brighter AI

Weltweite Datenschutzgesetze zur Verarbeitung öffentlicher Bild- und Videodaten

Ein Überblick über die wichtigsten internationalen Datenschutz-verordnungen und Best Practices in Zeiten von KI und Video Analytics

In Kooperation mit dem

KI BUNDESVERBAND

Mit Erkenntnissen von Entscheidern und Datenschutzexperten aus aller Welt, darunter

Capgemini EVOTEGRA iapp IBM IEF intel LiangDao pwc samasource SIGNATRIX

Verwendung dieses Dokuments

Dieser Bericht ist allgemeiner und informativer Natur und ist nicht als Rechtsberatung gedacht und sollte nicht als solche herangezogen werden. Die in diesem Bericht enthaltenen Informationen und Materialien sind möglicherweise nicht in allen (oder einigen) Situationen anwendbar und sollten nicht ohne spezifischen Rechtsberatung auf der Grundlage jeweiliger Umstände verwendet werden. brighter AI übernimmt keine Haftung oder Garantie für Aktualität, Richtigkeit und Vollständigkeit der Informationen.

Inhalt

Einführung 4

Übersicht 5

Datenschutzbestimmungen nach Region

- Europäische Union: DSGVO 6
- Kalifornien, USA: CCPA 8
- China: CSL & PIS 10
- Japan: APPI 12
- Südkorea: PIPA 14
- Brasilien: LGPD 16

Ausblick 18

Abkürzungsverzeichnis 20

Literaturverzeichnis 21

Einführung

Es besteht kein Zweifel daran, dass die andauernde Revolution im Bereich der künstlichen Intelligenz enorme Datenmengen erfordert. Vom Gesundheitswesen, über den Einzelhandel, bis hin zur Automobilbranche und dem öffentlichen Personenverkehr ist die Bild- und Videoanalyse eine Schlüsseltechnologie für neue digitale Lösungen. Intelligente Geschäfte sind bereits heute mit zahlreichen Kameras ausgestattet[1] und autonome Fahrzeuge werden Zettabytes an visuellen Daten erzeugen und verarbeiten[2].

Aufgrund jüngster Ereignisse, wie dem Einsatz von Gesichtserkennung während der Black-Lives-Matter-Proteste[3], nehmen die Bedenken hinsichtlich der Aufzeichnung und Verarbeitung öffentlicher Bilddaten zu. Nach starker Kritik der Öffentlichkeit stellten Unternehmen wie IBM, Microsoft und Amazon den Vertrieb der Software an die Polizei ein.[4] Während die Bedeutung von Datenschutz für die Bevölkerung und als Kernaspekt gesellschaftlicher Verantwortung von Unternehmen zunimmt, aktualisieren Gesetzgeber weltweit Richtlinien, um klare Regeln für die digitale Revolution aufzustellen. Für Unternehmen ist es wichtig, in diesem dynamischen Umfeld Schritt zu halten, um regulatorische Risiken zu minimieren und zukunftssichere Lösungen zu entwickeln, denen Verbraucher vertrauen.

In diesem Bericht tragen wir die wichtigsten internationalen Datenschutzgesetze und Best Practices zusammen, die bei der Verarbeitung öffentlicher Videodaten zu berücksichtigen sind. Basierend auf Erfahrungen aus Projekten in der ganzen Welt, fassen wir die wesentlichen Aspekte der Gesetzgebung aus sechs Regionen zusammen: der Europäischen Union, den Vereinigten Staaten, China, Japan, Südkorea und Brasilien. Darüber hinaus zeigen wir Ansichten führender Organisationen und Datenschutzexperten auf. Es besteht zwar eine gewisse Skepsis gegenüber dem Einfluss von Regulierungen auf den Fortschritt von KI und Analytics. Unternehmen schätzen die Einhaltung dieser Vorschriften jedoch immer mehr und entwickeln so zunehmend verantwortungsvolle, datengesteuerte Innovationen, da dies nicht nur von Behörden, sondern vor allem von Verbrauchern geschätzt wird.

"Etwa vier Terabyte Daten wird ein autonomes Fahrzeug in einer Fahrzeit von anderthalb Stunden erzeugen – dies entspricht, der Zeit, die eine Person durchschnittlich pro Tag im Auto verbringt". [2]

Kathy Winter
Vice President Automated Driving Solutions, Intel

"Regelungen zu Datenschutz und Datensicherheit sind der Be- bzw. Entschleuniger für Lösungen in den Bereichen autonomes Fahren und Smart City. Sie müssen auf dem Laufenden gehalten und an die digitale Revolution angepasst werden".

