, in terms of its intensity, is tantamount to "surveillance" of the data subjects (see Hornung in Simits/Hornung/Spiecker gen. Döhmann, Art. 3 para 61 GDPR).

25. **Technology-neutral wording**. Thus, it is recognized that tracking through cookies, tags and pixels falls within the scope of Article 3(2)(b) GDPR. A fortiori, tracking of data subjects on the Internet through matching of biometric data, as practiced by Clearview, opens the scope of Article 3(2)(b) GDPR. In particular, matching in the context of contextual data (e.g., from social media profiles) also covers the "behaviour" of the data subject.

26. Article 3(2)(b) GDPR does not differentiate between the technical ways of processing data or the content of the information collected. Therefore, whether Clearview collects, for example, cookie data or image data from European users cannot affect the applicability of the GDPR.

27. **Breite Formulierung von Artikel 3(2)(b) DSGVO.** Im Gegenteil, Artikel 3(2)(b) DSGVO kann bereits Anwendung finden, wenn die Datenverarbeitung des Verantwortlichen damit „*im Zusammenhang steht*" – eine extrem breite Formulierung.

28. Ob eine Verarbeitung mit einer Beobachtung des Verhaltens von betroffenen Personen „*im Zusammenhang steht*", muss auch anhand der möglichen nachfolgenden Verarbeitung personenbezogener Daten festgemacht werden (DSGVO-Erwägungsgrund 24 S. 2). Eine der Verfolgung nachgelagerte (geplante) Verarbeitung beeinflusst bereits die Einordnung der ersten Stufe als „Beobachtung" (Piltz in Gola, Art. 3 DSGVO Rn. 33; Klar in Kühling/Buchner, Art. 3 Rn. 91, 92 DSGVO).

29. Der Verordnungsgeber ist dadurch der Forderung der ehemaligen Art.-29-Datenschutzgruppe nachgekommen, die eine Verhaltensbeobachtung losgelöst von einer Profilerstellung erfassen wollte (Klar in Kühling/Buchner, Art. 3 Rn. 91, 92 DSGVO).

30. Die Anwendbarkeit der DSGVO teilen auch andere Aufsichtsbehörden, so z.B. der HmbBfDI. Dieser teilte am am 27. Januar 2021 aufgrund der Beschwerde einer betroffenen Person mit Wohnsitz in Hamburg seine Absicht mit, Clearview anzuweisen, bestimmte Schritte zur Löschung der Daten der betroffenen Person zu unternehmen. Der HmbBfDI machte seine eigene Zuständigkeit und die Anwendung der GDPR geltend, nachdem er zu dem Schluss gekommen war, dass Clearview das Verhalten der betroffenen Personen in der Union überwacht, und stellte insbesondere fest, dass *„es der Zweck des Unternehmens ist, Personen identifizieren zu können. Eine solche Identifizierung ist möglich, indem Veröffentlichungen/Profile/Accounts von Nutzern, die mit einem Foto verbunden sind, wie insbesondere in sozialen*

27. **Broad formulation of Article 3(2)(b) GDPR.** Article 3(2)(b) GDPR already applies if the Controller's processing is "*related to*" it - an extremely broad formulation.

28. Whether a processing operation is "*related to*" an observation of the behaviour of data subjects must also be determined on the basis of the possible subsequent processing of personal data (recital 24, p. 2). Downstream (planned) processing already influences the classification of the first stage as "observation" (Piltz in Gola, Art. 3 GDPR para. 33; Klar in Kühling/Buchner, Art. 3 para. 91, 92 GDPR).

29. As such, the legislator has complied with the demand of the former Art. 29 WP, which wanted to cover behavioral monitoring separately from profiling (Klar in Kühling/Buchner, Art. 3 para. 91, 92 GDPR).

30. Other supervisory authorities share the opinion that the GDPR is applicable, such the HmbBfDI. Following a complaint submitted by a data subject residing in Hamburg, on 27 January 2021 the HmbBfDI communicated its intention to order Clearview to take certain steps to delete the data subject's data. The HmbBfDI asserted its own competence and application of the GDPR after concluding that Clearview does monitor the behaviour of data subjects in the Union, in particular noting that "*it is the purpose of the company to be able to identify individuals. Such identification is possible by storing publications/profiles/accounts of users linked to a photograph, such as in particular in social networks, forums or blogs, in a profile, or at least being able to create a profile of an individual at any time. This*

Netzwerken, Foren oder Blogs, in einem Profil gespeichert werden oder zumindest jederzeit ein Profil einer Person erstellt werden kann. Dieser nachträgliche Einsatz von Techniken zur Verarbeitung personenbezogener Daten mit dem Ziel der Profilerstellung ist ein entscheidendes Indiz"(Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Letter to Clearview AI Inc. - Consultation prior to an order pursuant to Article 58(2)(g) GDPR, 27. Januar 2021, via https://noyb.eu/sites/default/files/2021-01/545_2020_Anh%C3%B6rung_CVAI_ENG_Redacted.PDF). Wir sehen keinen Grund, warum das ICO zu einer anderen Schlussfolgerung als der HmbBfDI hinsichtlich der Anwendbarkeit der DSGVO gelangen sollte.

31. In einem ähnlichen Fall machte die niederländische Datenschutzbehörde die Anwendbarkeit der DSGVO und ihre Zuständigkeit gegenüber dem Controller locatefamily.com geltend, welcher personenbezogene Daten wie Adressen und Namen "scraped", um Kontaktinformationen zu Einzelpersonen bereitzustellen (siehe Autoriteit Persoonsgegevens, 10. Dezember 2020, via https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/20210512_boetebesluit_ap_locatefamily.pdf).

32. Schließlich zeigte eine frühere Version der Datenschutzrichtlinie von Clearview, dass sich das Unternehmen offen der Zuständigkeit der Datenschutzbehörden des EWR unterwarf: „*Einwohner des Europäischen Wirtschaftsraums oder der Schweiz, die eine Beschwerde einreichen oder eine Streitigkeit im Zusammenhang mit der Verarbeitung personenbezogener Daten durch Clearview AI beilegen möchten, können sich kostenlos an die zuständige Datenschutzbehörde*

subsequent use of personal data processing techniques aimed at profiling is a decisive indicator" (Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Letter to Clearview AI Inc. - Consultation prior to an order pursuant to Article 58(2)(g) GDPR, 27 January 2021, available at https://noyb.eu/sites/default/files/2021-01/545_2020_Anh%C3%B6rung_CVAI_ENG_Redacted.PDF). We see no reason why the DSB should reach a different conclusion from the HmbBfDI as to applicability of the GDPR.

31. In a similar case, the Dutch DPA asserted the applicability of the GDPR and its jurisdiction over the Controller locatefamily.com, which scrapes personal data such as addresses and names to provide contact information on individuals (see Autoriteit Persoonsgegevens, 10 December 2020, available at https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/20210512_boetebesluit_ap_locatefamily.pdf).

32. Finally, a previous version of Clearview's privacy policy showed that it openly submitted itself to jurisdiction of EEA DPAs: "*Residents of the European Economic Area or of Switzerland who wish to submit a complaint or seek resolution of a dispute related to Clearview AI's processing of personal data may seek appropriate recourse free of charge by contacting the appropriate Data Protection Authority (DPA) in their respective country*" (**Attachment 5**).

(DPA) in ihrem jeweiligen Land wenden, um geeignete Rechtsmittel einzulegen" (**Beilage 5**).

33. Diese Datenschutzerklärung wurde im März 2021 durch eine Version ersetzt, die darauf achtet, sich nicht auf Bewohner des EWR oder die europäische Gesetzgebung zu beziehen (**Beilage 6**), anscheinend, um dieses Argument zu umgehen. Zum Zeitpunkt der Erstellung dieses Dokuments sind die alte Version der Datenschutzrichtlinie sowie ein "EU/UK/Schweiz Data Access Form" und ein "EU/UK/Schweiz/Australien Opt-Out"-Formular immer noch online verfügbar, wenn auch von der Clearview-Website nicht mehr direkt verlinkt (EU/UK/Schweiz Data Access Form, verfügbar unter https://clearviewai.typeform.com/to/ePcsEp und EU/UK/Schweiz/Australien Opt-Out, verfügbar unter https://clearviewai.typeform.com/to/zqMFnt). Diese beiden Formulare waren zuvor über eine Seite "Privacy Requests Form" verfügbar (Clearview AI, "Privacy Request Forms", verfügbar im Wayback Machine Internet Archive, https://web.archive.org/web/20210303033642/https://clearview.ai/privacy/requests). Da es jedoch keine Beweise dafür gibt, dass Clearview seine Praktiken geändert noch die Verarbeitung personenbezogener Daten von Einwohnern der EU eingestellt hat, sehen wir keinen Grund zu der Annahme, dass sich die Rechtsprechung zu seinen Praktiken in irgendeiner Weise geändert hat.

33. This privacy policy was replaced in March 2021 by a version that takes care not to reference residents of the EEA or European legislation (**Attachment 6**) seemingly so as to evade this submission argument. At the time of writing, the old version of the privacy policy and an "EU/UK/Switzerland Data Access Form" and "EU/UK/Switzerland/Australia Opt-Out" form, are still available online, though de-referenced from Clearview's website (EU/UK/Switzerland Data Access Form, available at https://clearviewai.typeform.com/to/ePcsEp and EU/UK/Switzerland/Australia Opt-Out, available at https://clearviewai.typeform.com/to/zqMFnt). These two forms were previously available through a "Privacy Requests Form" page (Clearview AI, "Privacy Request Forms", available at Wayback Machine Internet Archive, https://web.archive.org/web/20210303033642/https://clearview.ai/privacy/requests). As there is no evidence that Clearview has changed its practices nor stopped processing personal data of residents of the EU, as evidenced by the Complainant's subject access results, we see no reason to think that jurisdiction over their practices has changed in any way.

4.2. Clearview verarbeitet personenbezogene Daten und besondere Kategorien von personenbezogenen Daten

4.2.1. Clearview verarbeitet personenbezogene Daten

34. Erstens sind die Photos, die Clearview aus öffentlich zugänglichen Internetquellen sammelt, personenbezogene Daten. Photos fallen unter der Definition personenbezogener Daten nach Artikel 4(1) DSGVO, insbesondere bei Auslegung mit Hilfe von Erwägungsgrund 26 DSGVO: „*Die Grundsätze des Datenschutzes sollten für alle Informationen gelten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.. […] Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern*". Aufgrund der Einzigartigkeit eines Gesichts ermöglicht eine Fotografie eines Gesichts notwendigerweise durch „menschliche" Erkennung die Identifizierung eines Individuums. Wie die Technologie von Clearview zeigt, ermöglicht sie notwendigerweise auch die Identifizierung durch Maschinenerkennung.

35. Eine solche Schlussfolgerung steht auch im Einklang mit der Rechtsprechung des Gerichtshofs der Europäischen Union (**EuGH**). Letzterer hat festgestellt, dass „*das von einer Kamera aufgenommene Bild einer Person personenbezogene Daten im Sinne von Artikel 2 Buchstabe a der Richtlinie 95/46 darstellt, da es die Identifizierung der betreffenden Person ermöglicht*" (Case C-212/13 *František Ryneš v Úřad pro ochranu osobních údajů* [2014] ECLI:EU:C:2014:2428, RN 22). Die

4.2. Clearview processes personal data and special categories of personal data

4.2.1. Clearview processes personal data

34. First, the images that Clearview collects from publicly available Internet sources are personal data. Photographs fall within the definition of personal data under Article 4(1) GDPR, especially as interpreted with the help of Recital 26 GDPR: "*The principles of data protection should apply to all information relating to an identified or identifiable natural person. […] In determining whether a natural person is identifiable, account should be taken of all the means, such as uniqueness, reasonably likely to be used by the controller or by any other person to identify the natural person directly or indirectly.*" Owing to the uniqueness of a face, a photograph of a face necessarily enables, through "human" recognition, the identification of an individual. As demonstrated by Clearview's technology, it also necessarily enables identification through machine recognition.

35. Such a conclusion is also in line with the case law of the Court of Justice of the European Union ("**CJEU**"). The latter has held that "*the image of a person recorded by a camera constitutes personal data within the meaning of Article 2(a) of Directive 95/46 inasmuch as it makes it possible to identify the person concerned*" (Case C-212/13 *František Ryneš v Úřad pro ochranu osobních údajů* [2014] ECLI:EU:C:2014:2428, para 22). The definition of personal data under Directive 95/46 is, in essence, the same as the one contained within Article 4(1) of the GDPR.

Definition personenbezogener Daten gemäß der Richtlinie 95/46 entspricht im Wesentlichen der Definition in Artikel 4(1) DSGVO.

36. Zweitens können die Metadaten, die Clearview auch erhebt, speichert und mit den Bildern verknüpft, persönliche Daten enthalten. Wie aus den Ergebnissen des Auskunftsverlangens des Beschwerdeführers ersichtlich ist, enthält der unter den Suchergebnissen angegebene „Bildindex" Beschreibungen des Bildes und/oder der Webseite, auf der das Bild gefunden wurde, und kann personenbezogene Daten wie Namen von Personen enthalten - einschließlich des Namens einer anderen Person, dessen Einzelheiten wir abgegriffen haben. Dies bestätigt auch, dass die von Clearview gesammelten Fotos personenbezogene Daten sind, da sie „indirekt" die Identifizierung einer betroffenen Person ermöglichen können - der Verantwortliche verfügt über „*Mittel, die vernünftigerweise eingesetzt werden könnten*" um die betroffene Person zu bestimmen, was die Person indirekt identifizierbar macht, wie der EuGH in *Breyer* feststellte (Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* [2016] ECLI:EU:C:2016:779, RN 48).

37. Drittens werden diese persönlichen Daten gesammelt, gespeichert, durch Indizierung über Vektoren strukturiert und abgerufen, wenn ein Benutzer eine Suche durchführt. Dies sind alles Vorgänge, die Teil der Definition von „Verarbeitung" gemäß Artikel 4(2) DSGVO sind.

4.2.2. Clearview verarbeitet besondere Kategorien personenbezogener Daten

38. Zudem verarbeitet Clearview systematisch besondere Kategorien von Daten im Sinne von Artikel 9(1) DSGVO.

36. Second, the metadata that Clearview also collects, stores and associates with the images can contain personal data. As can be seen from the results of the Complainant's subject access request, the "Image Index" provided under face results contain descriptions of the image and/or webpage where the image was found, and can contain personal data such as names of individuals. This also reaffirms that the photos collected by Clearview are personal data, as they can "indirectly" enable identification of a data subject – the controller has "*the means which may likely reasonably be used in order to identify the data subject*", which makes the individual indirectly identifiable, as per the CJEU in *Breyer* (Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* [2016] ECLI:EU:C:2016:779, para 48).

37. Third, this personal data is collected, stored, structured through indexing via vectors, and retrieved when a user performs a search. These are all operations that form part of the definition of "processing" under Article 4(2) GDPR.

4.2.2. Clearview processes special categories of personal data

38. Moreover, Clearview systematically processes special categories data as prohibited by Article 9(1) GDPR.

39. Erwägungsgrund 51 DSGVO: „*Die Verarbeitung von Lichtbildern sollte nicht grundsätzlich als Verarbeitung besonderer Kategorien von personenbezogenen Daten angesehen werden, da Lichtbilder nur dann von der Definition des Begriffs ‚biometrische Daten' erfasst werden, wenn sie mit speziellen technischen Mitteln verarbeitet werden, die die eindeutige Identifizierung oder Authentifizierung einer natürlichen Person ermöglichen.*"

40. Während dies dazu führt, dass die Fotos von Gesichtern, die Clearview aus Online-Quellen erhebt, nicht notwendigerweise als besondere Kategorie personenbezogener Daten zu qualifizieren sind, stellt es auch klar, dass die Fotos zu solchen werden, sobald sie gemäß Schritt iii (siehe oben) des Verarbeitungsprozesses von Clearview verarbeitet werden. Das Scannen jedes Gesichts, die Extraktion seiner eindeutig identifizierenden Gesichtsmerkmale und die Übersetzung dieser Merkmale in Vektoren ist eine Verarbeitung mit „*speziellen technischen Mitteln, […] die die eindeutige Identifizierung oder Authentifizierung einer natürlichen Person ermöglichen*", wie in Artikel 4(14) DSGVO definiert.

41. Darüber hinaus können die gesammelten, gespeicherten und mit Gesichtsbildern verknüpften Metadaten personenbezogene Daten enthalten, die „*rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit*" offenbaren. Hierbei handelt es sich um Daten aus speziellen Kategorien. Zum Beispiel können Gesichtsbilder auf der Website eines Kirchenverbands oder auf der Website eines Gewerkschaftsmitglieds gefunden werden, wodurch eindeutig identifizierbare Personen solchen Merkmalen zugeordnet werden.

39. According to Recital 51 of the GDPR, "*[t]he processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person.*"

40. While this provides that the photographs of faces that Clearview collects from online sources are not necessarily special categories data, it also makes clear that these photographs become so as soon as they are processed through step iii (see above) of Clearview's database building. The scanning of every face, extraction of its uniquely identifying facial features, and translation of these features into vectors, consist of "*specific technical means allowing the unique identification […] of a natural person*", as defined in Article 4(14) GDPR.