Dr. Yang Ji
Geschäftsführer,
LiangDao GmbH

Übersicht

Kriterien	EU **DSGVO**	USA **CCPA**	China **CSL & PIS**	Japan **APPI**	Südkorea **PIPA**	Brasilien **LGPD**
Anwendbarkeit (Entitäten)	Alle privat-wirtschaftlichen und öffentlichen Einrichtungen	Unternehmen mit • >25 Mio. USD Umsatz • Daten von >50.000 Verbrauchern • >50% des Umsatzes durch Verkauf von Daten	Alle Arten von Organisationen und Einzelpersonen	Alle Unternehmen, die personen-bezogene Daten verarbeiten	Jede Entität, die direkt oder indirekt personenbezogene Daten verwaltet	Alle Entitäten und öffentlichen Behörden
Territorialer Geltungsbereich	Entitäten, die in der EU gegründet wurden oder dort Waren und Dienstleistungen anbieten oder das Verhalten von Personen in der EU überwachen	Entitäten, die im Bundesstat Kalifornien Geschäfte tätigen	*Nicht angegeben,* CSL gilt auch für Entitäten außerhalb Chinas, wenn deren Aktivitäten die kritische Infra-struktur betreffen (Art. 75)	Entitäten, die in Japan gegründet wurden, dort eine Niederlassung haben und Dienst-leistungen in Japan anbieten	Entitäten, die in Südkorea gegründet wurden oder dort personen-bezogene Daten verarbeiten	Jede Entität, die personenbezogene Daten in Brasilien sammelt oder verarbeitet oder Waren und Dienstleistungen in Brasilien anbietet
Rechte von betroffenen Personen	• Information • Einspruch / Verweigerung der Zustimmung • Löschung • Zugriff • Berichtigung • Übertragbarkeit • Einschränkung der Verarbeitung	• Information • Einspruch ("opt-out") • Löschung • Zugriff • Übertragung • Keine Diskrimi-nierung für Ausübung dieser Rechte	• Information vor Sammlung / Verwendung der Daten • Entfernung oder Korrektur	• Information vor Sammlung / Verwendung der Daten • Löschung oder Korrektur • Beschwerde bei der PPC bei Verstößen	• Information • Zugang • Korrektur • Löschung	• Informationen • Verweigerrung der Zustimmung • Zugriff • Korrektur • Anonymisierung oder Löschung unnötiger oder übermäßiger Daten • Übertragbarkeit
Datenschutz-beauftragter	Erforderlich, falls: • öffentliche Behörde • Umfangreiche Beobachtung von Einzelpersonen • Verarbeitung spezieller Datenkategorien	*Nicht angegeben*	PIS erfordert, dass eine Person für den Schutz personen-bezogener Informationen verantwortlich ist	*Nicht angegeben*	Jeder Anwender von personen-bezogenen Daten muss einen DSB benennen	Jede Organisation die Daten verarbeitet muss einen DSB stellen
Analyse von Risiken	Datenschutz-Folgenabschätzung erforderlich, wenn Projekt ein "hohes Risiko" für die Daten von Einzelpersonen beinhalten könnte	Privatsphäre-Folgenabschätzung ist empfohlen	Sicherheits-bewertung muss durchgeführt werden, wenn Daten außerhalb Chinas übertragen werden	*Nicht angegeben*	Erforderlich für öffentliche Einrichtungen (aber nicht privat-wirtschaftliche Unternehmen) im Falle einer Datenpanne	Keine Angabe darüber, wann eine Folgenabschätzung erforderlich ist, aber die ANPD kann zu jeder Zeit die Durchführung einer solchen verlangen
Bußgelder	Bis zu 20 Mio. EUR oder 4% der jährlichen weltweiten Umsatzes	Bis zu 7.500 USD für jede (absichtliche) Verletzung, plus eine Entschädigung von bis zu 750 USD pro Verbraucher	Bis zu 1 Mio. CNY (130.000 EUR), zuzüglich 1-10 mal den Betrag der unrechtmäßigen Gewinne, plus zivilrechtliche Bußgelder für verantwortliches Personal	Bis zu 500.000 JPY (4.000 EUR) und eine Gefängnis-strafe von bis zu einem Jahr	Geldstrafen bis zu 50 Mio. KRW (35.000 EUR), plus eine Gefängnis-strafe von bis zu fünf Jahren für verantwortliches Personal	Bis zu 50 Mio. BRL (11,5 Mio. EUR), oder bis zu 2% des jährlichen Umsatzes

Europäische Union
Datenschutz-Grundverordnung

Anwendbar seit

25.05.2018

Aufsichtsbehörde

Unabhängige Datenschutzbehörde in jedem Mitgliedsstaat, welche Handlungs-empfehlung äußert und Beschwerden bearbeitet

Die DSGVO wird weithin als globaler "Goldstandard" für Datenschutzgesetze gesehen und ist das wohl umfassendste und strengste Gesetz seiner Art.[5] Mit hohen Bußgeldern von bis zu 20 Millionen Euro oder 4% des weltweiten Jahresumsatzes, kann es schwerwiegende Auswirkungen haben, sodass der Schutz der Privatsphäre seit der Einführung in 2018 zunehmend zu einer Priorität auf der Agenda von Unternehmen geworden ist.[6]

Während einige europäische Unternehmen einen Wettbewerbsnachteil empfinden, gilt die Verordnung für alle Unternehmen, die in EU-Mitgliedstaaten tätig sind, und eine weltweite Übernahme von DSGVO-Grundsätzen ist klar erkennbar.[7] Selbst das kontroverse Urteil des Europäischen Gerichtshofs, in welchem "Privacy Shield", das Abkommen über den Datenaustausch zwischen der EU und den USA, entkräftet wurde, könnte letztlich eine internationale Konvergenz beschleunigen.

"Die ersten Jahre der DSGVO waren von Einschränkungen und schlechter User Experience geprägt. Dennoch hat mit dieser Gesetzgebung zum ersten Mal ein politisches System seine Grundwerte weit über sein eigenes Tech-Ökosystem hinaus durchgesetzt, und so Vertrauen und Akzeptanz der Anwender gefördert – die Einhaltung wird bereits zu einem globalen Wettbewerbsvorteil."

Clark Parsons
Geschäftsführer, Internet Economy Foundation
Partner, iconomy

Grundprinzipien:

Datenminimierung Personenbezogene Daten müssen angemessen und sachdienlich und “auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt“ sein (Art. 5). Grundlagen für eine rechtmäßige Verarbeitung können Einwilligung, ein Vertrag mit der betroffenen Person, gesetzliche Verpflichtungen, der Schutz lebenswichtiger Interessen der betroffenen Person, öffentliche Interessen und berechtigte Interessen des Verantwortlichen sein (Art. 6).

Zustimmung Die Einwilligung der betroffenen Person ist die häufigste Grundlage für eine rechtmäßige Verarbeitung. Diese Einwilligung muss "frei, ausdrücklich, informiert und unmissverständlich" erteilt werden (Art. 7 & Erwägungsgrund 32).

Folgenabschätzung Wenn die Verarbeitung zu Risiken für die Rechte betroffener Personen führen könnte, z.B. durch den Einsatz neuer Technologien wie Videoanalyse oder KI, sollte eine Datenschutz-Folgenabschätzung durchgeführt werden, um potenzielle Risiken zu ermitteln und abzuschwächen (Art. 35). Bei dieser Durchführung ist der Rat einer Datenschutzbeauftragten einzuholen, die für große datengesteuerte Unternehmen erforderlich ist.

Privacy by Default & by Design sind als Datenschutz-konzept nicht neu – mit der DSGVO aber gesetzliche Vorgabe. “by default" bedeutet, dass strengste datenschutzfreundliche Voreinstellungen der Standard sein müssen, und “by design", dass dem Stand der Technik entsprechende technische und organisatorische Maßnahmen (TOMs) vorhanden sein müssen, um bestmöglichen Datenschutz zu gewährleisten. Hier wird die Einführung von Technologien zur Verbesserung der Privatsphäre, z.B. Pseudonymisierung (Art. 25), empfohlen.

Verarbeitung zu wissenschaftlichen Forschungs-zwecken Auch hier findet die DSGVO Anwendung (Erwägungsgrund 159). Wie Art. 89 weiter ausführt, unterliegt die Verarbeitung für diese Zwecke geeigneten Bedingungen und Garantien für die Rechte und Freiheiten der betroffenen Person.