41. In addition, the metadata collected, stored and associated to facial images can contain personal data that can reveal "*racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership*", which is special categories data. For example, facial images can be found on a churchgoers' association website, or on a trade union members' website, thereby associating uniquely identifiable individuals to such characteristics.

42. Zudem, als Nebenbemerkung, sollte auch beachtet werden, dass Clearview die personenbezogenen Daten von Kindern verarbeitet, deren Gesichtsbilder online verfügbar sind (siehe Brief von Edward J. Markey (United States Senator) an Clearview CEO Herrn Hoan Ton-That (3. März 2020), S. 2, via https://www.markey.senate.gov/imo/media/doc/Markey%20Letter%20-%20Clearview%20II%203.3.20.pdf, zitierend: Kashmir Hill and Gabriel J.X. Dance, '*Clearview's Facial Recognition App Is Identifying Child Victims of Abuse*', New York Times, 7. Februar 2020, via https://www.nytimes.com/2020/02/07/business/clearview-facial-recognition-child-sexual-abuse.html), deren Verarbeitung in der gesamten GDPR noch strengeren Einschränkungen unterliegt (zB Artikel 8, 12(1), 17(1)(f) DSGVO, EG 38).

4.3. Keine Rechtsgrundlage nach Artikel 6(1) DSGVO

43. Clearview kann sich auf keine Rechtsgrundlage berufen, um seine Verarbeitungstätigkeiten zu rechtfertigen.

4.3.1. Berechtigte Interessen – Artikel 6(1)(f) DSGVO

44. Die einzige Rechtsgrundlage, auf die sich Clearview überhaupt theoretisch stützen könnte, um die Erhebung der Fotos und die anschließende biometrische Verarbeitung und Aufnahme in Clearviews Datenbank zu rechtfertigen, und auf die sich Clearview anscheinend auch stützt, ist „berechtigte Interessen" gemäß Artikel 6(1)(f) DSGVO. Dies ergibt sich aus der offensichtlichen Nichtanwendbarkeit anderer Rechtsgrundlagen und der Tatsache, dass sich Clearview in der alten Version seiner Datenschutzrichtlinie ausdrücklich auf eine solche Grundlage stützte: „*Die Verarbeitung ist*

42. Moreover, as a side comment, it should also be noted that Clearview processes the personal data of children whose facial images are available online (see letter from Edward J. Markey (United States Senator) to Clearview CEO Mr. Hoan Ton-That (3 March 2020), p. 2, available at: https://www.markey.senate.gov/imo/media/doc/Markey%20Letter%20-%20Clearview%20II%203.3.20.pdf, citing Kashmir Hill and Gabriel J.X. Dance, 'Clearview's Facial Recognition App Is Identifying Child Victims of Abuse', New York Times, 7 February 2020, available at https://www.nytimes.com/2020/02/07/business/clearview-facial-recognition-child-sexual-abuse.html), the processing of which is subject to even more onerous restrictions throughout the GDPR (eg Articles 8, 12(1), 17(1)(f) GDPR, and Recital 38).

4.3. Lack of lawful basis under Article 6(1) GDPR

43. Clearview cannot rely on any lawful basis to justify any of its processing activities.

4.3.1. Legitimate Interests – Article 6(1)(f) GDPR

44. The only lawful basis on which Clearview could feasibly rely for the collection of photos and their subsequent biometric processing and placement into Cleaview's database, and on which it seems to rely is "legitimate interests" (Article 6(1)(f) GDPR). This can be seen from the obvious inapplicability of other legal bases, and the fact that in the previous version of its privacy policy, Clearview explicitly relied on this basis: "*the processing is necessary for the legitimate interests of Clearview, and does not unduly affect your interests or fundamental rights and freedoms*".

für die berechtigten Interessen von Clearview erforderlich und beeinträchtigt nicht in unangemessener Weise Ihre Interessen oder Grundrechte und -freiheiten".

45. Die anderen Rechtsgrundlagen, auf die sich Clearview berufen wollte, galten nur für personenbezogenen Daten von Nutzer des Clearview Diensts. Zum Beispiel könnte die Rechtsgrundlage „*erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen*" (Artikel 6(1)(d) DSGVO) nur für den letzten Abschnitt der Verarbeitung im Lebenszyklus des Clearview-Dienstes gelten, d. h. wenn es z.B. von einer Strafverfolgungsbehörde im Rahmen der Untersuchung einer festgestellten Straftat verwendet wird - sie kann nicht die gesamte vorherige Verarbeitung rechtfertigen, insbesondere wo die „Erforderlichkeit" vollkommen hypothetisch ist.

46. Gemäß Erwägungsgrund 47 DSGVO:

> *Die Rechtmäßigkeit der Verarbeitung kann durch die berechtigten Interessen eines Verantwortlichen, auch eines Verantwortlichen, dem die personenbezogenen Daten offengelegt werden dürfen, oder eines Dritten begründet sein, sofern die Interessen oder die Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen;* ***dabei sind die vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, zu berücksichtigen****. Ein berechtigtes Interesse könnte beispielsweise vorliegen, wenn* ***eine maßgebliche und angemessene Beziehung zwischen der betroffenen Person und dem Verantwortlichen*** *besteht, z. B. wenn die betroffene Person ein Kunde des Verantwortlichen ist oder in seinen Diensten steht. Auf jeden Fall wäre das Bestehen eines berechtigten Interesses besonders sorgfältig abzuwägen, wobei auch zu prüfen ist,* ***ob eine betroffene Person zum***

45. The other bases on which it sought to rely only applied to data pertaining to users of its services. For example, the legal basis "*necessary in order to protect the vital interests of the data subject or of another natural person*" (Article 6(1)(d) GDPR) could only potentially apply to the last stretch of processing in the Clearview tool's lifecycle, i.e. when used by a law enforcement authority in the context of investigation of an identified crime – it cannot justify all of the prior processing, in particular where any such necessity is still hypothetical.

46. Recital 47 GDPR provides that the legitimate interests of a controller

> *may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding,* ***taking into consideration the reasonable expectations of data subjects based on their relationship with the controller****. Such legitimate interest could exist for example where there is* ***a relevant and appropriate relationship between the data subject and the controller*** *in situations such as where the data subject is a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including* ***whether a data subject can reasonably expect at the time and in the context of*** *the collection of the personal data that processing for that purpose may take place.* (Emphasis added.)

***Zeitpunkt der Erhebung der personenbezogenen Daten und angesichts der Umstände**, unter denen sie erfolgt, vernünftigerweise absehen kann, dass möglicherweise eine Verarbeitung für diesen Zweck erfolgen wird.*
(Hervorhebungen hinzugefügt)

47. Auch wenn die Rechtsgrundlage der „berechtigten Interessen" den Verantwortlichen eine gewisse Flexibilität einräumt, bedeutet dies nicht, dass sie grenzenlos ist oder genauso geformt werden kann, dass sie zu jedem Verarbeitungsvorgang passt oder diesen rechtfertigt (ICO, '*Guide to the General Data Protection Regulation (GDPR) – Lawful basis for processing – Legitimate interests*', via https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/). Aber diese Rechtsgrundlage wird immer wieder missbraucht: Eine aktuelle Entschließung des Europäischen Parlaments warnt, dass die Grundlage der berechtigten Interessen „*sehr oft missbräuchlich als Rechtsgrundlage für die Verarbeitung genannt wird*" (European Parliament resolution of 25 March 2021 on the Commission evaluation report on the implementation of the General Data Protection Regulation two years after its application (2020/2717(RSP)), RN 7). Es geht weiter:

> *Das Europäische Parlament [...] weist darauf hin, dass sich die für die Verarbeitung Verantwortlichen weiterhin auf das berechtigte Interesse berufen, ohne die erforderliche Prüfung der Interessenabwägung vorzunehmen, die eine Bewertung der Grundrechte einschließt; ist besonders besorgt darüber, dass einige Mitgliedstaaten nationale Rechtsvorschriften erlassen, um die Bedingungen für die Verarbeitung auf der Grundlage des berechtigten Interesses festzulegen, indem sie eine Abwägung der jeweiligen Interessen des für die Verarbeitung Verantwortlichen*

47. While the 'legitimate interests' basis does allow for some flexibility on the part of controllers, this does not imply that it is without limits or can be moulded exactly to fit or justify any processing operation (ICO, 'Guide to the General Data Protection Regulation (GDPR) – Lawful basis for processing – Legitimate interests', available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/). But this legal basis keeps being abused: a recent resolution of the European Parliament warns that the legitimate interests basis is "*very often abusively mentioned as a legal ground for processing*" (European Parliament resolution of 25 March 2021 on the Commission evaluation report on the implementation of the General Data Protection Regulation two years after its application (2020/2717(RSP)), para 7). It goes on:

> *The European Parliament […] points out that controllers continue to rely on legitimate interest without conducting the required test of the balance of interests, which includes a fundamental rights assessment; is particularly concerned by the fact that some Member States are adopting national legislation to determine conditions for processing based on legitimate interest by providing for the balancing of the respective interests of the controller and of the individuals concerned, while the GDPR obliges each and every controller to undertake this balancing test individually, and to avail themselves of that legal ground […].*

und der betroffenen Personen vorsehen, während die DSGVO jeden für die Verarbeitung Verantwortlichen dazu verpflichtet, diese Abwägung individuell vorzunehmen und sich auf diesen Rechtsgrund zu berufen [...].

4.3.1.1. Abwägung der berechtigten Interessen

48. Ein Verantwortlicher, der sich auf die Rechtsgrundlage der berechtigten Interessen berufen will, muss eine Abwägung durchführen und diese Abwägung den betroffenen Personen zur Verfügung stellen ((ICO, '*Guide to the General Data Protection Regulation (GDPR) – Lawful basis for processing – Legitimate interests*', via https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/). Clearview hat keine Abwägung der berechtigten Interessen öffentlich verfügbar gemacht.

49. Eine solche Bewertung der berechtigten Interessen sollte unter Berücksichtigung der drei in Artikel 6(1)(f) DSGVO festgelegten und in den EuGH-Urteilen *Rigas Satiksme* (Case 13/16 *Rigas Satiksme* [2017] ECLI:EU:C:2017:336, RN 28-31) und *Fashion ID* (Case C-40/17 *Fashion ID* [2019] ECLI:EU:C:2019:629, RN 95) näher erläuterten Bedingungen durchgeführt werden:

    i. **Die Verfolgung eines berechtigten Interesses durch den Verantwortlichen oder durch den oder die Dritten, an die die Daten weitergegeben werden („Zweck")** - im Fall von Clearview wäre dies ein kommerzielles Interesse, d.h. die Erbringung einer Dienstleistung für Dritte im Austausch gegen Geld. Es versteht sich von selbst, dass Unternehmen die alleinige

4.3.1.1. Legitimate Interests Assessment

48. A controller who seeks to rely on the legitimate interests basis must carry out an assessment and make that assessment available to affected data subjects (ICO, 'Guide to the General Data Protection Regulation (GDPR) – Lawful basis for processing – Legitimate interests', available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/). Clearview has not made any legitimate interests assessment publicly available.

49. Such a legitimate interests assessment must be conducted with regard to the three conditions laid down by Article 6(1)(f) GDPR and further expanded upon in CJEU judgments *Rigas Satiksme* (Case 13/16 *Rigas Satiksme* [2017] ECLI:EU:C:2017:336, paras 28-31) and *Fashion ID* (Case C-40/17 *Fashion ID* [2019] ECLI:EU:C:2019:629, para 95):

    i. **The pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed ("purpose")** – in Clearview's case, this would be a commercial interest, i.e. the provision of a service to third parties in exchange for money. It is self-evident that companies cannot treat the sole pursuit of their business models or of profit as "legitimate

Verfolgung ihrer Geschäftsmodelle oder des Gewinns nicht als „berechtigte Interessen" behandeln können, weil dadurch jede Verarbeitung gerechtfertigt werden könnte. Das berechtigte Interesse der Dritten, an die die Daten weitergegeben werden, kann als Identifizierung von Personen im wirklichen Leben angesehen werden. Nimmt man den häufigsten Clearview-Kunden, eine Strafverfolgungsbehörde, so sieht Artikel 6(1) DSGVO ausdrücklich vor, dass die Rechtsgrundlage der berechtigten Interessen „*nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung [gilt]*". Bei jedem anderen Clearview-Kunden, d.h. bei privaten Unternehmen und Einzelpersonen, ist die Legitimität ihres Interesses nur spekulativ und bestenfalls von begrenzter und sicherlich fragwürdiger Natur. In jedem Fall kann ein hypothetisches und nicht definiertes Interesse Dritter die ursprünglichen Verarbeitungsvorgänge nicht rechtfertigen. In diesem Fall erfolgt die Erfassung, biometrische Verarbeitung und Speicherung von Personenbildern, bevor irgendein Kunde die Daten nutzt und bevor überhaupt absehbar ist, welchen konkreten Nutzen die Kunden von Clearview daraus ziehen werden. Wie vom Büro des kanadischen Datenschutzbeauftragten beschrieben, bestehen die Aktivitäten von Clearview lediglich aus der „*Massenidentifizierung und Überwachung von Personen durch eine private Einrichtung im Rahmen kommerzieller Aktivitäten*" (Office of the Privacy Commissioner of Canada (OPCC), PIPEDA Report of Findings #2021-001, 2. Februar 2021, via https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/, RN 72).

ii. **Die Notwendigkeit der Verarbeitung personenbezogener Daten für die Zwecke der verfolgten berechtigten Interessen („Notwendigkeit")** - sollte Clearview ein berechtigtes Interesse haben, das für diese Abwägung relevant

interests", as this would legitimise any processing. The legitimate interest of the third parties to whom the data are disclosed can be taken to be the identification of real-life individuals. Taking the most common Clearview client, a law enforcement agency, Article 6(1) GDPR explicitly provides that the legitimate interests legal basis "*shall not apply to processing carried out by public authorities in the performance of their tasks*". Taking any other Clearview client, i.e. private companies and individuals, the legitimacy of their interest is only speculative, and at best of a limited and certainly creepy nature. In any case, a hypothetical and undefined third-party interest cannot justify the original processing operations. In this case, the collection, biometric processing and storage of individuals' images is performed before any client uses the data, and before one can even envisage what specific use Clearview's clients will make of it. As described by the Office of the Privacy Commissioner of Canada, Clearview's activities consist in nothing more than "*the mass identification and surveillance of individuals by a private entity in the course of commercial activity*" (Office of the Privacy Commissioner of Canada (OPCC), PIPEDA Report of Findings #2021-001, 2 February 2021, available at https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/, para 72).

ii. **The necessity of processing personal data for the purposes of the legitimate interests pursued ("necessity")** – were Clearview to have a legitimate interest relevant to this assessment, this condition would require assessing whether

ist, müsste weiterhin überprüft werden, ob Clearviews kommerzieller Nutzen mit Mitteln erreicht werden könnte, die weniger in die Grundrechte und -freiheiten der betroffenen Personen eingreifen, gemäß dem Grundsatz, dass Ausnahmen und Einschränkungen in Bezug auf den Schutz personenbezogener Daten nur insoweit gelten dürfen, wie sie unbedingt notwendig sind (Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* [2010] EU:C:2010:662, RN 86; Case C-473/12 *IPI* [2013] EU:C:2013:715, RN 39; Case C-212/13 *Ryneš* [2014] EU:C:2014:2428, RN 28). Nachdem festgestellt wurde, dass die Interessen einer Strafverfolgungsbehörde bei dieser Abwägung nicht berücksichtigt werden können, kann nicht argumentiert werden, dass private Kunden von Clearview den Dienst für ihre Interessen nutzen *müssen*. Das Vorhandensein von weniger einschneidenden Alternativen ist entscheidend, ebenso wie der Grundsatz der Datenminimierung, demzufolge Daten „*dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein*" sein müssen (C/Jorge Juan 6 28001 – Madrid, via https://edpb.europa.eu/sites/edpb/files/article-60-final-decisions/es_2010_10_right_to_erasure_transparency_and_information_decisionpublic_redacted.pdf). Clearview gibt beispielsweise an, dass Banken ihr Tool für Sicherheits- und Hintergrundüberprüfungen nutzen können; Banken führen solche Überprüfungen jedoch schon seit Jahrzehnten ohne ein solches Tool durch. Es ist auch schwer zu verstehen, warum solche Überprüfungen nur auf der Grundlage eines Gesichtsbildes und nicht anhand anderer Identifikatoren durchgeführt werden können.

iii. **Dass die Grundrechte und -freiheiten der betroffenen Person, deren Daten schutzbedürftig sind, keinen Vorrang haben („Abwägung")** - dies erfordert eine Abwägung der Interessen des Verantwortlichen und der Auswirkungen der Verarbeitung auf die betroffene Person. In *Google Spain* vertrat

Clearview's commercial benefit could be achieved by means less intrusive of data subjects' fundamental rights and freedoms, according to the principle that derogations and limitations in relation to the protection of personal data must apply only in so far as strictly necessary (Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* [2010] EU:C:2010:662, para 86; Case C-473/12 *IPI* [2013] EU:C:2013:715, para 39; Case C-212/13 *Ryneš* [2014] EU:C:2014:2428, para 28). Having established that the interests of a law enforcement authority cannot be taken into account in this particular assessment, it cannot be argued that private clients of Clearview *need* to use the tool for their interests. The existence of less intrusive alternatives is crucial, as is the principle of data minimisation, according to which data shall be "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*" (C/Jorge Juan 6 28001 – Madrid, available at https://edpb.europa.eu/sites/edpb/files/article-60-final-decisions/es_2010_10_right_to_erasure_transparency_and_information_decisionpublic_redacted.pdf). For example, Clearview reports that banks can use their tool for security and background checks; but banks have been conducting such checks without such a tool for decades. It is also difficult to understand why such checks could only be carried out on the basis of a facial image, rather than through other identifiers.

iii. **That the fundamental rights and freedoms of the data subject whose data require protection do not take precedence ("balance")** – this requires balancing the controller's interests and the effects of processing on the data

der EuGH die Auffassung, dass die Verarbeitung personenbezogener Daten, wie von einem Suchmaschinenbetreiber durchgeführt, kann

> *die Grundrechte auf Achtung des Privatlebens und Schutz personenbezogener Daten erheblich beeinträchtigen, wenn die Suche mit dieser Suchmaschine anhand des Namens einer natürlichen Person durchgeführt wird, da diese Verarbeitung es jedem Internetnutzer ermöglicht, mit der Ergebnisliste einen strukturierten Überblick über die zu der betreffenden Person im Internet zu findenden Informationen zu erhalten, die potenziell zahlreiche Aspekte von deren Privatleben betreffen und ohne die betreffende Suchmaschine nicht oder nur sehr schwer hätten miteinander verknüpft werden können, und somit ein mehr oder weniger detailliertes Profil der Person zu erstellen.*
> (Case C-131/12 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] ECLI:EU:C:2014:317, RN 80.)