Sanktionen

Bis Ende Januar 2020 haben die europäischen Datenschutzbehörden Geldstrafen in Höhe von 114 Mio. EUR für Verstöße gegen die DSGVO verhängt.[8]

"Es ist eine langsame Entwicklung zum Erreichen der Rechtssicherheit, die Aufsichtsbehörden benötigen, um höhere Geldbußen zu verhängen.“ [9]

Ross McKean
Partner, DLA Piper

Zahlen & Fakten

Nachdem eine Nieder-länderin Fotos ihrer Enkel ohne deren Zustimmung auf Facebook gepostet hatte, wurde sie durch ein Gerichtsurteil gezwungen, diese zu löschen. [10]

Kalifornien, USA
California Consumer Privacy Act

Anwendbar seit

01.01.2020

Aufsichtsbehörde

Der Generalstaatsanwalt hat die Befugnis, bei mutmaßlichen CCPA-Verstößen unabhängige Untersuchungen und Maßnahmen einzuleiten

Erst in diesem Jahr eingeführt, ist die CCPA das umfassendste Datenschutzgesetz der Vereinigten Staaten[12] und das erste, das Verbrauchern eine Kontrolle darüber gibt, wie ihre persönlichen Daten, insbesondere online, verwendet werden.[13] Angesichts seiner wirtschaftlichen Bedeutung (als eigenes Land wäre Kalifornien die fünftgrößte Volkswirtschaft der Welt) wird erwartet, dass die Auswirkungen von CCPA ähnlich weitreichend sind wie die der DSGVO.

Während der allgemeine Zweck der CCPA eindeutig ist, führen teils unklare Definitionen und Widersprüche mit branchenspezifischen Vorschriften bereits zu zahlreichen Debatten.[14] Außerdem werden Stimmen lauter, die ein landesweit einheitliches Gesetz fordern, da weitere US-Bundesstaaten damit beginnen eigene Datenschutzgesetze einzuführen.[15]

Zur Überraschung vieler ist ausgerechnet Kalifornien, Heimat des Silicon Valleys, Amerikas Vorreiter beim Datenschutz. Erst kürzlich hat die Stadt San Francisco als erste den behördlichen Einsatz von Gesichtserkennungstechnologien verboten.[16]

"Es ist wichtig, nicht davon auszugehen, dass die CCPA eine Art 'GDPR Lite' ist, denn es gibt diverse Unterschiede, die zu einer Nichteinhaltung führen können. Wenn der Unterschied zwischen den beiden verstanden wird, können Kontrollen eingeführt werden, um die Einhaltung beider Vorschriften zu gewährleisten."

Cindy Abramson
Vice President Customer Trust, Samasource

Grundprinzipien:

Benachrichtigungsanforderung Vor oder zum Zeitpunkt der Datenerhebung müssen Kategorien der zu erhebenden personenbezogenen Daten, Zweck der Erhebung und Rechte des Verbrauchers mitgeteilt werden. Die Informationen müssen offen zugänglich sein und jährlich aktualisiert werden (1798.100).

"Opt-Out" Es ist keine ausdrückliche Zustimmung erforderlich, aber Verbraucher können nachträglich Widerspruch einlegen – was bei öffentlich aufgezeichneten Videos nur schwer realisierbar ist.

Zweckbindung Unternehmen können personenbezogene Daten für geschäftliche oder kommerzielle Zwecke erheben und weiterverarbeiten. Während sich der Geschäftszweck auf betriebliche Aktivitäten einschließlich Rechnungsprüfung, F&E, Sicherheit oder Wartung bezieht, ist der kommerzielle Zweck als "Förderung der kommerziellen oder wirtschaftlichen Interessen einer Person" definiert (1798.140). Aufgrund der weitgefassten Definition und der Möglichkeit doppelter Zweckbestimmung ist eine eindeutige Unterscheidung nicht immer möglich.[17]

Datenminimierung Personenbezogene Daten sollten "notwendig und verhältnismäßig sein, um den operativen Zweck zu erreichen", für den sie erhoben wurden (1798.140).

Datentransfer Der grenzüberschreitende Datentransfer wird durch CCPA nicht eingeschränkt. Die Datenübermittlung an Dritte und Dienstleister erfordert eine schriftliche Vereinbarung, die bestimmte Klauseln enthalten muss.[18]

Anonymisierung & Pseudonymisierung CCPA gilt nicht für entpersonalisierte, aggregierte Informationen. Es wird nicht definiert, ob die gleichen Regeln für pseudonymisierte Daten gelten.[19]

"Der Schutz von Verbrauchern in Bezug auf persönliche Daten [...] wird höchstwahrscheinlich in anderen Bundesstaaten und schließlich auf Bundesebene kodifiziert. [...] Datenschutzgesetze werden an Umfang und Genauigkeit zunehmen.." [19]

Steve Stein
Principal, KPMG Cyber Security Services

Sanktionen

Die 6-monatige Frist zur Einführung endete am 1. Juli 2020 – bis heute gab es keine Urteile.[19] Allerdings laufen Verfahren, u.a. gegen Clearview AI, TikTok, Zoom & Walmart.

"Wenn man die DSGVO für holprig hielt, dann wird CCPA eine echte Achterbahnfahrt. Es handelt sich um eine komplexe Reihe neuer Regeln, die noch in Arbeit sind." [13]

Reece Hirsch
Partner, Morgan Lewis

Zahlen & Fakten

In einer aktuellen Umfrage von KPMG unter US-Verbrauchern gaben 97% der Befragten an, dass Datenschutz für sie wichtig ist, und 42% betrachten die Anmeldung mit Hilfe von Gesichtserkennungtechnologien als Datenschutzrisiko.[19]

China Cybersecurity Law & Personal Information Security Specification

Anwendbar seit

CSL: 01.06.2017
PIS (Update): 01.10.2020

Aufsichtsbehörde

Cyberspace-Verwaltung Chinas (Cyberspace Administration of China, CAC), Ministerium für öffentliche Sicherheit (Ministry of Public Security, MPS), Ministerium für Industrie und Informationstechnik (Ministry of Industry and Information Technology, MIIT)

Trotz des Fokus auf rasanter Innovationskraft gewinnt Datenschutz auch in China zunehmend an Bedeutung, was anhand erster Datenschutzklagen deutlich wird. Insgesamt sind die chinesischen Datenschutzgesetze sehr komplex. Unternehmen, die Videodaten erfassen und verarbeiten wollen, müssen mit lokalen Partnern zusammenarbeiten und sollten sich spezialisierten Rechtsrat einholen, um potenzielle Fallstricke zu vermeiden.

Das chinesische Cybersicherheitsgesetz CSL ist der Rechtsrahmen für die Datenverarbeitung und den Schutz personenbezogener Daten. Es enthält keine praktischen Richtlinien.[20] Dafür finden sich in der Spezifikation zur Sicherheit personenbezogener Daten (PIS), verschiedene De-facto-Datenschutz-vorschriften[21] und detailliertere Anforderungen an Erhebung & Verarbeitung personenbezogener Daten.

"In einer digitalisierten Gesellschaft ist Datensicherheit die Garantie für andere Formen der Sicherheit. Ohne Datenschutz verlieren alle Produkte und Dienstleistungen, die auf der Informationstechnologie basieren, ihre Sicherheitsunterstützung." [22]

Mo Jihong
Rechtsprofessor, Chinesische Akademie der Sozialwissenschaften

Grundprinzipien:

Zustimmungsverpflichtung Wenn ein Produkt oder eine Dienstleistung persönliche Informationen sammelt, muss der Anbieter dies angeben und die Zustimmung des Nutzers einholen (CSL, Art. 22). Dies bedeutet, dass die betroffene Person über Zweck, Methode, Umfang und Regeln der Verarbeitung informiert werden muss (CSL, Art. 41).

Zweckbindung Die Verarbeitung von personenbezogenen Daten ist legal, wenn sie gerechtfertigt, notwendig und für einen bestimmten Zweck festgelegt ist (PIS, Art. 4). Der "Data Controller" trägt die Verantwortung für Verletzungen der Rechte und Interessen einer betroffenen Person, die durch eine unsachgemäße Verarbeitung personenbezogener Daten verursacht werden. [21]

Minimierungsgrundsatz Es darf nur ein Minimum an Arten und Mengen personenbezogener Daten verarbeitet werden, die für die Zwecke erforderlich sind, für die eine Einwilligung eingeholt wurde – es sei denn, die betroffene Person stimmt ausdrücklich zu (PIS, Art. 4). Nach Erreichen des Zwecks sind die Daten umgehend zu löschen (PIS, Art. 4).

Grenzüberschreitender Transfer Persönliche Informationen, die in China generiert und gesammelt werden, müssen innerhalb von China gespeichert werden. Der grenzüberschreitende Transfer unterliegt besonderen Regeln: Verantwortliche müssen eine Sicherheitsbeurteilung durchführen und die Anforderungen der von den zuständigen Ämtern erlassenen Maßnahmen und einschlägigen Normen einhalten (PIS, Art. 8).

Persönliche biometrische Informationen Dazu gehören Gesichtserkennungsmerkmale, die das häufigste Merkmal öffentlich aufgezeichneter Bild- und Videodaten sind. Auch hier muss die betroffene Person über die Erfassung informiert werden und ihre ausdrückliche Zustimmung geben. Biometrische Daten müssen getrennt von persönlichen Identifikationsdaten gespeichert werden.[23]

Anonymisierung & Pseudonymisierung Anonymisierte Daten gelten nicht als personenbezogen und unterliegen nicht dem Datenschutz (PIS Art. 3). Auch eine Pseudonymisierung vermindert das Risiko der Nichteinhaltung.[20]

Sanktionen

Im Jahr 2019 hat das Cybersecurity Center 683 Software-Unternehmen aus diversen Branchen von E-Commerce bis Bankwesen bestraft.[24]

"Die Verkündung und Umsetzung des Cybersicherheitsgesetzes schützt nicht nur die Interessen der Massen im Internet rechtlich, sie schützt auch die nationale Netz-Souveränität und -Sicherheit und fördert die Anwendung von IT und das große Potenzial des Internets." [25]

Zhuang Rongwen
Leiter, Behörde für Cyber-Sicherheit

Zahlen & Fakten

Im Juli 2019 führte der Safaripark Hangzhou die Gesichtserkennung für Inhaber von Jahreskarten ein und erklärte Tickets für ungültig, deren Inhaber ihre biometrischen Daten nicht bis Oktober des Jahres registrierten. Der Park wurde hierfür verklagt.[26]

Japan
Act on the Protection of Personal Information

Anwendbar seit

Neue Zusatzartikel: 30.05.2017

Aufsichtsbehörde

Die Kommission zum Schutz personenbezogener Daten (PPC) hat das Recht, Audits durchzuführen und Unterlassungsverfügungen zu erlassen, kann jedoch keine Strafen verhängen

Ursprünglich im Jahr 2003 eingeführt, war APPI, das japanische Gesetz zum Schutz personenbezogener Daten, die erste umfassende Datenschutzvorschrift in Asien. Die letzte Änderung im Jahr 2017 wurde von der Kommission zum Schutz personenbezogener Daten verabschiedet. Die unabhängige Behörde, schützt die Rechte und Interessen von Einzelpersonen und schafft gleichzeitig Rahmenbedingungen für eine ordnungsgemäße und effektive Nutzung persönlicher Informationen.

Im Jahr 2019 gab die EU-Kommission ihren Angemessenheitsbeschluss in Bezug auf Japan bekannt, womit dies die erste formelle Anerkennung der bilateralen und gegenseitigen Angemessenheit von Datenschutzstandards mit einem Nicht-EU-Land darstellt.

"Als Japan seine Regeln zum Schutz persönlicher Daten schuf, übernahm es einzelne Elemente aus den Gesetzen anderer Länder (...). Ein ausgewogener Ansatz ist gesund – wir müssen die Privatsphäre schützen, aber gleichzeitig Raum für Innovationen lassen." [27]

Jonathan Soble
Communication Lead, World Economic Forum

Grundprinzipien:

Zweckveröffentlichung Eine Entität, die personenbezogenene Daten verarbeitet, muss den Zweck der Nutzung dieser Daten vor oder nach deren Erwerb veröffentlichen (Art. 18). Die betroffene Person kann also entweder vorher ihre Einwilligung geben oder später die Zustimmung verweigern. APPI definiert biometrische Daten, die gewöhnlich in visuellen Daten erfasst werden, ausdrücklich als Teil personenbezogener Daten.

Datenminimierung Persönliche Informationen dürfen nicht über den zur Erreichung des veröffentlichten Verwendungszwecks notwendigen Umfang hinaus verarbeitet werden (Art. 16). Die Daten dürfen nicht durch eine Täuschung oder auf andere unrechtmäßige Weise erlangt werden (Art. 17).

Transfer über die Landesgrenzen Hierfür ist die vorhergegangene Einwilligung der betroffenen Person erforderlich, es sei denn, das Zielland ist ein Land mit angemessenen Standards für den Schutz der Privatsphäre (Art. 24), z.B. die Europäische Union.

Anonymisierung & Pseudonymisierung Die Verarbeitung von pseudonymisierten Informationen befreit von der Verpflichtung, bestimmte Anforderungen der APPI zu erfüllen, wie z.B. Forderungen nach Offenlegung oder Löschung.[28] Anonymisierte Informationen können über den mitgeteilten Verwendungszweck hinaus verarbeitet und ohne Zustimmung an Dritte weitergegeben werden.[29]

Berichterstattung an die PPC Gemäß neuen Zusatzartikeln wird in 2020 eine Berichterstattung von Verstößen an die PPC verpflichtend. Diese Verpflichtung wird voraussichtlich auf bestimmte Verstöße beschränkt, die ein erhebliches Risiko für die Rechte und Interessen von Einzelnen darstellen.[29]

"Unternehmen müssen personenbezogene Daten strenger verwalten, da ihre zunehmend globalisierten Aktivitäten zu einer häufigeren Übertragung solcher Daten zwischen (Japan und) Übersee führen." [30]

Harumichi Yuasa
Professor, Institute of Information Security Yokohama

Sanktionen

PPC urteilte, dass Unternehmen, einschließlich der Mitsubishi Corp, Mitsubishi Electric Corp. und Toyota Motor Corp, personenbezogene Daten unangemessen verarbeitet haben. [31] Bis heute gibt es allerdings noch keine Strafzahlungen.