Der EuGH kam ferner zu dem Schluss, dass „*[w]egen seiner potenziellen Schwere kann ein solcher Eingriff nicht allein mit dem wirtschaftlichen Interesse des Suchmaschinenbetreibers an der Verarbeitung der Daten gerechtfertigt werden*" (Case C-131/12 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] ECLI:EU:C:2014:317, RN 81).

50. Was der EuGH hier als erheblichen Eingriff in die Grundrechte des Einzelnen beschrieben hat, ist genau das, was Clearview tut, aber mit Faktoren, die die Schwere dieses Eingriffs nur verstärken können: (a) bei Clearview braucht man nicht den Namen einer Person, um

subject. In *Google Spain*, the CJEU considered that processing of personal data such as that

> *carried out by the operator of a search engine is liable to affect significantly the fundamental rights to privacy and to the protection of personal data when the search by means of that engine is carried out on the basis of an individual's name, since that processing enables any internet user to obtain through the list of results a structured overview of the information relating to that individual that can be found on the internet – information which potentially concerns a vast number of aspects of his private life and which, without the search engine, could not have been interconnected or could have been only with great difficulty – and thereby to establish a more or less detailed profile of him.*
> (Case C-131/12 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] ECLI:EU:C:2014:317, para 80.)

The CJEU also concluded that "*[i]n the light of the potential seriousness of that interference, it is clear that it cannot be justified by merely the economic interest which the operator of such an engine has in that processing*" (Case C-131/12 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] ECLI:EU:C:2014:317, para 81).

50. What the CJEU described here as constituting significant interference with individuals' fundamental rights is precisely what Clearview is doing, but with factors that can only reinforce the seriousness of this interference: (a) with Clearview, one does not need an individual's

Suchergebnisse zu erhalten, sondern nur ihr Gesicht, das man erhalten kann, indem man einfach an einer Person auf der Straße vorbeigeht und sie fotografiert; und (b) im Fall von Clearview kann eine Person, ohne das Produkt von Clearview selbst zu benutzen, nicht wissen, welche Informationen über sie „öffentlich" verfügbar ist (wohingegen sie über Google eine Suche nach ihrem eigenen Namen und andere (Text-)Identifikatoren durchführen kann).

51. Die Stellungnahme 06/2014 zum Begriff des berechtigten Interesses der Art. 29 Datenschutzgruppe (**Art. 29-Gruppe**) (Art 29-Gruppe, *Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG.* Hinweis: Der EDSA aktualisiert diese Stellungnahme, um auf Fragen einzugehen, die in dem von der oben erwähnten Entschließung des Europäischen Parlaments angenommenen Bericht der Kommission hervorgehoben wurden. Es ist zu erwarten, dass die aktualisierte Stellungnahme eher eine strengere als eine weniger strenge Bewertung als die in dieser Vorlage dargelegte verlangt.) legt einige der Faktoren dar, die bei der Durchführung einer solchen Abwägungsprüfung zu berücksichtigen sind:

    i. **Die Art und Quelle des berechtigten Interesses** - wie oben erläutert, ist das Interesse von Clearview an der Verarbeitung ein rein kommerzielles Interesse.

    ii. **Die Auswirkungen auf die betroffenen Personen**, einschließlich:

        a. die Art der Daten, z. B. ob die Verarbeitung Daten betrifft, die als sensibel angesehen werden können, oder ob sie aus öffentlich zugänglichen Quellen gewonnen wurden - Clearview verarbeitet

name to produce search results, but only their face, which can be acquired by simply passing an individual in the street and taking their picture; and (b) in the case of Clearview, an individual cannot, without using Clearview's product themselves, know what information about them is "publicly" available (whereas they can perform a search of their own name and other text identifiers through Google).

51. The Art 29 WP Opinion on Legitimate Interests (Art 29 WP, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. NB: The EDPB is updating this opinion in order to address issues highlighted in the Commission's report adopted by the European Parliament resolution mentioned above, and that the updated opinion can only be expected to require a more, rather than less stringent assessment than that set out in this submission) sets out some of the factors to be considered when carrying out such a balancing test:

    i. **The nature and source of the legitimate interest** – as explained above, Clearview's interest in processing is a purely commercial interest.

    ii. **The impact on the data subjects**, including:

        a. the nature of the data, such as whether the processing involves data that may be considered sensitive or has been obtained from publicly available sources – Clearview processes biometric data, which is

biometrische Daten, bei denen es sich um besonders sensible Daten handelt, und wie in den Absätzen **Error! Reference source not found.**-85 unten erläutert wird, ändert die Tatsache, dass die Daten aus öffentlich zugänglichen Quellen gewonnen wurden, nichts an ihrer sensiblen Qualität und der Notwendigkeit des Schutzes der Privatsphäre. Art 29 WP stellte fest auf Seite 50:

> *Hierzu ist zunächst festzustellen, dass personenbezogene Daten, selbst wenn sie öffentlich zugänglich sind, nach wie vor als personenbezogene Daten gelten und dass ihre Verarbeitung daher weiterhin angemessene Schutzmaßnahmen erfordert. Es existiert keine Blankogenehmigung für die Wiederverwendung und erneute Verarbeitung öffentlich zugänglicher personenbezogener Daten nach Artikel 7 Buchstabe f.*

Er erkannte zwar an, dass die Tatsache, dass personenbezogene Daten öffentlich zugänglich sind, ein relevanter Faktor für die Feststellung berechtigter Interessen sein kann, warnte dann aber, dass dies nur dann der Fall sei, „*wenn die Veröffentlichung in der realistischen Erwartung der weiteren Verwendung dieser Daten für bestimmte Zwecke erfolgte (z.B.für Forschungszwecke oder für Zwecke der Transparenz und Rechenschaftspflicht)*". Wie unten ausgeführt, kann die Verarbeitung durch Clearview beim besten Willen nicht unter diese vernünftige Erwartung der Weiterverwendung fallen.

b. Die Art und Weise, wie die Daten verarbeitet werden (einschließlich der Frage, ob die Daten öffentlich bekannt gegeben oder auf andere Weise einer großen

particularly sensitive data and as will be explained below, the fact that the data was obtained from publicly available sources does not detract from its sensitive quality and need for privacy protections. The Art 29 WP noted on p. 39 that:

> *it is important to highlight that personal data, even if it has been made publicly available, continues to be considered as personal data, and its processing therefore continues to require appropriate safeguards. There is no blanket permission to reuse and further process publicly available personal data under Article 7(f).*

While recognising that the fact that personal data is publicly available may be a relevant factor in favour of finding legitimate interests, it then warned that this would only be the case "*if the publication was carried out with a reasonable expectation of further use of the data for certain purposes (e.g. for purposes of research of for purposes related to transparency and accountability).*" As explained below, by no stretch of the imagination can Clearview's processing fall within this reasonable expectation of further use.

b. the way data are being processed (including whether the data are publicly disclosed or otherwise made accessible to a large number of persons, or whether

Anzahl von Personen zugänglich gemacht werden, oder ob große Mengen personenbezogener Daten verarbeitet oder mit anderen Daten kombiniert werden, z.B. im Falle der Profilerstellung, für kommerzielle, Strafverfolgungs- oder andere Zwecke) - die von Clearview verarbeiteten Daten werden durch ihren Gesichtserkennungsalgorithmus laufen gelassen, was eine besonders eingreifende Art der Verarbeitung darstellt. Jeder von Clearviews Kunden kann auf die von Clearview verarbeiteten Daten zugreifen. Dies ist eine riesige, undefinierte und unbegrenzte Personengruppe. Darüber hinaus kann das Zusammensetzen von Informationen über das Privatleben einer Person, wie sie im Internet absichtlich oder versehentlich preisgegeben werden, dazu führen, dass ein sehr aufdringliches und intimes Bild ihres Lebens entsteht, das durch eine manuelle Online-Recherche oder die Verwendung von Schlüsselwort-Suchmaschinen niemals hätte erreicht werden können. In Anbetracht der Tatsache, dass solche Erkenntnisse dazu verwendet werden können, Entscheidungen über Verhaftungen oder strafrechtliche Verurteilungen zu treffen, können die Auswirkungen nur als höchstgradig angesehen werden.

large amounts of personal data are processed or combined with other data e.g. in case of profiling, for commercial, law enforcement or other purposes) – the data processed by Clearview is subject to being run through their facial recognition algorithm, which is a particularly intrusive type of processing. Any of Clearview's clients may access the data processed by Clearview. This is a vast, undefined and unlimited population. In addition, piecing together bits of information about an individual's private life as advertently or inadvertently disclosed on the Internet can lead to forming a very intrusive and intimate view of their lives, which could never have been achieved through manual online research or use of keyword search engines. Considering that such intelligence can be used to make decisions about arrests or criminal convictions, the impact can only be considered of the highest level.

c. Ihre angemessenen Erwartungen insbesondere in Bezug auf die Verwendung und Offenlegung der Daten im relevanten Kontext - wie unten weiter erläutert, kann die Verarbeitung durch Clearview nicht unter die angemessenen Erwartungen der betroffenen Personen in Bezug auf die Verwendung und Offenlegung der Daten fallen.

c. their reasonable expectations especially with regard to the use and disclosure of the data in the relevant context – as further explained below, Clearview's processing cannot fall within data subjects' reasonable expectations with regard to the use and disclosure of the data.

d. Der Status des Verantwortlichen und der betroffenen Person, einschließlich des Machtverhältnisses

d. the status of the data controller and data subject, including the balance of power between the data

zwischen der betroffenen Person und dem für die Datenverarbeitung Verantwortlichen, oder ob die betroffene Person ein Kind ist oder anderweitig zu einem schutzbedürftigeren Teil der Bevölkerung gehört - die Umstände der Verarbeitung durch Clearview machen die Auswirkungen auf die betroffenen Personen besonders akut. Wie Erwägungsgrund 47 DSGVO deutlich macht, sollte sich die Rechtmäßigkeit zumindest teilweise danach richten, ob aufgrund der Beziehung zwischen dem Verantwortlichen und der betroffenen Person ein berechtigtes Interesse besteht. Clearview steht nicht nur in keiner Beziehung zu den betroffenen Personen, sondern Clearviews Existenz und Aktivitäten sind den meisten betroffenen Personen völlig unbekannt. In Kombination mit der unvorhersehbaren Nutzung seines Tools durch Strafverfolgungsbehörden und private Einrichtungen auf der ganzen Welt machen diese Umstände das Kräfteverhältnis besonders ungünstig für die betroffenen Personen. Darüber hinaus verarbeitet Clearview aufgrund seiner wahllosen Praktiken zwangsläufig personenbezogene Daten von Kindern und gefährdeten Bevölkerungsgruppen. Diese Schutzbedürftigkeit wird oft noch dadurch verstärkt, dass diese Bevölkerungsgruppen keine Kontrolle über ihre Online-Identitäten haben.

Die Art. 29-Gruppe vertritt in ihrer Stellungnahme zu berechtigten Interessen auf Seite 48 die Ansicht, dass in Fällen, in denen es besonders schwierig ist, Schäden oder Beeinträchtigungen der betroffenen Personen vorherzusehen oder festzustellen, *„kommt es umso mehr darauf an, das Schwergewicht auf die Vorbeugung zu legen und dafür zu sorgen, dass Datenverarbeitungsmaßnahmen*

subject and the data controller, or whether the data subject is a child or otherwise belongs to a more vulnerable segment of the population – the circumstances of Clearview's processing make the impact on data subjects particularly acute. As Recital 47 GDPR makes clear, what is legitimate should turn at least in part on whether a legitimate interest is served due to the relationship between the controller and subject. Not only does Clearview have no relationship with the affected individuals, its existence and activities are entirely unknown to most data subjects. Combined with the unforeseeable use of its tool by law enforcement authorities and private entities around the world, these circumstances make the balance of power particularly unfavourable to data subjects. In addition, due to its indiscriminate practices, Clearview necessarily processes personal data of children and vulnerable segments of the population. This vulnerability is often compounded by these populations' lack of control over their online identities.

The Art 29 WP Opinion on Legitimate Interests, p. 37, considers that in cases where anticipating or establishing harm or damage to data subjects is especially difficult, "*it is all the more important to focus on prevention and ensuring that data processing activities may only be carried out, provided they carry no risk or a very low risk of undue*

nur dann erfolgen dürfen, wenn sichergestellt ist, dass sie keine oder zumindest nur eine sehr geringe Gefahr unzulässiger nachteiliger Folgen für die Interessen oder die Grundrechte und Grundfreiheiten der betroffenen Personen mit sich bringen".

iii. **Zusätzliche Schutzmaßnahmen, um unangemessene Auswirkungen auf die betroffenen Personen zu verhindern**, einschließlich:

a. **Datenminimierung** - Das Betriebsmodell von Clearview beruht auf Prinzipien, die der Datenminimierung entgegengesetzt sind. Durch das wahllose Sammeln und Verarbeiten von Daten mithilfe seiner Gesichtserkennungsalgorithmen ähnelt es weitgehend der Massenerfassung von Datensätzen und der Massenüberwachung.

b. **Technische und organisatorische Maßnahmen**, um sicherzustellen, dass die Daten nicht dazu verwendet werden können, Entscheidungen oder andere Handlungen in Bezug auf Einzelpersonen zu treffen („funktionale Trennung") - der letztendliche Zweck des Clearview-Produkts besteht darin, Entscheidungen und Handlungen in Bezug auf Einzelpersonen zu treffen, was erhebliche negative Auswirkungen auf deren Leben haben kann, wie weiter unten erläutert.

c. **Datenschutz durch Technikgestaltung** - Umfangreiche Verwendung von Anonymisierungstechniken, Datenaggregation, Technologien zur Verbesserung des Datenschutzes, Datenschutz durch Technikgestaltung und Datenschutzfolgenabschätzungen. Nach unserem Kenntnisstand sind keine Technologien oder Designs

negative impact on the data subjects' interests or fundamental rights and freedoms".

iii. **Additional safeguards to prevent undue impact on the data subjects**, including:

a. **data minimisation** – Clearview's operating model relies on principles opposite to data minimisation. By indiscriminately collecting and processing data through its facial recognition algorithms, it is very much akin to bulk collection of datasets and mass surveillance.

b. **technical and organisational measures** to ensure that the data cannot be used to take decisions or other actions with respect to individuals ('functional separation') – the ultimate purpose of Clearview's product is for decisions and actions to be taken with respect to individuals, which can have a substantial negative impact on their lives, as further explained below.

c. **data protection by design** - extensive use of anonymisation techniques, aggregation of data, privacy-enhancing technologies, privacy by design, privacy and data protection impact assessments. To our knowledge, no privacy-enhancing technologies or designs are integrated in Clearview's product. In any case, the very purpose of its product is to strip every

zur Verbesserung der Privatsphäre in das Produkt von Clearview integriert. In jedem Fall besteht der eigentliche Zweck seines Produkts darin, jeder Person mit irgendeiner (gewollten oder ungewollten) Online-Präsenz den Schutz zu entziehen, den sie vernünftigerweise für ihre Identität erwarten kann.

d. Erhöhte Transparenz, allgemeines und bedingungsloses Recht auf Opt-out, Datenübertragbarkeit & verwandte Maßnahmen zur Befähigung der betroffenen Personen (diese Faktoren „*spielen (…) häufig eine sehr wichtige Rolle*", Art-29-Gruppe, Stellungnahme zu berechtigten Interessen, S. 65) - dies erfordert vom Verantwortlichen, „*vorab eine sorgfältige und wirksame Prüfung (…), die nicht abstrakt ist, sondern auf dem konkreten Sachverhalt beruht, und dabei hat er auch den begründeten Erwartungen der betroffenen Personen Rechnung zu tragen*" (S. 55). Trotz mehrfacher Gelegenheiten, wie z.B. in ihrer Datenschutzrichtlinie oder den zahlreichen Auskunftsverlangen von betroffenen Personen, hat Clearview augenscheinlich nie eine Abwägung durchgeführt oder nachgewiesen. Die Aktivitäten von Clearview weisen einen völligen Mangel an Transparenz und Rechenschaftspflicht gegenüber den betroffenen Personen auf. Clearview bietet ein begrenztes Recht an, der Verarbeitung zu widersprechen. Dabei ist aber unklar, was ein Widerspruch gegen die Verarbeitung bedeuten würde. Aufgrund der Art der Clearview-Technologie ist es wahrscheinlich, dass ein Opt-out nur die Ausgabe von Suchergebnissen beeinflussen würde und nicht die weitere Sammlung von personenbezogenen Daten und die weitere Verarbeitung durch die Gesichtserkennungsalgorithmen einschränken würde.

individual with some (wilful or unintentional) online presence of the protection they can reasonably expect for their identity.

d. increased transparency, general and unconditional right to opt-out, data portability & related measures to empower data subjects (issues which play "*a crucial role in the context of Article 6(f)*" Art 29 WP Opinion on Legitimate Interests, p. 51) – this requires the controller to "*perform a careful and effective test in advance, based on the specific facts of the case rather than in an abstract manner, taking also into account the reasonable expectations of data subjects*" (p. 43). Despite multiple opportunities such as in their privacy policy, or the numerous data subject access requests they receive, Clearview has apparently never performed or shown performance of the balancing test. Clearview's activities exhibit a complete lack of transparency and accountability to data subjects. Clearview provides a limited right to opt out of processing, though it is unclear what opting out of processing would entail. Owing to the nature of Clearview's technology, it is likely that any opt out would only affect the return of results when a search is performed, and would not limit further collection of personal data and further processing through its facial recognition algorithms.