Zahlen & Fakten

Telefonhersteller und -betreiber haben freiwillig zur Implementierung eines Kamera-"Shutter-Sounds" kooperiert, um "Datenschutzprobleme" zu vermeiden, obwohl dies gesetzlich nicht vorgeschrieben wurde. [32]

Südkorea
Personal Information Protection Act

Anwendbar seit

30.09.2011
Neue Zusatzartikel:
01.07.2020

Aufsichtsbehörde

Die Kommission zum Schutz personenbezogener Daten (Personal Information Protection Commission, PIPC) konsultiert und veröffentlicht Richtlinien; das Ministerium für Inneres und Sicherheit (Ministry of the Interior and Safety , MOIS) ist für die Untersuchung und Durchsetzung verantwortlich

Südkoreas Gesetz zum Schutz personenbezogener Daten PIPA ist eines der strengsten Datenschutzgesetze der Welt.[33] Ähnlich wie die DSGVO schützt es das Recht auf Privatsphäre aus der perspektive der betroffenen Person, ist umfassend und gilt für die meisten Organisationen, inklusive für staatliche Behörden.[33]

Das Gesetz zielt darauf ab, das Recht und die Interessen des Einzelnen zu stärken und die Würde und den Wert des Einzelnen anzuerkennen (Art. 1). Anfang 2020 verabschiedete die Koreanische Nationalversammlung neue Zusatzartikel ihrer Datenschutzgesetze, um die behördliche Aufsicht zu stärken und vermutlich auch, um den Angemessenheitsbeschluss der EU-Kommission zu beschleunigen, die den Datenfluss zwischen der EU und Südkorea erleichtern soll.

"Fragen des Datenschutzes haben in den letzten Jahren in Südkorea erheblich an Bedeutung gewonnen. Dieses Phänomen spiegelt sich darin wider, dass einschlägige Gesetze und Vorschriften häufig verändert wurden." [34]

Haksoo Ko
Professor, Seoul National University School of Law

Grundprinzipien:

Grundsätze zum Schutz personenbezogener Daten Personenbezogene Daten müssen für spezifische, rechtmäßige Zwecke gesammelt und dürfen nicht für unvereinbarte, Zwecke verwendet werden. Darüber hinaus müssen die Daten korrekt sein und sicher aufbewahrt werden. Die Verarbeiter werden aufgefordert, ihre Datenschutzrichtlinien zu veröffentlichen und personenbezogene Daten, wo immer möglich, zu anonymisieren (Art. 3).

Zustimmung und Wahl Die betroffene Person hat das Recht, in die Verarbeitung personenbezogener Daten einzuwilligen oder diese abzulehnen, darüber informiert zu werden, sowie den Umfang der Einwilligung zu wählen, die Verarbeitung zu bestätigen, auf die personenbezogenen Daten zuzugreifen, sie zu berichtigen und zu löschen (Art. 4). Keine Einwilligung ist jedoch erforderlich, wenn der neue Umfang "in einem angemessenen Verhältnis" zum ursprünglichen Zweck der Verarbeitung steht (Art. 15).

Pseudonymisierung & Anonymisierung: Anonymisierte Informationen werden als nicht-personenbezogene informationen betrachtet und unterliegen daher nicht dem PIPA (Art. 58). Pseudonymisierte Daten können ohne Einwilligung der betroffenen Person für verschiedene Zwecke verarbeitet werden, einschließlich "kommerzieller Zwecke wie die Entwicklung datenbasierter, innovativer Technologien, Produkte und Dienstleistungen"[3].

Spezifikationen über Visuelle Daten "Visuelle Datenverarbeitungsgeräte" sind definiert als Geräte, die fest installiert sind, um Bilder von Personen und/oder Dingen aufzunehmen und/oder zu übertragen (Art. 2). An öffentlichen Orten dürfen sie nur zur Vermeidung von Straftaten[4] und Bränden oder für Verkehrs-(kontroll-)Informationen installiert werden (Art. 25). Hierbei ist ein sichtbarer Hinweis a) zum Zweck der Installation und den genauen Standort, b) die Reichweite und Dauer des Einsatzes, sowie c) Name und Kontakt der Firma oder der verantwortlichen Person erforderlich. PIPA weist ausdrücklich darauf hin, dass visuelle Datenverarbeitungsgeräte nicht für andere Zwecke als die ursprünglichen verwendet werden dürfen (Art. 25).

Sanktionen

Kim Jin-Hwan, Datenschutzbeauftragter von Hana Tour Service Inc., wurde der Verletzung des PIPA für schuldig befunden und musste eine Strafe in Höhe von 10 Mio. KRW (7.000 EUR) zahlen. Gegen das Unternehmen wurde eine separate Geldstrafe in Höhe von 327,25 Mio. KRW (232.750 EUR) erlassen.[37]

Zahlen & Fakten

Eine Umfrage von Ipsos ergab, dass 9% der Südkoreaner der Meinung sind, dass die Verwendung von KI und Gesichtserkennung durch die Regierung "unter keinen Umständen erlaubt sein sollte, um die Privatsphäre eines jeden zu jeder zeit vollständig zu gewährleisten", verglichen mit 19% in Japan, 18% in China und 16% im weltweiten Durchschnitt.[38]

Brasilien
General Data Protection Act

Anwendbar ab

16.08.2020
(Verzögerung aufgrund von COVID-19 verzögert)

Aufsichtsbehörde

Die Nationale Datenschutzbehörde (ANPD) wird befugt sein, Vorschriften und Verfahren bzgl. dem Schutz personen-bezogener Daten zu erlassen und Verstöße zu überwachen und zu sanktionieren

Das Allgemeine Datenschutzgesetz LGPD, auf Portugiesisch "Lei Geral de Proteção de Dados", soll den brasilianischen Rechtsrahmen in Bezug auf personenbezogene Daten klären, indem es einige der über 40 bestehenden Bundesvorschriften ersetzt und andere ergänzt. Es soll die Behandlung der persönlichen Daten aller natürlichen Personen in Brasilien regeln und bildet die erste umfassende Datenschutzvorschrift des Landes.[39]

Das LGPD sollte im Februar 2020 in Kraft treten, wurde jedoch auf August 2020 verschoben. Als COVID-19 das Land traf, versuchte der Senat, das Gesetz bis Mai 2021 und seine Sanktionen bis August 2021 zu verschieben. Bis heute gibt es hierzu keine Entscheidung.

"Wir sehen LGPD als eine Chance für die nachhaltige Entwicklung des Landes mit der sichergestellt wird, dass entscheidende Grundrechte und datengesteuerte Innovationen in einem Umfeld von Transparenz und Vertrauen koexistieren können." [40]

Fabricio Lira
Head of Data and Artificial Intelligence, IBM Brasilien

Grundprinzipien:

Anforderungen an die Verarbeitung personenbezogener Daten LGPD nennt zehn Rechtsgrundlagen inklusive Einwilligung, aber auch für den Schutz von Krediten (Kap. 1, Art. 7). Damit ist dies das erste und bisher einzige Gesetz zum Schutz der Privatsphäre, das eine Spezifikation enthält, die es Finanzinstituten erlaubt, Daten für Kreditbeurteilungen zu verwenden. Biometrische Daten wie die Abbildung von Gesichtern in Kameraaufnahmen, sind in LGPD zu sensiblen personenbezogenen Daten erklärt worden. Hier ist die Einwilligung der betroffenen Person die vorhergesehene Grundlage für Erhebung und Verarbeitung (Art. 11).

Grundsätze für die Datenverarbeitung Notwendigkeit der Datenminimierung, Genauigkeit, Speicherbegrenzung, Sicherheit, Rechtmäßigkeit, Fairness, Verantwortlichkeit, Zweckbindung und Transparenz bei der Verwendung personenbezogener Daten.[41] Ferner verbietet LGPD ausdrücklich die Verarbeitung personenbezogener Daten für "diskriminierende" Zwecke.[42]

Privacy by Default & by Design Das Gesetz definiert die Übernahme von Praktiken, die Privatsphäre und Datenschutzrechte garantieren, als obligatorisch bei der Gestaltung von Dienstleistungen, Produkten und Geschäftsmodellen. Außerdem sollten die Kontrollen der Privatsphäre, insbesondere im Online-Bereich, nach Voreinstellung bestmöglich geschützt sein, und die betroffenen Personen sollten die Möglichkeit des "opt-in" haben.[42]

Pseudonymisierung & Anonymisierung Laut LGPD sollen personenbezogene Daten nach Möglichkeit pseudonymisiert oder gar anonymisiert werden (Kap. 2, Art. 7). Anonymisierte Daten gelten nicht als personenbezogene Daten und sind daher ausdrücklich von der Gesetzesanwendung ausgeschlossen – außer, wenn der Prozess der Anonymisierung rückgängig gemacht wurde bzw. gemacht werden kann (Kap. 2, Art. 12).

Sanktionen

LGPD ist noch nicht in Kraft, und Sanktionen werden voraussichtlich nicht vor August 2021 durchführbar sein.

"Noch vor der Verpflichtung zur Einhaltung lokaler Gesetze, ist Datenschutz für IBM ein Anliegen im Kontext von Vertrauen und Transparenz."[40]

Fabricio Lira
Head of Data and Artificial Intelligence, IBM Brasilien

Zahlen & Fakten

Eine Umfrage von YouGov zeigt, dass fast 83% der Brasilianer denken, dass die Regierungen mehr tun sollten, um Technologieunternehmen und deren Kontrolle über das Leben von Menschen im Internet zu regulieren.[43]

Ausblick

Die Betrachtung von Datenschutzbestimmungen verschiedener Märkte zeigt: In einer Welt, in der Datenerfassungs- und KI-Projekte oftmals global sind, sind Datenschutzgesetze dies von Natur aus nicht.

Dennoch sind Staaten zunehmend darum bemüht die Gesetze zu harmonisieren – nicht nur um Datentransfers für multinationale Unternehmen zu erleichtern, sondern auch, um Menschen dieselben Grundrechte zu geben. Gleichzeitig ist es hierbei unvermeidlich, dass konstitutionelle, gesellschaftliche und wirtschaftliche Gegebenheiten auch zukünftig zu Unterschieden führen werden. Darüber hinaus hat die jüngste Entscheidung des Europäischen Gerichtshof zu "Privacy Shield" gezeigt, dass Maßnahmen zur Angleichung zwischen Ländern schnell wieder aufgehoben werden können.[44] Daher bleibt eine globale Perspektive für die Compliance entscheidend.

Die meisten Datenschutzbestimmungen definieren personenbezogene Daten recht allgemein und enthalten nur selten spezifische Richtlinien für Bild- und Videodaten. Beim Blick auf jüngste Ereignisse zeigt sich, dass "visueller" Datenschutz selbst bei den großen Themen des Jahres thematisiert wurde: COVID-19 beschleunigte die Nutzung von Videoanalysen[45] und die Proteste in Hongkong und den USA führten zu intensiven Debatten über den Einsatz von Gesichtserkennungstechnologien und ihrer Gefahren.[46,47]

Bereits 2017 fragte *The Atlantic*: "Who owns your face?".[48] Der Schutz visueller Daten ist somit kein neues Thema, sondern eines, das sich ähnlich schnell entwickelt wie die Technologie selbst. Das südkoreanische PIPA ist das einzige Datenschutzgesetz in unserem Bericht, das Videodaten explizit adressiert – jedoch nur mit Bezug auf "stationäre visuelle Datenerfassungsgeräte". Da die Vorschriften stets an neue Entwicklungen angepasst werden und es Forderungen nach mehr Klarheit gibt, ist es wahrscheinlich, dass dieser Bereich weiter spezifiziert wird. In Hinblick auf den Einsatz von Gesichtserkennung durch die Polizei gibt es außerdem zunehmende Sorgen in der Bevölkerung. Auch hier scheint das Verbot von Gesichtserkennung in San Francisco der Anfang eines stärkeren Fokus auf Bilddaten zu sein.

"Es gibt noch viel zu tun, bevor wir uns eine Zukunft vorstellen können, in der Datenschutzgesetze 'harmonisiert' sind. (...) Viele Länder im asiatisch-pazifischer Raum haben sich von der (...) DSGVO inspirieren lassen, indem sie entweder ähnliche oder strengere Gesetze erlassen." [30]

Deloitte

"Dein Gesicht gehört dir. Es ist ein bestimmendes Merkmal deiner Identität. Es ist aber auch nur ein weiterer Datenpunkt, der darauf wartet, gesammelt zu werden. In einer Zeit, in der Kameras allgegenwärtig sind (...), sind Gesichter zunehmend auffindbar." [48]

Adrienne LaFrance
Chefredakteurin, The Atlantic

Insgesamt wird deutlich, dass Unternehmen sich bei der Erfassung und Verarbeitung von Videodaten in der Öffentlichkeit in einem sensiblen, volatilen und fragmentierten regulatorischen Umfeld bewegen. Gesetze und Vereinbarungen werden fortwährend aktualisiert und eine weltweite Annäherung ist weiterhin "work-in-progress". Während gesellschaftliche Bedenken allgemein zunehmen, besteht weiterhin eine große Akzeptanz, wenn es um Sicherheit geht. Dies ist auch anhand der Corona-Krise sichtbar.