52. Unter Verwendung des obigen Rahmens zur Analyse der Anwendbarkeit der Rechtsgrundlage der berechtigten Interessen auf die Verarbeitungstätigkeiten von Clearview ist es klar, dass Clearview bei jedem einzelnen Faktor in die Kategorie „hohes Risiko, hohe negative Auswirkungen" fällt. Darüber hinaus sind die verschiedenen „rettenden" Faktoren, über die Clearview verfügt und die diese Auswirkungen mindern würden, bei ihren Aktivitäten einfach nicht vorhanden. Und da jedes berechtigte Interesse bestenfalls ein kommerzielles Interesse ist, spricht die Abwägung dagegen, dass die Verarbeitung Clearviews zulässig ist und eine Rechtsgrundlage nach Artikel 6(1)(f) DSGVO vorliegt.

53. Einige Beurteilungen der berechtigten Interessen wurden von Datenschutzbehörden in ganz Europa vorgenommen. Diese deuten auf eine sehr enge Auslegung der berechtigten Interessen hin, die sich sicherlich nicht auf die Art der systematischen und wahllosen Verarbeitung durch Clearview erstrecken können. In ihrer Entscheidung Nr. 35/2020 (Autorité de Protection des Données, Chambre Contentieuse, '*Décision quant au fond 35/2020 du 30 juin 2020*', Numéro de dossier: DOS-2019-01240, via https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-35-2020.pdf) untersuchte die Prozesskammer der belgischen Datenschutzbehörde beispielsweise, ob die Weiterverwendung des öffentlich zugänglichen Facebook-Profilbilds einer Person durch eine belgische Justizbehörde zur Durchsetzung eines „Anwesenheitsverbots" unter die berechtigten Interessen der Behörde fällt. Sie stellte fest:

> *Die DSGVO schränkt die Freiheit zur Weiterverwendung öffentlich zugänglicher personenbezogener Daten erheblich ein. Die*

52. Using the above framework to analyse the applicability of the legitimate interests legal basis to Clearview's processing activities, it is clear that on every single factor Clearview falls in the high risk, high negative impact category. In addition, the various "redeeming" factors at their disposition that would mitigate this impact are simply absent from their activities. And because any legitimate interest is at best a commercial interest, the balance lies against their processing being acceptable and granted a legal basis under Article 6(1)(f) GDPR.

53. Some assessments of legitimate interests have been made by data protection authorities around Europe and indicate a very narrow interpretation of legitimate interests that certainly cannot extend to the type of systematic and indiscriminate processing carried out by Clearview. For example, in its decision No 35/2020 (Autorité de Protection des Données, Chambre Contentieuse, 'Décision quant au fond 35/2020 du 30 juin 2020', Numéro de dossier: DOS-2019-01240, available at https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-35-2020.pdf), the Litigation Chamber of the Belgian Data Protection Authority assessed whether the re-use of an individual's publicly available Facebook profile picture by a Belgian judicial authority to enforce a "ban on presence" fell within the authority's legitimate interests. It noted that:

> *The GDPR carries a significant limitation to the freedom to re-use publicly available personal data. The Litigation Chamber notes*

Prozesskammer stellt fest, dass der anwendbare Grundsatz wie folgt lautet: Die Tatsache, dass das Profilbild einer Person der Öffentlichkeit frei zugänglich ist, bedeutet nicht, dass andere es frei verwenden können. Die Verwendung dieses Bildes ist nur möglich, wenn eine gültige Rechtsgrundlage vorliegt.
(Eigene Übersetzung aus dem Französischen.)

54. Die Prozesskammer entschied, dass die Weiterverwendung des Bildes der Person unter die Rechtsgrundlage der berechtigten Interessen fiel, da die Behörde ein berechtigtes Interesse hatte (die Durchsetzung ihres Beschlusses), für dessen Verwirklichung die Verarbeitung erforderlich war (sie konnte nicht auf andere Weise erreicht werden, und die Behörde achtete darauf, die Gesichter anderer Personen auf dem Bild unkenntlich zu machen). Diese Rechtsgrundlage war spezifisch für die individuelle Beschwerde und konnte nicht wahllos erweitert werden. Die Sorgfalt, die die belgische Datenschutzbehörde walten ließ, um die **spezifische und begrenzte** Weiterverwendung (ohne biometrische Verarbeitung) des Profilbildes des Beschwerdeführers zu genehmigen, zeigt die völlige Unverhältnismäßigkeit und Unannehmbarkeit der Genehmigung der systematischen und wahllosen Sammlung und Weiterverwendung jedes einzelnen im Internet verfügbaren Gesichtsbildes durch Clearview, insbesondere für biometrische Verarbeitungen.

55. In ähnlicher Weise führte das *Office of the Privacy Commissioner of Canada* das Äquivalent zu einer Bewertung der berechtigten Interessen in seinem Zuständigkeitsbereich durch und kam zu dem Schluss:

Wir sind der Ansicht, dass Clearview unter den gegebenen Umständen die nachfolgenden Ziele nicht verfolgt:

that the applicable principle is as follows: the fact that an individual's profile picture is freely available to the public does not mean that others can use it freely. The use of this picture is possible only if a valid legal basis exists.
(Own translation from the French.)

54. The Litigation Chamber decided that the re-use of the individual's picture did fall within the legitimate interests legal basis because the authority had a legitimate interest (the enforcement of its decision), for which the processing was necessary (it could not be achieved by any other means, and the authority took care to blur the faces of other individuals in the picture). However, this legal basis was specific to the individual complaint and could not be extended indiscriminately. The care taken by the Belgian Data Protection Authority to authorise the **specific and limited re-use** of the complainant's profile picture (without biometric processing) demonstrates the utter disproportionality and unacceptability of allowing Clearview's systematic and indiscriminate collection and re-use of every single facial image available on the Internet, in particular for biometric processing.

55. Similarly, the Office of the Privacy Commissioner of Canada conducted their jurisdiction's equivalent to a legitimate interests assessment, and concluded:

It is our view that Clearview does not, in the circumstances, have an appropriate purpose, for:

i. *das massenhafte und wahllose Abgreifen von Bildern von Millionen von Personen in ganz Kanada, einschließlich Kindern, unter den über 3 Milliarden weltweit abgegriffenen Bildern;*
ii. *die Entwicklung biometrischer Gesichtserkennungsarrays basierend auf diesen Bildern und die Aufbewahrung dieser Informationen, selbst nachdem das Quellbild oder der Quelllink aus dem Internet entfernt wurde; oder*
iii. *die spätere Verwendung und Offenlegung dieser Informationen für eigene kommerzielle Zwecke;*

wenn diese Zwecke:

iv. *in keinem Zusammenhang mit den Zwecken stehen, für die die Bilder ursprünglich gepostet wurden (z.B. soziale Medien oder berufliche Netzwerke);*
v. *oft zum Nachteil der Person sind (z.B. Ermittlungen, mögliche Strafverfolgung, Verlegenheit usw.); und*
vi. *das Risiko eines erheblichen Schadens für Personen schaffen, deren Bilder von Clearview erfasst werden (einschließlich Schäden im Zusammenhang mit einer falschen Identifizierung oder der Exposition gegenüber potenziellen Datenschutzverletzungen), wobei die überwiegende Mehrheit dieser Personen nie in eine Straftat verwickelt war und auch nie sein wird oder identifiziert wird, um bei der Aufklärung einer schweren Straftat zu helfen* (Office of the Privacy Commissioner of Canada (OPCC), PIPEDA Report of Findings #2021-001, 2. Februar 2021, via https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/, RN 76.).

56. Um die obige Bewertung der Auswirkungen auf die betroffenen Personen zu ergänzen und zu verdeutlichen, werden in den folgenden Abschnitten drei Schlüsselaspekte des Schadens hervorgehoben, der den betroffenen Personen durch das Tool von Clearview entsteht:

i. *the mass and indiscriminate scraping of images from millions of individuals across Canada, including children, amongst over 3 billion images scraped world-wide;*
ii. *the development of biometric facial recognition arrays based on these images, and the retention of this information even after the source image or link has been removed from the Internet; or*
iii. *the subsequent use and disclosure of that information for its own commercial purposes;*

where such purposes:

iv. *are unrelated to the purposes for which the images were originally posted (for example, social media or professional networking);*
v. *are often to the detriment of the individual (for example, investigation, potential prosecution, embarrassment, etc.); and*
vi. *create the risk of significant harm to individuals whose images are captured by Clearview (including harms associated with misidentification or exposure to potential data breaches), where the vast majority of those individuals have never been and will never be implicated in a crime, or identified to assist in the resolution of a serious crime*
(Office of the Privacy Commissioner of Canada (OPCC), PIPEDA Report of Findings #2021-001, 2 February 2021, available at: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/, para 76.)

56. To complement and flesh out the above assessment of impact on data subjects, the following sections highlight three key aspects of the harm caused to data subjects by Clearview's tool:

i. die anerkannten Risiken der Verarbeitung biometrischer Daten,
ii. eine unvermeidliche abschreckende Wirkung auf die Grundrechte und
iii. die besonderen Nachteile, die für schutzbedürftige Gemeinschaften zu erwarten sind.

4.3.1.1.1. Risiken Verarbeitung biometrischer Daten

57. Biometrische Daten sind eine besondere Kategorie personenbezogener Daten, da es sich um einzigartige und praktisch unveränderliche Daten handelt, die aus Merkmalen von Menschen wie Fingerabdrücken, Stimme, Gesicht, Netzhaut- und Irismustern, Handgeometrie, Gangbild oder DNA-Profilen erzeugt werden. Es handelt sich dabei an sich um sensible Daten, unabhängig davon, woher sie stammen oder wie sie erhoben werden (*S. and Marper v. UK* [GC], App nos 30562/04 and 30566/0 (ECtHR, 12. April 2008)). Wie das *Office of the Privacy Commissioner of Canada* festgestellt hat:

> *Biometrische Informationen sind unverwechselbar, variieren wahrscheinlich nicht im Laufe der Zeit, sind schwer zu ändern und weitgehend individuell. Biometrische Gesichtsdaten sind besonders sensibel, da sie ein Schlüssel zur Identität einer Person sind und die Fähigkeit unterstützen, Personen zu identifizieren und zu überwachen.*
> (Office of the Privacy Commissioner of Canada (OPCC), PIPEDA Report of Findings #2021-001, 2 February 2021, via https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/, RN 74)

i. the recognised risks of biometric data processing,
ii. an inevitable chilling effect on fundamental rights, and
iii. the particular harms to be envisaged for vulnerable communities.

4.3.1.1.1. Risks of biometric data processing

57. Biometric data is a special category of personal data because it is unique and practically unalterable data, generated from characteristics of humans, such as fingerprints, voice, face, retina and iris patterns, hand geometry, gait or DNA profiles. It is in itself sensitive data, no matter where it comes from or how it is collected (*S. and Marper v. UK* [GC], App nos 30562/04 and 30566/0 (ECtHR, 12 April 2008)). As found by the Office of the Privacy Commissioner of Canada:

> *Biometric information is distinctive, unlikely to vary over time, difficult to change and largely unique to the individual. Facial biometric data is particularly sensitive given that it is a key to an individual's identity, supporting the ability to identify and surveil individuals.*
> (Office of the Privacy Commissioner of Canada (OPCC), PIPEDA Report of Findings #2021-001, 2 February 2021, available at: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/, para 74)

58. Es ist kein Wunder, dass auch die DSB eine Datenschutz-Folgenabschätzung gemäß Artikel 35 DSGVO verlangt, sofern die Verarbeitung personenbezogener Daten umfangreich ist (DSB, Fragen & Antworten, Wann benötige ich eine Datenschutz-Folgenabschätzung?, via https://www.dsb.gv.at/download-links/fragen-und-antworten.html).

59. Wenn biometrische Technologien mangels strenger rechtlicher Rahmenbedingungen und strenger Schutzmaßnahmen verabschiedet werden, stellen sie eine ernsthafte Bedrohung für die Privatsphäre und die persönliche Sicherheit dar, da ihre Anwendung erweitert werden kann, um Diskriminierung, Profilerstellung und Massenüberwachung zu ermöglichen (Privacy International, 'Biometrics', via https://privacyinternational.org/learn/biometrics).

60. Gegenwärtig kann mit einem Dienst wie dem von Clearview der Gesichtsabdruck einer Person verwendet werden, um deren Namen und Konten in sozialen Medien zu finden und diese Informationen mit deren physischen Präsenz auf der Straße oder in den Geschäften, die sie besucht, und mit den Fotos, die sie oder ihre Freunde online posten, zu kombinieren - eine massive Ausweitung der meist begrenzten Möglichkeiten, in denen biometrische Daten bisher verwendet wurden.

61. Da es von Natur aus schwierig oder unmöglich ist, Änderungen vorzunehmen, können biometrische Daten eine Person während ihres gesamten Lebens identifizieren. Dies macht die Einrichtung biometrischer Datenbanken problematisch, da Risiken weit in die Zukunft hinein antizipiert werden müssten - sei es eine Änderung der politischen Situation oder des Regimes, ein zukünftiger

58. It is no wonder that the DSB also requires a data protection impact assessment under Article 35 GDPR if there is an extensive processing of personal data (DSB, Fragen & Antworten, Wann benötige ich eine Datenschutz-Folgenabschätzung?, available at https://www.dsb.gv.at/download-links/fragen-und-antworten.html).

59. When adopted in the absence of strong legal frameworks and strict safeguards, biometric technologies pose grave threats to privacy and personal security, as their application can be broadened to facilitate discrimination, profiling and mass surveillance (Privacy International, 'Biometrics', available at https://privacyinternational.org/learn/biometrics).

60. As it stands, with a tool like Clearview's, a person's faceprint can be used to find their name and social media accounts, and to combine that information with their physical presence in the street, the stores they visit, and the photos they or their friends post online – a massive extension of the mostly limited ways in which biometrics have been used until now.

61. As it is inherently difficult or impossible to change, biometric data can identify a person for their entire lifetime. This makes the creation of biometric databases problematic, as risks would need to be anticipated far into the future – whether that be a change in political situation or regime, a future data breach, or the development of technology meaning that biometrics can be used for new purposes, and could

Datenschutzverstoß oder die Entwicklung von Technologien, die bedeuten, dass biometrische Daten für neue Zwecke verwendet werden können und mehr Informationen über Personen offenbaren könnten, als es derzeit möglich ist. Die Erhebung und Speicherung biometrischer Daten hat somit das Potenzial, in schwerwiegender Weise missbraucht zu werden (UN High Commissioner for Human Rights, '*The right to privacy in the digital age*' (Doc.A/HRC/39/29, 3. August 2018), via https://undocs.org/A/HRC/39/29).

62. Die Art. 29-Gruppe hat bereits vor einigen Jahren die Bedeutung der Verarbeitung biometrischer Daten erkannt: „*Biometrische Daten wirken sich insoweit unwiderruflich auf die Verbindung zwischen Körper und Identität aus, als sie die Merkmale des menschlichen Körpers ‚maschinenlesbar' machen und damit vielfältige Nutzungsmöglichkeiten erschließen*" (Art. 29-Gruppe, '*Stellungnahme 3/2012 zu Entwicklungen im Bereich biometrischer Technologien*', S. 4, via https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_de.pdf). Die Art. 29-Gruppe hat den Schaden, der durch die Extraktion biometrischer Merkmale aus öffentlich zugänglichen Informationen entstehen würde, bereits vorhergesehen und die Verarbeitung durch Clearview präzise vorweggenommen:

> ***Fotos*** *im Internet, in sozialen Medien und in Online-Anwendungen zur Verwaltung und Weitergabe von Fotos dürfen nicht zur Erstellung biometrischer Templates oder zum Einlesen von Daten in ein System verwendet werden, das die automatische Erkennung der fotografierten Personen (Gesichtserkennung) ermöglichen würde, ohne dass eine konkrete Rechtsgrundlage (z.B. eine Einwilligung) für diesen neuen Zweck gegeben wäre.*
> (Art. 29-Gruppe, '*Stellungnahme 3/2012 zu Entwicklungen im Bereich biometrischer Technologien*', S. 8)

reveal more information about individuals than is currently possible. As such, the collection and storage of biometric data has the potential to be gravely abused (UN High Commissioner for Human Rights, 'The right to privacy in the digital age' (Doc.A/HRC/39/29, 3 August 2018), available at https://undocs.org/A/HRC/39/29).

62. The Art 29 WP already recognised some years ago the significance of biometric data processing: "*Biometric data changes irrevocably the relation between body and identity, because they make the characteristics of the human body 'machine-readable' and subject to further use*" (Article 29 Data Protection Working Party, 'Opinion 03/2012 on developments in biometric technologies', p. 4, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf). It already predicted the harm that would be raised by the extraction of biometric features from publicly available information, and precisely pre-empted Clearview's processing activities:

> ***Photographs*** *on the internet, in social media, in online photo management or sharing applications may not be further processed in order to extract biometric templates or enrol them into a biometric system to recognise the persons on the pictures automatically (facial recognition) without a specific legal basis (e.g. consent) for this new purpose.*
> (Article 29 Data Protection Working Party, 'Opinion 03/2012 on developments in biometric technologies', p. 7)

4.3.1.1.2. Abschreckende Wirkung auf Grundrechte

63. Die Art. 29-Gruppe erklärt, dass bei der Bewertung der Auswirkungen der Verarbeitung die „*abschreckende Wirkung, die eine fortwährende Überwachung/Verfolgung auf geschütztes Verhalten wie die Freiheit der Forschung oder die Redefreiheithaben kann, ist ebenfalls entsprechend in Betracht zu ziehen*" (Art 29-Gruppe, Stellungnahme zu berechtigten Interessen, S. 47).

64. Wir möchten auf die Rechtsprechung deutscher Gerichte und Behörden hinweisen, die die Auswirkungen der Videoüberwachung auf die Grundrechte im Rahmen der Abwägung berechtigter Interessen umfassend bewertet haben.

65. Insbesondere der Landesbeauftragte für den Datenschutz Baden-Württemberg hat die Bedeutung des Rechts auf freie Entfaltung der Persönlichkeit für die Beurteilung der Intensität der Überwachung durch Videoüberwachung hervorgehoben: (Der Landesbeauftragte für den Datenschutz Baden-Württemberg, Orientierungshilfe „*Videoüberwachung durch nicht-öffentliche Stellen*", S. 9). Er stellte fest, dass in Gaststätten, Erlebnisparks und allgemein an Orten, an denen Menschen zusammenkommen, um zu essen, zu trinken, zu diskutieren und sich zu entspannen, das Recht auf freie Entfaltung der Persönlichkeit die berechtigten Interessen des Verantwortlichen überwiegt.

66. Da das Internet zu einem Ort der Geselligkeit geworden ist, der solchen öffentlichen Räumen gleichgestellt ist, sollte derselbe Grundsatz gelten. Darüber hinaus werden die festgestellten Risiken der Videoüberwachung noch verstärkt, wenn durch die Technologie von

4.3.1.1.2. Chilling effect on fundamental rights

63. The Art 29 WP provides that in assessing the impact of the processing, "*[t]he chilling effect on protected behaviour, such as freedom of research or free speech, that may result from continuous monitoring/tracking, must also be given due consideration*" (Art 29 WP Opinion on Legitimate Interests, p. 43).

64. We also would like to draw attention to the jurisprudence of German courts and authorities, which have conducted extensive assessments of the impact of video surveillance on fundamental rights in the context of legitimate interests assessments.

65. In particular, the Data Protection Authority of Baden-Württemberg emphasized the importance of the right to free development of personality to assess the intensity of the monitoring through video surveillance (Der Landesbeauftragte für den Datenschutz Baden-Württemberg, Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen", p. 9): it found that in restaurants, adventure parks and in general places where people gather to eat, drink, discuss and relax, the right to free development of personality shall override the legitimate interests of the controller.

66. As the Internet has become a socialising place on equal footing with such public spaces, the same principle ought to apply. In addition, the risks of video surveillance identified are compounded when mass real-world identification is enabled by Clearview's technology.

Clearview eine massenhafte Identifizierung in der realen Welt ermöglicht wird.

67. Der Europäische Datenschutzbeauftragte (**EDSB**) ist ausdrücklich der Ansicht, dass SOCMINT, also genau die Praxis, die durch die Technologie von Clearview ermöglicht und erleichtert werden soll, erhebliche abschreckende Auswirkungen auf verschiedene Rechte und Freiheiten hat:

> *Die Überwachung von Social-Media-Nutzern ist eine personenbezogene Datenverarbeitungstätigkeit, die ein hohes Risiko für die Rechte und Freiheiten des Einzelnen darstellt. Die Weitergabe von Daten ist geeignet, die informationelle Selbstbestimmung einer Person zu beeinträchtigen, die Kontrolle der Betroffenen über ihre Daten weiter zu reduzieren... In der Tat hat die Verringerung des intimen Raums, der den Menschen zur Verfügung steht, als Ergebnis der unvermeidlichen Überwachung durch Unternehmen und Regierungen eine abschreckende Wirkung auf die Fähigkeit und Bereitschaft der Menschen, sich frei auszudrücken und Beziehungen zu knüpfen, auch in der zivilen Sphäre, die für die Gesundheit der Demokratie so wichtig ist.*
> (EDPS, 'Formal consultation on EASO's social media monitoring reports (case 2018-1083)' (Brussels, D(2019) 1961), S. 3, via https://edps.europa.eu/sites/edp/files/publication/19-11-12_reply_easo_ssm_final_reply_en.pdf)

68. Das Internet und die Plattformen der sozialen Medien spielen eine entscheidende Rolle für die Entwicklung des privaten sozialen und politischen Lebens des Einzelnen sowie für dessen Online-Identität. Sie bilden das digitale Lebensumfeld der heutigen öffentlichen Räume, in denen Menschen auf Informationen zugreifen, Ideen formulieren und diskutieren, abweichende Meinungen äußern, mögliche Reformen erwägen, Voreingenommenheit und Korruption aufdecken und sich

67. The European Data Protection Supervisor ("**EDPS**") explicitly considers SOCMINT, which is precisely the practice that Clearview's technology enables and is designed to facilitate, has considerable chilling effects on various rights and freedoms:

> *Social media users monitoring is a personal data processing activity that creates high risk for individuals' rights and freedoms. Repurposing of data is likely to affect a person's information self-determination, further reduce the control of data subjects over their data... Indeed, the diminution of intimate space available to people, as a result of unavoidable surveillance by companies and governments, has a chilling effect on people's ability and willingness to express themselves and form relationships freely, including in the civic sphere so essential to the health of democracy.*
> (EDPS, 'Formal consultation on EASO's social media monitoring reports (case 2018-1083)' (Brussels, D(2019) 1961), p. 3, available at https://edps.europa.eu/sites/edp/files/publication/19-11-12_reply_easo_ssm_final_reply_en.pdf).

68. The Internet and social media platforms have come to play a vital role for the development of individuals' private social and political life, as well as their online identity. They constitute the digital life setting of today's civic spaces where people access information, formulate and discuss ideas, raise dissenting views, consider possible reforms, expose bias and corruption, and organise to advocate for political, economic, social, environmental, and cultural change (Privacy

organisieren, um für politische, wirtschaftliche, soziale, ökologische und kulturelle Veränderungen einzutreten (Privacy International, '*Protecting civic spaces*', Mai 2019, via https://privacyinternational.org/sites/default/files/2019-07/Protectin%20civic%20spaces%20PI%20May%202019.pdf.).

69. Für ein gesundes, aufstrebendes und offenes Internet ist es entscheidend, dass der Einzelne sich frei fühlt, persönliche Informationen und Fotos so zu teilen, wie er es für richtig hält, ohne befürchten zu müssen, dass diese persönlichen Informationen sofort abgegriffen und für unveröffentlichte Zwecke gespeichert werden. Die Freiheit, sich in verschiedenen Internetforen so zu definieren, wie man es für richtig hält, indem man die Verbreitung verschiedener Informationen an verschiedenen Orten kontrolliert, wird durch die drohende Gefahr genommen, dass all diese verschiedenen Informationen auf Knopfdruck auffindbar und vereinheitlicht sind.

4.3.1.1.3. Risiken für gefährdete Gemeinschaften

70. Der Dienst von Clearview kann auch besonders schutzbedürftigen Personen Schaden zufügen. Für diesen Abschnitt wurden wir stark von der Arbeit der ACLU in ihren Eingaben gegen Clearview im Bundesstaat Illinois unter dem BIPA informiert und möchten darauf hinweisen (Complaint, *ACLU and others v. Clearview AI, Inc.*, Circuit Court of Cook County, Illinois, Case No.: 2020 CH 04353, via https://www.aclu.org/legal-document/aclu-v-clearview-ai-complaint).

71. Schutzbedürftige Gruppen sind einem erhöhten Risiko ausgesetzt, wenn sie bei der Ausübung ihres täglichen Lebens identifiziert werden. Überlebende von sexuellem Schaden oder kommerzieller sexueller

International, 'Protecting civic spaces', May 2019, available at https://privacyinternational.org/sites/default/files/2019-07/Protectin%20civic%20spaces%20PI%20May%202019.pdf.)

69. It is crucial for a healthy, striving and open Internet that individuals feel free to share personal information and photos as they see fit without fear of this personal information being immediately grabbed and stored for undisclosed purposes. The freedom to define oneself as one sees fit in different Internet fora, by controlling the distribution of different pieces of information in different places, is taken away by the looming threat of all this diverse information being traceable and unified at the click of a button.

4.3.1.1.3. Harms for vulnerable communities

70. Clearview's tool can also cause particular harm to vulnerable individuals. For this section we have been greatly informed by, and would like to draw attention to, the work of the American Civil Liberties Union (ACLU) in their submissions against Clearview in the state of Illinois under the BIPA (Complaint, ACLU and others v. Clearview AI, Inc., Circuit Court of Cook County, Illinois, Case No.: 2020 CH 04353, available at https://www.aclu.org/legal-document/aclu-v-clearview-ai-complaint).

71. Vulnerable groups are at heightened risk if identified when going about their lives. Survivors of sexual harm or commercial sexual exploitation, for example, or migrants, have repeatedly been targeted for

Ausbeutung zum Beispiel oder Migranten sind immer wieder zur Zielscheibe von Belästigungen oder Diskriminierungen durch Privatpersonen und Polizeibeamte gleichermaßen geworden. „*Indem das System von Clearview diesen Personen die Kontrolle und Sicherheit über ihre sensiblen biometrischen Bezeichner entzieht und ihnen der Gefahr aussetzt, es trivial einfach zu machen, sie sowohl online als auch in der physischen Welt zu identifizieren und zu verfolgen, setzt es diesen Personen Stalking, Belästigung und Gewalt aus*" (Plaintiff's response to defendant's motion to dismiss, ACLU and others v. Clearview AI, Inc., Circuit Court of Cook County, Illinois, Case No.: 2020 CH 04353). Die Angst, identifiziert zu werden, kann auch dazu führen, dass diese Personen es vermeiden, Orte und Treffen aufzusuchen, um auf die von ihnen benötigten Unterstützungsdienste zuzugreifen.

72. Darüber hinaus ermöglicht das Hashing von Vektoren, das durchgeführt wird, wenn Clearview biometrische Merkmale aus Gesichtsbildern extrahiert, potenziell eine Kategorisierung der Gesichter von Personen nach dem Grad der Ähnlichkeit. Dies eröffnet den Kunden von Clearview die Möglichkeit, automatische Gruppierungen von Menschen auf der Grundlage ihrer ethnischen Zugehörigkeit, Hautfarbe oder anderer Kategorisierungen vorzunehmen - und öffnet die Tür für diskriminierende Verfolgung und Überwachung oder Praktiken wie vorausschauende Polizeiarbeit.

73. Nachdem die vielfältigen und schwerwiegenden Risiken und Schäden dargelegt wurden, die die Aktivitäten von Clearview für die Rechte und Freiheiten des Einzelnen mit sich bringen, führt die Abwägung der berechtigten Interessen zum Ergebnis, dass keine gültige Rechtsgrundlage nach Artikel 6(1)(f) DSGVO vorliegt.

harassment or discrimination by private citizens and police officers alike. "*By divesting these individuals of control over and security in their sensitive biometric identifiers and threatening to make it trivially easy to identify and track them both online and in the physical world, Clearview's system exposes them to stalking, harassment, and violence*" (Plaintiff's response to defendant's motion to dismiss, ACLU and others v. Clearview AI, Inc., Circuit Court of Cook County, Illinois, Case No.: 2020 CH 04353). The fear of being identified may also cause these individuals to avoid attending places and meetings to access the support services they need.

72. In addition, the hashing of vectors performed when Clearview extracts biometric features from facial images potentially allows for categorisation of people's faces according to degrees of similarity. This raises the possibility for Clearview's clients to perform automatic groupings of people based on their ethnicity, colour, or other categorisation – and opens the door to discriminatory tracking and monitoring, or practices like predictive policing.

73. Having set out the multiple and serious risks and harms raised by Clearview's activities for individuals' rights and freedoms, the balance of legitimate interests assessment must lie against the finding of a valid legal basis under Article 6(1)(f) GDPR.

4.4. Fehlen einer Rechtmäßigkeitsbedingung gemäß Artikel 9(1) DSGVO

74. Zusätzlich zum Vorliegen einer Rechtsgrundlage gemäß Artikel 6 DSGVO ist die Verarbeitung von biometrischen Daten als besondere Kategorie personenbezogener Daten verboten, es sei denn, dass eine der in Artikel 9(2) DSGVO abschließend aufgeführten Bedingungen vorliegt.

75. Die Bedingung „offensichtlich öffentlich gemacht" gemäß Artikel 9(2)(e) DSGVO ist die einzige, auf die sich Clearview theoretisch verlassen könnte.

4.4.1. Offensichtlich öffentlich gemacht - Artikel 9(2)(e) DSGVO

76. Informationen, die online öffentlich zugänglich sind, sind keine automatische Rechtsgrundlage für die Verarbeitung gemäß Artikel 9 DSGVO. Wie in verschiedenen (wenn auch begrenzten) Leitlinien von Datenschutzbehörden und entsprechenden wissenschaftlichen Kommentaren verbindlich anerkannt wird (Edward S Dove and Jiahong Chen, '*What does it mean for a data subject to make their personal data 'manifestly public'? An analysis of GDPR Article 9(2)(e)*' (2021) Vol. 00, No. 0, International Data Privacy Law, 1, 2, via https://doi.org/10.1093/idpl/ipab005), muss die Ausnahme nach Artikel 9(2)(e) DSGVO eng ausgelegt werden. Insbesondere das Erfordernis, dass es sich um personenbezogene Daten handeln muss „*die die betroffene Person offensichtlich öffentlich gemacht hat*", verlangt sehr spezifische Umstände, unter denen die personenbezogenen Daten öffentlich gemacht wurden.

4.4. Lack of lawful condition under Article 9(1) GDPR

74. In addition to requiring a legal basis under Article 6, the processing of biometric data as a special category of personal data is prohibited unless one of the conditions in the exhaustive list given at Article 9(2) GDPR is met.

75. The condition of having been "*manifestly made public*" under Article 9(2)(e) GDPR is the only theoretically possible condition that Clearview could rely on.

4.4.1. Manifestly made public – Article 9(2)(e) GDPR

76. Information being publicly available online is not the same as the condition of Article 9(2)(e) GDPR. As recognised by various (even if limited) guidance from data protection authorities and related academic commentary (Edward S Dove and Jiahong Chen, 'What does it mean for a data subject to make their personal data 'manifestly public'? An analysis of GDPR Article 9(2)(e)' (2021) Vol. 00, No. 0, International Data Privacy Law, 1, 2, available at https://doi.org/10.1093/idpl/ipab005) the exception under Article 9(2)(e) GDPR must be narrowly construed. In particular, the terms "manifestly" and "by the data subject" require very specific circumstances of the personal data having been made public.

77. Erstens müssen Informationen, die online öffentlich zugänglich sind, immer noch ein erhebliches Maß an Schutz der Privatsphäre genießen. Dies ist entscheidend für ein gesundes und offenes Internet, in dem Einzelpersonen ihre Grundrechte und -freiheiten ausüben können und folgt aus dem Grundsatz der Zweckbindung, denn die Veröffentlichung ist immer zu einem bestimmten Zweck.

78. So ist die Veröffentlichung eines Lebenslaufs mit Kontaktdaten auf der eigenen Webseite für Zwecke der Arbeitssuche gedacht. Würde ein Verantwortlicher die Daten für Werbezwecke oder eine Auskunftei für die Bonitätseinstufung verwenden, wäre das eine klare Missachtung der ursprünglichen Zweckbestimmung.