Begleitet vom rechtlichen und gesellschaftlichen Diskurs, wird erkennbar, dass sich die Einstellung der Technologiebranche – bekannt für "Speed over Caution" – ändert und immer mehr Unternehmen Grundsätze wie "Privacy by Design" aufgreifen, um so von rechtmäßig gesammelten Daten und dem Vertrauen der Konsumenten zu profitieren.

Unternehmen, die sich mit Analytics- und KI-Projekten befassen, sollten Datenschutz und Innovation nicht als unlösbares Dilemma, sondern als Chance sehen. Datenschutzbestimmungen sind keine Sackgasse für Projekte in Computer Vision und Machine Learning. (Das will auch der Gesetzgeber nicht!) Beispiele führender Unternehmen zeigen, dass es möglich ist, den Datenschutzrahmen anzulegen und Daten auf legitime Weise zu erheben und zu verarbeiten, um nachhaltige Innovationen im Einklang mit Gesetz und sozialer Verantwortung zu entwickeln. Hierzu gehört, dass Unternehmen auf dem neuesten Stand bleiben, spezialisierte Mitarbeiter einstellen und die Sicherheitsmaßnahmen ständig anpassen. Im besten Fall führen Maßnahmen zu Respekt und Vertrauen, der Minimierung von Risiken wie Reputationsverlust und Geldbußen – ohne eine Beeinträchtigung der Entwicklung und Nutzung datengesteuerter Innovation.

"Wir arbeiten mit Computer Vision und nehmen den Datenschutz sehr ernst. Unsere Kunden schätzen diesen Mehrwert unseres Produkts, da es die perfekte Kombination aus Sicherheit und Innovation bietet. Am Ende wird es zu einem Wettbewerbsvorteil, die Privatsphäre als integralen Bestandteil des Produktdesigns zu betrachten. "

Christoph Schwerdtfeger
Head of AI & Co-Founder Signatrix

"Unternehmen müssen das Datenschutzbewusstsein von Mitarbeiter fördern und fortschrittliche Technologien integrieren, um die Effizienz bei der Datenerkennung, -verwaltung, und -qualität, sowie Cyber- und Informationssicherheit zu steigern. Unternehmen, die diese Maßnahmen proaktiv ergreifen und Datenschutzgesetze als Chance sehen, werden sich einen erheblichen Wettbewerbsvorteil sichern." [11]