79. Clearview ist der Archetyp einer scheinbar harmlosen neuen Technologie, die, wenn sie in großem Umfang eingesetzt und verwendet werden darf, das Internet, wie wir es kennen, und das Online-Verhalten des Einzelnen tiefgreifend verändern könnte. Es geht von der fehlerhaften Annahme aus, dass alles, was im Internet öffentlich zugänglich ist, sofort zu einer völlig öffentlichen Sphäre gehört und der ganzen Welt wohlwollend angeboten wird, damit sie es sofort sehen und nach Belieben weiterverwenden kann. Aber eine strikte Trennung zwischen der öffentlichen und der privaten Sphäre ist für moderne Gesellschaften, in denen große Teile unseres wirtschaftlichen, sozialen und demokratischen Lebens online geführt werden, wenig relevant. Es ist ein Missverständnis, das Internet als ein homogenes, völlig öffentliches und voll zugängliches Forum zu sehen, in dem jeder zustimmt, dass seine persönlichen Informationen „Freiwild" für alle sind, sobald sie in einen „öffentlichen" Teil des Internets gelangt sind (EDSB, 'Formal consultation on EASO's social

77. First, information publicly available online must still carry a significant degree of privacy protection. This is crucial to a healthy and open Internet where individuals can exercise their fundamental rights and freedoms, and follows from the principle of purpose limitation because every "making public" occurs for a specific purpose.

78. The making public of a CV with contact data on one's own website is for the purposes of finding a job. A controller would clearly disregard the original purpose if they were to use the data for advertising purposes or if a credit rating agency were to use the data to assess the individual's credit worthiness.

79. Clearview is the archetype of a seemingly innocuous new technology that if allowed to be deployed and used at scale, could profoundly alter the Internet as we know it and individuals' behaviour online. It is operating on the flawed assumption that what is publicly available on the Internet immediately belongs to an entirely public sphere and has been benevolently offered to the whole world to see instantly and to re-use at will. But a stark divide between the public and the private spheres bears little relevance to modern societies where major parts of our economic, social and democratic lives are led online. It is misunderstanding the Internet to see it as a homogeneous, entirely public and fully accessible forum on which everyone consents to their personal information being "fair game" for all to grab as soon as it has entered a, technically, public part of the Internet (EDPS, 'Formal consultation on EASO's social media monitoring reports (case 2018-1083)' (Brussels, D(2019) 1961), available at

media monitoring reports (case 2018-1083)' (Brussels, D(2019) 1961), via https://edps.europa.eu/sites/edp/files/publication/19-11-12_reply_easo_ssm_final_reply_en.pdf).

80. Die Gefahren einer solch krassen Trennung sind auch in der Offline-Welt sehr real, wie der EGMR bereits anerkannt hat. Wie der Gerichtshof in der Rechtssache *Peck vs. UK (*App no 44647/98, ECtHR, 28. Januar 2003, RN 53, 61-62) feststellte, stellte die Weitergabe von Videomaterial des Klägers, dessen Selbstmordversuch von Überwachungskameras aufgezeichnet wurde, an die Medien zum Zwecke der Ausstrahlung einen schwerwiegenden Eingriff in das Privatleben des Klägers dar, ungeachtet dessen, dass er sich zu diesem Zeitpunkt an einem öffentlichen Ort befand. In diesem Fall beruhte die Argumentation des EGMR auf der Annahme, dass keine Person vernünftigerweise erwarten kann, dass Filmmaterial, das sensible Aspekte ihres Privatlebens zeigt, später in den Medien veröffentlicht wird, selbst wenn ihre Handlungen „*bereits öffentlich sind* " sind *(*App no 44647/98, ECtHR, 28. Januar 2003, RN 53, 61-62).

81. Zweitens ist es für jeden, der sich auch nur einigermaßen mit der Nutzung des Internets und sozialer Medien auskennt, allgemein bekannt, dass viele Online-Fotos von Personen nicht *von der betroffenen Person* selbst veröffentlicht wurden. Mithilfe von sozialen Medien kann ein Benutzer Fotos von sich selbst und von jeder anderen Person hochladen. Diese anderen Personen (möglicherweise Freunde des Uploaders oder unbekannte Zuschauer im öffentlichen Raum) haben ihre Gesichtsbilder nicht selbst online hochgeladen und wissen möglicherweise nicht einmal, dass Fotos mit ihren Gesichtern hochgeladen wurden und im öffentlichen Internet vorhanden sind.

https://edps.europa.eu/sites/edp/files/publication/19-11-12_reply_easo_ssm_final_reply_en.pdf).

80. The dangers of such a stark divide are also very real in the offline world, as previously recognised by the ECtHR. As the Court held in *Peck v. UK (*App no 44647/98, ECtHR, 28 January 2003, paras 53, 61-62), the disclosure to the media for broadcast use of video footage of the applicant whose suicide attempt was caught on close circuit television cameras constituted a serious interference with the applicant's private life, notwithstanding that he was in a public place at the time. In that case, the ECtHR's reasoning rested on the assumption that no person could reasonably expect footage depicting sensitive aspects of their private life to be later released in the media, even if their actions are "*already in the public domain*" *Peck v. UK (*App no 44647/98, ECtHR, 28 January 2003, paras 53, 61-62).

81. Second, it is common knowledge for anyone even mildly versed in using the Internet and social media that many online photos of individuals have not been made public *by the data subject* themselves. Social media allows a user to upload photos of themselves, and of any other person. These other persons (may they be friends of the uploader or unknown bystanders in public spaces) have not themselves uploaded their facial images online, and may not even know that photos containing their faces have been uploaded and are present on the public Internet.

82. Das OPCC kam zu demselben Schluss, als es bewertete, ob die von Clearview gesammelten personenbezogenen Daten unter die kanadische „Veröffentlichungs"-Ausnahme fallen, die nur dann gilt, „*„wenn die Person die Informationen zur Verfügung gestellt hat*" oder wenn „*vernünftigerweise anzunehmen ist, dass die Person, um die es bei den Informationen geht, diese Informationen zur Verfügung gestellt hat*": „*Da Clearview massenhaft Bilder durch automatisierte Tools sammelt, ist es unvermeidlich, dass die Bilder in vielen Fällen stattdessen von einer dritten Partei hochgeladen wurden*" (Office of the Privacy Commissioner of Canada (OPCC), PIPEDA Report of Findings #2021-001, 2 Februar 2021, via https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/, RN 66).

82. The OPCC reached the same conclusion when assessing whether the personal data that Clearview collects falls within the Canadian "publications" exception, which applies only "*where the individual has provided the information*" or where "*it is reasonable to assume that the individual that the information is about provided that information*": "*As Clearview engages in mass collection of images through automated tools, it is inevitable that in many instances, the images would have instead been uploaded by a third party*" (Office of the Privacy Commissioner of Canada (OPCC), PIPEDA Report of Findings #2021-001, 2 February 2021, available at: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/, para 66).

83. Drittens werden, wie oben erläutert, einmal gesammelte Fotos auf *unbestimmte* Zeit in der Datenbank von Clearview gespeichert, ohne Rücksicht darauf, ob diese Fotos zu einem bestimmten Zeitpunkt noch öffentlich zugänglich sind. Wie in einem Artikel der New York Times über Clearview richtig bemerkt wurde, es ist „*zu spät, wenn Ihr Profil bereits abgegriffen wurde. Das Unternehmen behält alle Bilder, die es abgegriffen hat, auch wenn sie später gelöscht oder heruntergenommen werden*" (Kashmir Hill, '*Before Clearview Became a Police Tool, It Was a Secret Plaything of the Rich*', The New York Times, 5 March 2020, available at https://www.nytimes.com/2020/03/05/technology/clearview-investors.html). Der Artikel erklärt dabei jedoch, dass, „*Herr Ton-That sagte, dass die Firma an einem Tool arbeitet, mit dem man die Entfernung von Bildern beantragen kann, wenn diese von der Ursprungswebsite entfernt wurden.*"

83. Third, as explained above, once collected, photos are kept in Clearview's database indefinitely, with no regard for whether these photos are still publicly available at any one point. As rightly observed in the New York Times article on Clearview, "*if your profile has already been scraped, it is too late. The company keeps all the images it has scraped even if they are later deleted or taken down*" (Kashmir Hill, 'Before Clearview Became a Police Tool, It Was a Secret Plaything of the Rich', The New York Times, 5 March 2020, available at https://www.nytimes.com/2020/03/05/technology/clearview-investors.html). The article went on to note, "*though Mr. Ton-That said the company was working on a tool that would let people request that images be removed if they had been taken down from the website of origin.*"

84. Was die letztgenannte „Ausrede" betrifft, so ist es erstens inakzeptabel, dass Clearview seine Technologie ohne die Existenz dieses Tools eingesetzt hat, und zweitens würde ein solches Tool in jedem Fall nur einen äußerst begrenzten Regress für Einzelpersonen bieten - es würde voraussetzen, dass Einzelpersonen (1) überhaupt wissen, dass Clearview ihre Gesichtsbilder sammelt, (2) systematisch Datenzugriffsanfragen stellen, um zu erfahren, welche Fotos von Clearview gesammelt wurden, (3) die Ergebnisse dieser Anfragen mit dem vergleichen, was sie online zur Verfügung gestellt haben, und (4) individuelle Anträge auf Entfernung einreichen. Dies ist völlig unangemessen und ein eklatanter Affront gegen das Recht eines Jeden, seine Online-Identität zu kontrollieren, und verhindert jede wirksame Ausübung der Rechte der betroffenen Personen gemäß der DSGVO.

85. Schließlich ist es notorisch schwierig, die Privatsphären-Einstellungen richtig zu gestalten und so anzupassen, dass die Informationen, die man in „privaten" Online-Kreisen haben möchte, auch tatsächlich so sind und bleiben. Untersuchungen haben wiederholt gezeigt, wie komplex es für Einzelpersonen ist, ihre Einstellungen so anzupassen, dass sie datenschutzfreundlich sind, und dass die gesetzlichen Zustimmungsanforderungen häufig nicht erfüllt werden (Privacy International, '*Most cookie banners are annoying and deceptive*. This is not consent.', 21. Mai 2019, via https://privacyinternational.org/explainer/2975/most-cookie-banners-are-annoying-and-deceptive-not-consent. Privacy International, 'Facebook - Profile Settings', 7. Januar 2021, via https://privacyinternational.org/guide-step/3959/facebook-profile-settings). „Dark Patterns", wie vom norwegischen Verbraucherrat geprägt, bedeutet, dass betroffene Personen nicht immer die Kontrolle über ihre persönlichen Daten online haben, weil sie durch Design und

84. As to this latter "excuse", it is first unacceptable that Clearview has deployed its technology without the existence of this tool, and second, such a tool would in any case only provide an extremely limited recourse for individuals – it would imply individuals (1) knowing in the first place that Clearview collects their facial images, (2) systematically submitting data subject access requests to know what photos have been collected by Clearview, (3) cross-checking results from these requests with what they have made available online, and (4) submitting individual requests for removal. This is entirely unreasonable and a blatant affront to individuals' right to control their online identities, preventing any effective exercise of data subject rights provided under the GDPR.

85. Finally, privacy settings are notoriously difficult to get right and to adjust so that the information one wants to remain within private online circles actually is and remains so. Research has repeatedly shown how complex it is for individuals to adjust their settings to be privacy friendly, and that legal consent requirements are often not met (Privacy International, 'Most cookie banners are annoying and deceptive. This is not consent.', 21 May 2019, available at https://privacyinternational.org/explainer/2975/most-cookie-banners-are-annoying-and-deceptive-not-consent. Privacy International, 'Facebook - Profile Settings', 7 January 2021, available at https://privacyinternational.org/guide-step/3959/facebook-profile-settings). "Dark patterns", as used by the Norwegian Consumer Council, mean that data subjects are not always in control of their personal data online because of how they are nudged by design and other subtle methods in the direction of less privacy (Norwegian Consumer Council, 'Deceived by Design – How tech companies use

andere subtile Maßnahmen zu weniger Datenschutz „gelenkt" werden (Norwegian Consumer Council, '*Deceived by Design – How tech companies use dark patterns to discourage us from exercising our rights to privacy*' (27. Juni 2018), via https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf).

4.5. Verstoß gegen Artikel 5(1)(a) DSGVO, Grundsatz von Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

86. Transparenz ist ein zentraler Bestandteil des ersten Datenschutzprinzips, der in Artikel 5(1)(a) DSGVO festgelegt ist und durch das Informationsrecht in den Artikeln 13 und 14 unterstützt wird. In Erwägungsgrund 60 DSGVO heißt es: „*Die Grundsätze einer fairen und transparenten Verarbeitung machen es erforderlich, dass die betroffene Person über die Existenz des Verarbeitungsvorgangs und seine Zwecke unterrichtet wird.*" Gemäß Artikel 14(3)(a) DSGVO muss der Verantwortliche, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden, wie dies bei der Verarbeitung durch Clearview der Fall ist, der betroffenen Person „*innerhalb einer angemessenen Frist nach Erlangung der personenbezogenen Daten, längstens jedoch innerhalb eines Monats*", Informationen zur Verfügung stellen.

87. Clearview zeigt auf seiner Website eine Datenschutzrichtlinie, die im März 2021 von einer früheren Version aktualisiert wurde, die explizit an ein globales Publikum gerichtet war. In der neuen Fassung wurde der Hinweis auf Einwohner des Europäischen Wirtschaftsraums oder der Schweiz gestrichen. Dennoch gilt sie ausdrücklich für „*Fotos, die öffentlich im Internet verfügbar sind*" und für die Extraktion von

dark patterns to discourage us from exercising our rights to privacy' (27 June 2018), available at https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf).

4.5. Violation of Article 5(1)(a) GDPR, the lawfulness, fairness and transparency principle

86. Transparency is a core component of the first data protection principle, set out in Article 5(1)(a) GDPR and supported by the right to information in Articles 13 and 14 GDPR. Recital 60 GDPR provides that "*[t]he principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes.*" Under Article 14(3)(a) GDPR, where personal data have not been obtained from the data subject, as is the case for Clearview's processing, the controller must provide the data subject with information "*within a reasonable period after obtaining the personal data, but at the latest within one month*".

87. Clearview displays on its website a Privacy Policy, which was updated in March 2021 from an earlier version explicitly addressed to a global audience. The new version removed reference to residents of the European Economic Area or of Switzerland. Yet, it expressly applies to "*photos that are publicly available on the Internet*" and for the

„*Geolokalisierung und Messungen von Gesichtsmerkmalen für Personen auf den Fotos*". Das bedeutet, dass auch die neue Datenschutzrichtlinie notwendigerweise für alle Personen in der Welt gilt, die, wissentlich oder unwissentlich, ihre Gesichtsbilder auf öffentlich zugänglichen Teilen des Internets haben, und daher auch für EU-Einwohner und damit dem Beschwerdeführer.

88. Clearview bietet in mindestens zwei Punkten nicht die erforderliche Transparenz. Erstens benachrichtigt Clearview Personen niemals darüber, dass sie ihre persönlichen Daten verarbeiten, so dass betroffene Personen niemals die Datenschutzrichtlinien von Clearview lesen können, bevor oder nachdem ihre persönlichen Daten verarbeitet wurden.

89. Nach der Art. 29-Gruppe stellt beim Transparenzgrundsatz *„die Tatsache einen zentralen Erwägungsfaktor dar, dass die betroffene Person den Umfang und die Folgen der Verarbeitung im Vorfeld ermitteln kann und nicht später von der Art und Weise überrascht werden sollte, in der ihre personenbezogenen Daten verwendet worden sind.* " (Art. 29-Gruppe, Leitlinien für Transparenz gemäß der Verordnung 2016/679, angenommen am 29. November 2017 zuletzt überarbeitet und angenommen am 11. April 2018, RN 10). Im Fall von Clearview ist die Überraschung komplett - die einzige Möglichkeit für eine betroffene Person, zu erfahren, dass ihre Daten verarbeitet wurden, ist die Lektüre der verschiedenen Medienberichte über ihre Praktiken.

90. Zweitens liefert Clearview unvollständige und irreführende Informationen, selbst wenn man zum geeigneten Zeitpunkt vor oder kurz nach der Verarbeitung der Daten auf die Richtlinie zugreifen

extraction of "*geolocation and measurements of facial features for individuals in the photos*" – meaning it necessarily applies to all individuals in the world who, knowingly or unknowingly, have their facial images on publicly available parts of the Internet, and therefore also to EU resident and as such the Complainant.

88. Clearview fails to provide the required transparency in at least two respects. First, Clearview never notifies individuals that it is processing their personal data, so that affected individuals never get to read Clearview's privacy policy before or after their personal data has been processed.

89. According to the Art 29 WP Guidelines on transparency, "*a central consideration of the principle of transparency [...] is that the data subject should be able to determine in advance what the scope and consequences of the processing entails and that they should not be taken by surprise at a later point about the ways in which their personal data has been used*" (Article 29 Data Protection Working Party, 'Guidelines on transparency under Regulation 2016/679', 17/EN WP260 rev.01, adopted on 29 November 2017, revised and adopted on 11 April 2018, para 10, available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227). The surprise in Clearview's case is complete – the only way for a data subject to know their data has been processed is to read the various media reports about their practices.

90. Second, even if one were able to access the Policy at the appropriate time before or shortly after their data is processed, Clearview provides incomplete and misleading information. In the section "What Data Do We Collect?", it notes that it "*collects photos that are publicly available*

konnte. Im Abschnitt „What Data Do We Collect" wird darauf hingewiesen, dass Clearview „*Fotos sammelt, die im Internet öffentlich zugänglich sind*" und „*möglicherweise Informationen aus diesen Fotos extrahiert, einschließlich Geolokalisierung und Messungen von Gesichtsmerkmalen von Personen auf den Fotos*".

91. Diese Aussage ist in zweierlei Hinsicht unvollständig und irreführend: (1) Sie stellt die Extraktion von Informationen und Messungen von Gesichtsmerkmalen als bloße Möglichkeit dar (durch Verwendung des Wortes „kann", das in Datenschutzrichtlinien vermieden werden sollte, siehe Art. 29-Gruppe, Leitlinien für Transparenz gemäß der Verordnung 2016/679, angenommen am 29. November 2017 zuletzt überarbeitet und angenommen am 11. April 2018, RN 13), während es sich in Wirklichkeit um einen automatischen Prozess handelt, und (2) sie lässt verschiedene andere Arten personenbezogener Daten aus, die Clearview automatisch sammelt, nämlich Namen und andere Daten, die aus gesammelten URLs, Fotos und Webseitentiteln gewonnen werden.

92. Darüber hinaus wurden in dieser neuen Version der Clearview-Datenschutzerklärung Informationen über die Rechtsgrundlagen, auf die sich Clearview bei der Verarbeitung personenbezogener Daten stützt, entfernt. Die vorherige Version der Datenschutzrichtlinie von Clearview bezog sich auf DSGVO-spezifische Rechtsgrundlagen wie berechtigte Interessen oder ausdrückliche Zustimmung. Wiederum in einem Versuch, die DSGVO-Rechtsprechung zu umgehen, hat Clearview wesentliche Informationen entfernt, die bei der Verarbeitung personenbezogener Daten von EU-Bewohnern bereitgestellt werden müssen.

on the Internet" and "*may extract information from those photos including geolocation and measurements of facial features for individuals in the photos*".

91. This statement is incomplete and misleading in two ways: (1) it presents the extraction of information and measurements of facial features as a mere possibility (by using the word "may", which should be avoided in privacy policies, see Article 29 Data Protection Working Party, 'Guidelines on transparency under Regulation 2016/679', 17/EN WP260 rev.01, adopted on 29 November 2017, revised and adopted on 11 April 2018, para 13, available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227)), while in reality this is an automatic process, and (2) it omits various other types of personal data that Clearview automatically collects, namely names and other data obtained from URLs, photo and webpage titles collected.

92. In addition, this new version of Clearview's privacy has removed information about the legal bases upon which Clearview relies for the processing of personal data. The previous version of Clearview's privacy policy referred to GDPR-specific legal bases such as legitimate interests or explicit consent. Again, in what can be perceived as an effort to evade GDPR jurisdiction, Clearview has removed essential information that must be provided when processing EU residents' personal data.

93. In verschiedenen öffentlichen Erklärungen (wie zB beim CNN Business YouTube Kanal, '*Clearview AI's founder Hoan Ton-That speaks out [Extended interview]*', 6. März 2020, via https://www.youtube.com/watch?v=q-1bR3P9RAw) scheint Clearview davon auszugehen, dass jegliches Recht auf Information durch die Tatsache negiert wird, dass die gewonnenen personenbezogenen Daten öffentlich zugänglich sind, und dass die betroffenen Personen daher dieses Recht „aufgegeben" hätten, indem sie stillschweigend duldeten, dass ihre Bilder online öffentlich zugänglich sind. Wie jedoch in dieser Stellungnahme weiter unten analysiert und erläutert wird, gibt es zahlreiche Gründe, warum dies falsch ist. Es ist daher inakzeptabel, dass Clearview davon ausgeht, dass der Einzelne vollständig informiert ist und der Verarbeitung seiner Gesichtsbilder auf diese Weise zustimmt.

94. Dieser Mangel an Transparenz, der an sich schon einen Verstoß gegen die DSGVO darstellt, bedeutet auch, dass die überwältigende Mehrheit der betroffenen Personen keine Kenntnis von der Verarbeitung ihrer personenbezogenen Daten durch Clearview hat und daher möglicherweise keines ihrer Betroffenenrechte in Bezug auf diese Verarbeitung ausüben kann.

4.5.1. Verarbeitung nach Treu und Glauben und die vernünftigen Erwartungen der betroffenen Personen

95. Treu und Glauben ist ein weiterer Bestandteil des ersten Datenschutzgrundsatzes in Artikel 5(1)(a) DSGVO. Kernpunkt von Treu und Glauben ist, dass die betreffende Datenverarbeitung mit den vernünftigen Erwartungen der betroffenen Personen übereinstimmen sollte: „*Treu und Glauben bedeutet, dass Sie personenbezogene Daten nur auf eine Art und Weise verarbeiten sollten, die Menschen*

93. In various public statements (such as CNN Business YouTube channel, 'Clearview AI's founder Hoan Ton-That speaks out [Extended interview]', 6 March 2020, available at https://www.youtube.com/watch?v=q-1bR3P9RAw), Clearview seems to assume that any right to information is obliterated by the fact that the personal data obtained is publicly available, and that data subjects would have therefore "given up" this right by quietly acquiescing to their images being publicly available online. However, as this submission will further analyse and explain below, there are numerous reasons why this is false. It is therefore unacceptable for Clearview to assume full information and acquiescence by individuals to their facial images being processed in this way.

94. This lack of transparency, a violation of the GDPR in itself, also implies that an overwhelming majority of data subjects are not aware of Clearview's processing of their personal data and therefore cannot possibly exercise any of their data subject rights in relation to that processing.

4.5.1. Fairness and data subjects' reasonable expectations

95. Fairness is one component of the first data protection principle in Article 5(1)(a) GDPR. Core to fairness is that the data processing concerned should be in line with individuals' reasonable expectations: "*fairness means that you should only handle personal data in ways that people would reasonably expect and not use it in ways that have unjustified adverse effects on them*" (ICO, 'Guide to the General Data

vernünftigerweise erwarten würden, und sie nicht auf eine Art und Weise verwenden sollten, die ungerechtfertigte nachteilige Auswirkungen auf sie hat" (ICO, '*Guide to the General Data Protection Regulation (GDPR) – Principle (a): Lawfulness, fairness and transparency*', via https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/#fairness; Ehmann/Selmayr/Heberlein, 2. Aufl. 2018, DS-GVO Art. 5 Rn. 9, 10.

96. Die plausible Erwartung der Privatsphäre ist auch ein Schlüsselprinzip in der Rechtsprechung des EGMRs, das verwendet wird, um zu beurteilen, ob ein Eingriff in das Privatleben einer Person gemäß Artikel 8 der Europäischen Menschenrechtskonvention (**EMRK**) stattgefunden hat. Der EGMR hat mehrfach untersucht, ob Personen „*eine vernünftige Erwartung hatten, dass ihre Privatsphäre respektiert und geschützt wird*" (*Barbulescu v. Romania* [GC] App no 1496/08 (ECtHR, 5 September 2017), RN 73).

97. In seiner Rechtsprechung hat der Gerichtshof unterstrichen, dass keine Person vernünftigerweise erwarten kann, dass Filmmaterial, das sensible Aspekte ihres Privatlebens zeigt, später in den Medien veröffentlicht wird, selbst wenn ihre Handlungen „*bereits öffentlich*" sind (*Peck v. United Kingdom* App No 44647/98 (ECtHR, 28. Januar 2003), RN 61-62), und dass die Verwendung von Fotoausrüstungen zur Erfassung und Verarbeitung biometrischer Daten von Personen zu anderen als den ursprünglich von ihnen erwarteten Zwecken nicht unter ihre vernünftigen Erwartungen an die Privatsphäre fallen kann (*Perry v. United Kingdom* App No 63737/00 (ECtHR, 17. Juli 2003), RN 41).

Protection Regulation (GDPR) – Principle (a): Lawfulness, fairness and transparency', available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/#fairness; Ehmann/Selmayr/Heberlein, 2. Ed. 2018, GDPR Art. 5 para. 9, 10).

96. Reasonable expectation of privacy is also a key principle in jurisprudence of the European Court of Human Rights (the "**ECtHR**"), which is used to assess whether there has been an interference with an individual's private life under Article 8 of the European Convention on Human Rights ("**ECHR**"). The ECtHR has on several occasions investigated whether individuals "*had a reasonable expectation that their privacy would be respected and protected*" (*Barbulescu v. Romania* [GC] App no 1496/08 (ECtHR, 5 September 2017), para 73).

97. In its case law, the Court has underlined that no person could reasonably expect footage depicting sensitive aspects of their private life to be later released in the media, even if their actions are "*already in the public domain*" (*Peck v. United Kingdom* App No 44647/98 (ECtHR, 28 January 2003), paras 61-62) and that the use of photographic equipment to capture and process individuals' biometric data for purposes other than originally anticipated by them cannot fall within their reasonable expectations of privacy (*Perry v. United Kingdom* App No 63737/00 (ECtHR, 17 July 2003), para 41).

98. Die vernünftigen Erwartungen des Beschwerdeführers werden von Clearviews Verarbeitungen offenkundig mit Füßen getreten. In seiner jüngsten Entscheidung stellte das OPCC fest, dass *„Personen, die ihre Bilder online gestellt haben oder deren Bilder von Dritten eingestellt wurden, keine vernünftigen Erwartungen hatten, dass Clearview ihre Bilder zu Identifizierungszwecken sammeln, verwenden und weitergeben würde*" (Office of the Privacy Commissioner of Canada (OPCC), PIPEDA Report of Findings #2021-001, 2. Februar 2021, via https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/).

99. Dies wird auch durch eine von der Europäischen Agentur für Grundrechte (**FRA**) durchgeführte Umfrage gestützt, in der europäische Bürger zu ihrer Bereitschaft befragt wurden, verschiedene Arten von persönlichen Daten sowohl an staatliche Stellen als auch an private Unternehmen weiterzugeben (European Union Agency for Fundamental Rights, '*Your rights matter: Data protection and privacy - Fundamental Rights Survey*', 18 Juni 2020, via https://fra.europa.eu/en/publication/2020/fundamental-rights-survey-data-protection#TabPubSharingdataonline1). In den EU-27-Ländern gaben 94% der Befragten ausdrücklich an, dass sie nicht bereit sind, ihr Gesichtsbild zu Identifizierungszwecken mit privaten Unternehmen zu teilen.

100. Die Praxis, öffentlich verfügbare Daten von Social-Media-Plattformen zu sammeln und zu verarbeiten, die als „Social-Media-Intelligence" (**SOCMINT**) oder „Social-Media-Überwachung" bezeichnet werden, wurde in den letzten Jahren wegen Bedenken

98. The Complainant's reasonable expectations are blatantly trampled by Clearview's practices. In its recent decision, the OPCC found that "*individuals who posted their images online, or whose images were posted by third party(ies), had no reasonable expectations that Clearview would collect, use and disclose their images for identification purposes*" (Office of the Privacy Commissioner of Canada (OPCC), PIPEDA Report of Findings #2021-001, 2 February 2021, available at: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/).

99. This is further supported by a survey conducted by the European Agency for Fundamental Rights ("**FRA"**), in which European citizens were consulted on their willingness to share different types of personal data with both governmental agencies and private companies (European Union Agency for Fundamental Rights, 'Your rights matter: Data protection and privacy - Fundamental Rights Survey', 18 June 2020, available at https://fra.europa.eu/en/publication/2020/fundamental-rights-survey-data-protection#TabPubSharingdataonline1), according to which, Across the EU-27 countries, 94% of the surveyed explicitly stated they were not willing to share their facial images with private companies for identification purposes.

100. In general, the practice of gathering and processing publicly available data from social media platforms, coined "social media intelligence" ("**SOCMINT**") or "social media monitoring", has been decried in recent years for concerns about its compatibility with reasonable expectations of privacy.

hinsichtlich der Kompatibilität mit angemessenen Erwartungen an den Datenschutz abgelehnt.

101. Im Rahmen einer Konsultation über die Nutzung der Überwachung sozialer Medien durch das Europäische Amt für Asylunterstützung vertrat der EDSB die Auffassung, dass die Überwachung sozialer Medien „*die Verwendung personenbezogener Daten beinhaltet, die den angemessenen Erwartungen des Einzelnen widersprechen oder diese übertreffen. Solche Praktiken führen häufig dazu, dass personenbezogene Daten über ihren ursprünglichen Zweck und ihren ursprünglichen Kontext hinaus und in einer Weise verwendet werden, die die betroffene Person vernünftigerweise nicht vorhersehen konnte*" (EDPS, '*Formal consultation on EASO's social media monitoring reports (case 2018-1083*)' (Brussels, D(2019) 1961), S. 3, via https://edps.europa.eu/sites/edp/files/publication/19-11-12_reply_easo_ssm_final_reply_en.pdf).

102. Die Verarbeitung von Clearview ist eine besonders aufdringliche Form der Überwachung sozialer Medien, die weit über die Konsultation und Analyse öffentlich verfügbarer Informationen auf Ad-hoc-Basis hinausgeht. Durch die automatische Erfassung, Speicherung und Verarbeitung von Clearview zur Extraktion biometrischer Bezeichner entfernt sich Clearview immer mehr von allen angemessenen Erwartungen der betroffenen Personen und ist daher in keiner Weise mit dem Grundsatz der Verarbeitung nach Treu und Glauben vereinbar.

103. Die Anwendung der Gesichtserkennung auf die Datenerfassung verschärft das Problem: In ihrem Schreiben an das Europäische Parlament, in dem eine vorläufige Stellungnahme zur Verwendung von

101. As part of a consultation on the use of social media monitoring by the European Asylum Support Office, the EDPS considered that social media monitoring "*involves uses of personal data that go against or beyond individuals' reasonable expectations. Such uses often result in personal data being used beyond their initial purpose, their initial context and in ways the individual could not reasonably anticipate*" (EDPS, 'Formal consultation on EASO's social media monitoring reports (case 2018-1083)' (Brussels, D(2019) 1961), p. 3, available at https://edps.europa.eu/sites/edp/files/publication/19-11-12_reply_easo_ssm_final_reply_en.pdf).

102. Clearview's processing is a particularly intrusive form of social media monitoring, which goes far beyond the consultation and analysis of publicly available information on an ad hoc basis. Clearview's automatic collection, storage and processing for extraction of biometric identifiers make it further removed from any reasonable expectations of data subjects and therefore in no way compatible with the principle of fairness.

103. The application of facial recognition to the collection of data compounds the issue: in its letter to the European Parliament giving a preliminary opinion on the use of Clearview by law enforcement, the EDPB highlighted that facial recognition technology may "*affect*

Clearview durch die Strafverfolgungsbehörden abgegeben wurde, betonte der EDSA, dass die Gesichtserkennungstechnologie *„die angemessene Erwartung des Einzelnen an Anonymität im öffentlichen Raum beeinträchtigen kann*" (EDSA, *Letter to Members of the European Parliament*, Ref: OUT2020-0052, 10. Juni 2020, via https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-response-meps-sophie-t-veld-moritz-korner-michal-simecka_en).

104. Durch die Kombination von SOCMINT und Gesichtserkennungstechnologie vernichtet der von Clearview angebotene Service effektiv die Erwartung des Einzelnen, dass sein Leben und seine Identität in seinem physischen, privaten Leben nicht sofort mit seinem Leben und seiner Identität im Internet verbunden werden können.

4.5.1.1. Vergleich mit der Google-Suchmaschine

105. Clearview hat in verschiedenen öffentlichen Berichten seinen Dienst häufig mit der Suchmaschine von Google verglichen und argumentiert, dass sein Dienst lediglich eine „Gesichtssuchmaschine" anstelle einer Website-Suchmaschine sei und Gesichter anstelle von Wörtern als Suchbegriffe verwenden würde (CNN Business, '*Clearview AI sued in California by immigrant rights groups, activists*', 10. März 2021, via https://edition.cnn.com/2021/03/09/tech/clearview-ai-mijente-lawsuit/index.html). Dieser Vergleich soll anscheinend zeigen, dass der Dienst von Clearview den vernünftigen Erwartungen der betroffenen Personen an den Datenschutz entspricht, da jeder weiß, dass seine Daten von Suchmaschinen erfasst werden. Wir möchten jedoch einige Klarstellungen zu den technischen Prozessen geben, die

individuals' reasonable expectation of anonymity in public spaces" (EDPB, Letter to Members of the European Parliament, Ref: OUT2020-0052, 10 June 2020, available at https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-response-meps-sophie-t-veld-moritz-korner-michal-simecka_en).

104. By combining SOCMINT and facial recognition technology, the service that Clearview offers is effectively annihilating individuals' expectation that their lives and identities in their physical, private lives cannot be immediately connected to their lives and identities on the Internet.

4.5.1.1. Comparison with Google's search engine

105. Clearview has, in various public reports, often compared its service to Google's search engine, arguing that its service is merely a "face search engine" instead of a website search engine, using faces rather than words as search terms (CNN Business, 'Clearview AI sued in California by immigrant rights groups, activists', 10 March 2021, available at https://edition.cnn.com/2021/03/09/tech/clearview-ai-mijente-lawsuit/index.html). This comparison seems intended to show that Clearview's tool would fall within data subjects' reasonable expectation of privacy, as everyone is aware that their data is scraped by search engines. We would like to provide some clarifications as to the technical processes performed by Google's and Clearview's platforms, which will show that they are fundamentally different.

von den Plattformen von Google und Clearview ausgeführt werden, um zu zeigen, dass sie sich grundlegend unterscheiden.

106. Die „Suchmaschinen" von Google und Clearview führen beide drei verschiedene Aktionen aus:

i. **Crawling** - automatischer Zugriff auf eine Website und Abrufen von Daten von dieser Website;
ii. **Indizierung** - Herunterladen von Inhalten von einer Webseite auf den Server der Suchmaschine, wodurch Inhalte zu ihrem „Index" hinzugefügt werden; und
iii. **Listing** - übereinstimmenden Inhalt auf den Suchergebnisseiten anzeigen.

107. Beim Crawling kann ein Websitebetreiber eine robots.txt-Datei verwenden, in der Webroboter angewiesen werden, wie Seiten auf ihrer Website gecrawlt werden sollen. Dies ist eine Textdatei, mit der Webmaster einer Suchmaschine mitteilen können, dass sie beispielsweise den Inhalt ihrer Seite nicht indizieren möchten. Das Einhalten der robots.txt-Datei ist technisch gesehen optional und kann von Crawlern ignoriert werden. Plattformen wie LinkedIn oder Facebook haben solche Dateien auf ihren Webseiten aufgenommen und verbieten das Crawling ausdrücklich in den Nutzungsbedingungen ihrer Website.

108. Google gibt Webmastern die Kontrolle darüber, welche Informationen auf ihrer Seite indiziert und in den Suchergebnissen aufgeführt werden, einschließlich der Option, sich vollständig abzumelden.

106. Google's and Clearview's "search engines" both perform three distinct actions:

i. **Crawling** – automatically accessing a website and obtaining data from that website;

ii. **Indexing** – downloading content from a webpage to the server of the search engine, thereby adding content to its "index"; and

iii. **Listing** – showing matching content in the search result pages.

107. At the crawling stage, a website owner can make use of a robots.txt file instructing web robots how to crawl pages on their website. This is a text file that allows webmasters to tell a search engine they do not want the contents of their page indexed, for example. Abiding by the robots.txt file is optional from a technical perspective, and can be disregarded by crawlers. Platforms such as LinkedIn or Facebook have included such files on their webpages, and specifically forbid crawlers in their website terms and conditions.

108. Google gives webmasters control over what information from their page is indexed and listed on its search results, including the option to opt-out entirely.

109. Obgleich Clearview angegeben hat, dass ihr Image-Crawler so konfiguriert ist, dass alle Anweisungen in den robots.txt-Dateien berücksichtigt werden (Office of the Privacy Commissioner of Canada (OPCC), PIPEDA Report of Findings #2021-001, .2 Februar 2021, RN17, via: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/), hat Clearview nichtsdestotrotz Inhalte von YouTube, Facebook, Twitter und Instagram indiziert ((Kashmir Hill, '*Before Clearview Became a Police Tool, It Was a Secret Plaything of the Rich*', The New York Times, 5. März 2020, viahttps://www.nytimes.com/2020/03/05/technology/clearview-investors.html). Dies passierte, obwohl YouTube ausdrücklich die automatische Erhebung von Informationen, die eine Person identifizieren könnten, verbietet sowie das Scraping von Informationen, außer durch „öffentliche Suchmaschine" wie Google (YouTube, 'Terms of Service', via https://www.youtube.com/static?template=terms).

110. Clearview respektiert daher tatsächlich nicht die Anweisungen, Inhalte von bestimmten Websites nicht zu crawlen und zu scrapen, und wurde aus diesem Grund von verschiedenen großen Plattformen wegen Verstoßes gegen ihre Richtlinien verklagt (Alfred Ng and Steven Musil, '*Clearview AI hit with cease-and-desist from Google, Facebook over facial recognition collection*' (CNET, 5. Februar 2020), via https://www.cnet.com/news/clearview-ai-hit-with-cease-and-desist-from-google-over-facial-recognition-collection/).

111. Die systematische und wahllose Sammlung von Gesichtsbildern von Einzelpersonen aus dem Internet entspricht daher nicht den angemessenen Erwartungen des Einzelnen und verstößt gegen den

109. While Clearview has stated that their image crawler is configured to respect whatever instructions are present in robots.txt files (Office of the Privacy Commissioner of Canada (OPCC), PIPEDA Report of Findings #2021-001, 2 February 2021, para 17, available at: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/), Clearview has nevertheless indexed content from YouTube, Facebook, Twitter and Instagram ((Kashmir Hill, 'Before Clearview Became a Police Tool, It Was a Secret Plaything of the Rich', The New York Times, 5 March 2020, available at https://www.nytimes.com/2020/03/05/technology/clearview-investors.html). This is despite the fact that YouTube explicitly forbids automated collection of any information that might identify a person, and scraping of any data except by "public search engines", such as Google's (YouTube, 'Terms of Service', available at https://www.youtube.com/static?template=terms).

110. Clearview therefore actually does not respect instructions not to crawl and scrape content from certain websites, and has for this reason been sued by various large platforms for violation of their policies (Alfred Ng and Steven Musil, 'Clearview AI hit with cease-and-desist from Google, Facebook over facial recognition collection' (CNET, 5 February 2020), available at https://www.cnet.com/news/clearview-ai-hit-with-cease-and-desist-from-google-over-facial-recognition-collection/).

111. The systematic and indiscriminate collection of individuals' facial images from the Internet therefore does not fall within individuals' reasonable expectations and violates the fairness principle. The issue

Grundsatz von Treu und Glauben. Das Problem der Verarbeitung nach Trau und Glauben wird durch die fehlende Transparenz und die Missachtung des Rechts des Einzelnen auf Information sowie durch verschiedene andere Verstöße gegen die Datenschutzgrundsätze verschärft, wie in dieser Eingabe weiter ausgeführt wird.

4.6. Verstoß gegen den Grundsatz der Zweckbindung

112. Ein weiteres Kernprinzip des Datenschutzes, das durch die Verarbeitung von Clearview offenkundig mit Füßen getreten wird, ist das der Zweckbindung gemäß Artikel 5(1)(b) DSGVO als Folge dessen, dass Clearview sich auf Artikel 9(2)(e) DSGVO stützt, wie oben erwähnt.

113. Die Frage der Zweckbindung ist untrennbar mit der Frage verbunden, was eine Person mit ihren für einen bestimmten Zweck "offensichtlich öffentlich gemachten" personenbezogenen Daten erwarten kann, wie oben untersucht. Die Weiterverwendung für die Verarbeitung in einer biometrischen Datenbank fällt eindeutig nicht unter diesen Erwartungen. Wie der EDSB feststellte, führt die Verwendung personenbezogener Daten im Zusammenhang mit der Überwachung sozialer Medien *„häufig dazu, dass personenbezogene Daten über ihren ursprünglichen Zweck und ihren ursprünglichen Kontext hinaus und in einer Weise verwendet werden, die der Einzelne vernünftigerweise nicht vorhersehen konnte*" (EDPS, 'Formal consultation on EASO's social media monitoring reports (case 2018-1083)' (Brussels, D(2019) 1961), S. 3, via https://edps.europa.eu/sites/edp/files/publication/19-11-12_reply_easo_ssm_final_reply_en.pdf)

of fairness is compounded by the absence of transparency and disrespect for individuals' right to information, and various other violations of data protection principles as further set out in this submission.

4.6. Violation of the purpose limitation principle

112. Another core principle of data protection overtly trampled by Clearview's processing is that of purpose limitation under Article 5(1)(b) GDPR as a result of Clearview relying on Article 9(2)(e) GDPR, as explained above.

113. The question of purpose limitation is intrinsically linked to what one can expect to be done with their personal data "manifestly made public" for a specific purpose, as explored above. The re-use for processing in a biometric database clearly falls outside of such expectations. As stated by the EDPS, uses of personal data in the context of social media monitoring *"often result in personal data being used beyond their initial purpose, their initial context and in ways the individual could not reasonably anticipate*" (EDPS, 'Formal consultation on EASO's social media monitoring reports (case 2018-1083)' (Brussels, D(2019) 1961), p. 3, available at https://edps.europa.eu/sites/edp/files/publication/19-11-12_reply_easo_ssm_final_reply_en.pdf).

114. Die folgende Aussage in der Stellungnahme der Art. 29-Gruppe zur Biometrie ist ebenfalls aufschlussreich:

> ***Fotos*** *im Internet, in sozialen Medien und in Online-Anwendungen zur Verwaltung und Weitergabe von Fotos dürfen nicht zur Erstellung biometrischer Templates oder zum Einlesen von Daten in ein System verwendet werden, das die automatische Erkennung der fotografierten Personen (Gesichtserkennung) ermöglichen würde, ohne dass eine konkrete Rechtsgrundlage (z. B. eine Einwilligung) für diesen neuen Zweck gegeben wäre. Auch wenn eine Rechtsgrundlage für diesen nachgeordneten Verarbeitungszweck besteht, muss die Verarbeitung bezogen auf diesen Zweck angemessen und relevant sein, und die Verarbeitung darf nicht in übermäßigem Umfang erfolgen. Wenn die betroffene Person eingewilligt hat, dass Fotos, auf denen diese Person zu sehen ist, automatisch derart verarbeitet werden, dass die Personen in einem Online-Fotoalbum mit einem Algorithmus zur Gesichtserkennung identifiziert werden können, muss diese Verarbeitung unter Berücksichtigung der geltenden Datenschutzvorschriften erfolgen. Biometrische Daten, die nach der Kennzeichnung der Bilder mit dem Namen, einem Benutzernamen oder einem sonstigen von der betroffenen Person eingegebenen Text nicht mehr benötigt werden, müssen gelöscht werden. Die Erzeugung einer permanenten Datenbank mit biometrischen Daten ist für diesen Zweck nicht unbedingt nicht erforderlich.*
> (Art. 29-Gruppe, '*Stellungnahme 3/2012 zu Entwicklungen im Bereich biometrischer Technologien*', S. 8)

115. In Anbetracht dieser Aussage stellt die Verarbeitung durch Clearview einen völlig neuen Zweck gegenüber der ursprünglichen Veröffentlichung dar, für den es eine eigene, gültige Rechtsgrundlage geben müsste. Wie oben gezeigt, ist diese nicht vorhanden, und Clearview verstößt daher gegen den Grundsatz der Zweckbindung.

114. The following statement in the Art 29 WP's opinion on biometrics is also telling:

> ***Photographs*** *on the internet, in social media, in online photo management or sharing applications may not be further processed in order to extract biometric templates or enrol them into a biometric system to recognise the persons on the pictures automatically (facial recognition) without a specific legal basis (e.g. consent) for this new purpose. If there is a legal basis for this secondary purpose the processing must also be adequate, relevant and not excessive in relation to that purpose. If a data subject has consented that photographs where he appears may be processed to automatically tag him in an online photo album with a facial recognition algorithm, this processing has to be achieved in a data protection friendly way: biometric data not needed anymore after the tagging of the images with the name, nickname or any other text specified by the data subject must be deleted. The creation of a permanent biometric database is a priori not necessary for this purpose.*
> (Article 29 Data Protection Working Party, 'Opinion 03/2012 on developments in biometric technologies', p. 7)

115. In light of this statement, Clearview's processing constitutes an entirely new purpose from original publication, for which it ought to have a separate, valid legal basis. As demonstrated above, this is non-existent, and Clearview therefore violates the purpose limitation principle.

4.7. Verstoß gegen die Pflicht, einen Vertreter zu benennen

116. Angesichts der Anwendbarkeit von Artikel 3(2) DSGVO ist Clearview auch verpflichtet, einen Vertreter in der EU gemäß Artikel 27(1) DSGVO zu benennen, da keine der Ausnahmen gemäß Artikel 27(2) DSGVO gilt (siehe auch für ähnliche Entscheidungen über das Fehlen eines Vertreters durch Datenschutzbehörden der EU-Mitgliedstaaten: Autoriteit Persoonsgegevens, 10 Dezember 2020, via https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/20210512_boetebesluit_ap_locatefamily.pdf; Commission Nationale pour la Proteccion de les Donees, 04 Februar 2020, via https://gdprhub.eu/index.php?title=CNPD_-_3018).

4.8. Schlussfolgerung

117. Clearview verstößt gegen die Grundsätze der Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz und der Zweckbindung, sowie gegen das Erfordernis einer Rechtsgrundlage.

5. ANTRÄGE UND ERSUCHEN

118. Der Beschwerdeführer stellt die folgenden Anträge und weist darauf hin, dass ähnliche Beschwerden bei verschiedenen europäischen Aufsichtsbehörden eingereicht wurden. Folglich wäre eine gemeinsame Untersuchung gemäß Artikel 62 DSGVO ggf. angebracht.

4.7. Violation of the requirement to appoint a representative

116. In light of the applicability of Article 3(2) GDPR, Clearview is also required to appoint a representative in the EU under Article 27(1) GDPR, as none of the exceptions under Article 27(2) GDPR applies (see also for similar decisions on the lack of a representative by EU Member State data protection authorities Autoriteit Persoonsgegevens, 10 December 2020, available at https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/20210512_boetebesluit_ap_locatefamily.pdf; Commission Nationale pour la Proteccion de les Donees, 04 February 2020, available at https://gdprhub.eu/index.php?title=CNPD_-_3018).

4.8. Conclusion

117. Clearview's processing constitutes a violation of the transparency, fairness and purpose limitation principles, and of the requirement for a lawful basis, as well as not having appointed a representative.

5. REQUESTS

118. The complainant makes the following requests and notes that similar complaints have been lodged with various European supervisory authorities. As such, a joint operation under Article 62 GDPR may be appropriate.

5.1. Ersuchen auf Unterrichtung über Stand und Ergebnisse der Beschwerde

119. Der Stand und die Ergebnisse dieser Beschwerde sollen uns in Einklang mit Artikel 77(2) DSGVO mitgeteilt werden.

5.2. Ersuchen einer umfassender Untersuchung

120. Der Beschwerdeführer ersucht die DSB, dass diese Beschwerde in Übereinstimmung mit den ihr gemäß Artikel 58(1)(a) DSGVO übertragenen Befugnissen vollständig zu untersuchen.

5.3. Antrag auf Erhängung eines Verarbeitungsverbots

121. Der Beschwerdeführer beantragt, dass Clearview gemäß Artikel 58(2)(f) DSGVO verboten wird,

i. die personenbezogenen Daten des Beschwerdeführers zu verarbeiten.
ii. personenbezogenen Daten von betroffenen Personen innerhalb der EU zu verarbeiten.

5.4. Ersuchen der Verhängung wirksamer, verhältnismäßiger und abschreckender Geldstrafen

122. Letztlich regt der Beschwerdeführer an, gemäß Artikel 58(2)(i) in Verbindung mit Artikel 83(5)(b) DSGVO, eine wirksame, angemessene und abschreckende Geldstrafe gegen Clearview zu verhängen.

5.1. Request to receive progress and the results of this investigation

119. We request that the progress and the results of this investigation are made available to us in accordance with Article 77(2) GDPR.

5.2. Request to fully investigate

120. The complainant hereby requests the DSB to fully investigate this complaint, in accordance with the powers vested in you by Article 58(1)(a) GDPR.

5.3. Request to impose a ban on processing

121. The Complainant requests that Clearview be imposed a ban according to Article 58(2)(f) DSGVO as follows:

i. The processing of the personal data of the Complainant.

ii. The processing of the personal data of data subjects within the EU.

5.4. Request to impose an effective, proportionate and dissuasive fine

122. Finally, the complainant requests that, by virtue of the powers provided by Article 58(2)(i) in combination with Article 83(5)(a) GDPR, impose an effective, proportionate and dissuasive fine against Clearview.

6. KONTAKT UND ÜBERSETZUNG

6.1. Kommunikation mit *noyb*

123. **Die Kommunikation zwischen *noyb* und der Datenschutzbehörde im Rahmen dieses Verfahrens kann per E-Mail an XXX unter Bezugnahme auf die im Titel dieser Beschwerde genannte Fallnummer erfolgen. Gerne stehen wir Ihnen auch unter der XXX zur Verfügung.**

6.2. Englische Übersetzung

124. Die Übersetzung ins Englisch ist eine Gefälligkeitsübersetzung. Sollte es zu Unstimmigkeiten zwischen den Übersetzungen kommen, ist die Version auf Deutsch die Maßgebliche, weil wir gesetzlich verpflichtet sind, bei der DSB auf Deutsch einzureichen.

6. CONTACT AND TRANSLATION

6.1. Communication with *noyb*

123. **Communication between *noyb* and the Data Protection Authority in the course of this procedure can be done by email at XXX with reference to the Case-No.as mentioned in the title of this complaint. We are also available by phone at XXX.**

6.2. English translation

124. We provide an informal English translation of this complaint. If there is any conflict in the translations, the German version should prevail because the law requires us to file this complaint with the Austrian supervisory authority in German.

Signature