Capgemini

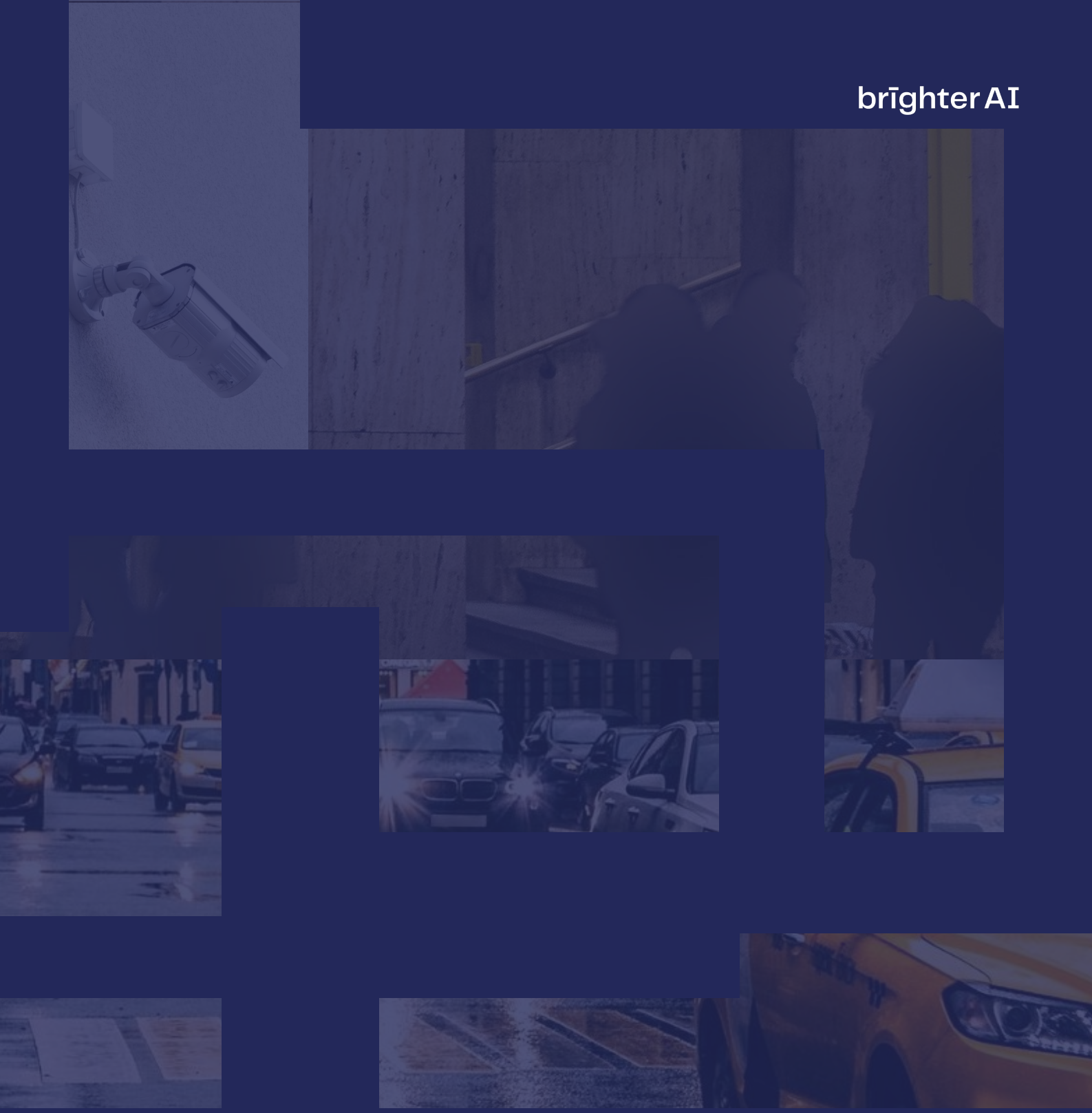
Abkürzungsverzeichnis

ANPD	National Data Protection Authority (Brasilianische Datenschutzbehörde)
APPI	Act of the Protection of Personal Information (Japanisches Gesetz zum Schutz personenbezogener Daten)
BRL	Brasilianische Real (Währung)
CAC	Cyberspace Administration of China (Cyberspace-Verwaltung Chinas)
CCPA	California Consumer Privacy Act (Kalifornisches Datenschutzgesetz)
CSL	Cybersecurity Law (Chinesisches Cybersicherheitsgesetz)
CNY	Chinesischer Yuan, Renminbi (Währung)
DSB	Datenschutzbeauftragter
DSGVO	Datenschutzgrundverordnung
EUR	Euro (Währung)
F&E	Forschung und Entwicklung
IAPP	International Association of Privacy Professionals (Internationale Vereinigung von Datenschutzfachleuten)
JPY	Japanischer Yen (Währung)
KI	Künstliche Intelligenz
KRW	Südkoreanische Won (Währung)
LGPD	Lei Geral de Proteção de Dados (Brasilianisches Datenschutzgesetz)
MIIT	Minister of Industry and Information Technology (Chinas Ministerium für Industrie und Informationstechnik)
MOIS	Ministry of the Interior and Safety (Südkoreas Ministerium für Inneres und Sicherheit)
MPS	Ministry of Public Security (Chinas Ministerium für öffentliche Sicherheit)
PIPA	Personal Information Protection Act (Südkoreanisches Datenschutzgesetz)
PIPC	Personal Information Protection Commission (Südkoreanische Datenschutzbehörde)
PIS	Personal Information Security Specification (Chinas Spezifikation zur Sicherheit personenbezogener Daten)
PPC	Personal Information Protection Commission (Japanische Datenschutzbehörde)
TOM	Technische und organisatorische Maßnahmen
USD	US-Dollar (Währung)

Literaturverzeichnis

1 The Verge; Nick Statt; "Amazon is expanding its cashierless Go model into a full-blown grocery store"; 2020-02-25
2 Intel Newsroom; Kathy Winter; "For Self-Driving Cars, There's Big Meaning Behind One Big Number: 4 Terabytes"; 2017-04-14
3 The Guardian; Evan Selinger & Albert Fox Cahn; "Did you protest recently? Your face might be in a database"; 2020-07-17
4 Forbes; Larry Magid; "IBM, Microsoft And Amazon Not Letting Police Use Their Facial Recognition Technology"; 2020-06-12
5 The Economist; "The EU guarantees its citizens' data rights, in theory"; 2018-04-05
6 PWC; "Top Policy Trends 2020: Data privacy"; 2020-03-30
7 Politico; Mark Scott & Laurens Cerulus; "Europe's new data protection rules export privacy standards worldwide"; 2018-06-02
8 DLA Piper; "DLA Piper GDPR Data Breach Survey 2020"; 2020-01-20
9 CNBC; Ryan Browne; "Europe's privacy overhaul has led to $126 million in fines — but regulators are just getting started"; 2020-01-19
10 CNN; Rose Roobeek & Rob Picheta; "Grandmother must delete Facebook pictures posted online without permission, court rules"; 2020-05-22
11 Capgemini Research Institute; "Championing Data Protection and Privacy"; 2019-10-14
12 Skadden, Arps, Slate, Meagher & Flom LLP and Affiliates; "California Consumer Privacy Act: A Compliance Guide"; 2019-03-20
13 The Verge; Kim Lyons; "No one is ready for California's new consumer privacy law"; 2019-12-31
14 Future of Privacy Forum; Marianne Varkiani; "Comparing Privacy Laws: GDPR v. CCPA"; 2019-12-18
15 Future of Privacy Forum; Pollyanna Sanderson; "It's Raining Privacy Bills: An Overview of the Washington State Privacy Act and other Introduced Bills"; 2020-01-13
16 The Guardian; Veena Dubal; "San Francisco was right to ban facial recognition. Surveillance is a real danger"; 2019-05-30
17 Clarip; "What is a CCPA business purpose or commercial purpose?"; 2018
18 Ernst & Young LLP; "The California Consumer Privacy Act: Overview and Comparison to the EU GDPR"; 2018
19 KPMG; "The new imperative for corporate data privacy"; 2019-07-29
20 The Law Reviews; Hongquan (Samuel) Yang; "The Privacy, Data Protection and Cybersecurity Law Review – Edition 6 CHINA"; 2019-10-23
21 DLA Piper Blog; "China: Important clarifications and changes to china's data privacy standards"; 2020-03-24
22 XinhuaNet; "Data security legislation significant to national security: expert"; 2019-04-15
23 CMS Legal Services EEIG; Nick Beckett; "China publishes new specification on personal data security"; 2020-03-11
24 South China Morning Post; Celia Chen; "China punishes 100 apps for breaches of personal information as consumer anxiety rises over privacy"; 2019-12-09
25 China Daily; "The head of the Cyber Security Coordination Bureau of the State Internet Information Office answers questions"; 2017-05-31
26 The Guardian; Michael Standaert; "China wildlife park sued for forcing visitors to submit to facial recognition scan"; 2019-11-04
27 The Japan Times; Jonathan Soble; "How COVID-19 has shown us that society needs resetting"; 2020-06-29
28 Baker McKenzie; Kensaku Takase & Daisuke Tatsuno; "Japan enacts amendments to the Act on the Protection of Personal Information"; 2020-07-06
29 One Trust; Daniel Hounslow & Ryuichi Nozaki; "Japan – Data Protection Overview"; 2020-07-29
30 Deloitte; "Unity in Diversity"; 2019-07-12
31 Japan Times; ‚Panel warns over 30 firms that got Japan job-seeker data from scandal-hit Recruit Career"; 2019-12-05
32 Japan Times; Akky Akimoto; "Google Glass may shatter Japan's 'manner' mode"; 2013-05-15
33 IAPP; Alex Wall; "GDPR matchup: South Korea's Personal Information Protection Act"; 2018-01-18
34 Brussels Privacy Hub; Haksoo Ko & John Leitner & Eunsoo Kim & Jong-Gu Jung; "Structure and enforcement of data privacy law in South Korea"; 2016-10
35 Lee&Ko Legal; "Major Amendment to the Personal Information Protection Act Passed by National Assembly"; 2020-01
36 Korean LII; "Personal Information Protection Act"; 2020-05-14
37 Hunton Andrews Kurth LLP; "South Korean Court Imposes Personal Liability on Privacy Officer for Data Breach"; 2020-01-09
38 Ipsos; "Global public opinion on government use of AI and facial recognition"; 2019-09-11
39 Morrison & Foerster LLP; "Clarity at Last? We Will Soon Know When the Brazilian LGPD Comes into Effect"; 2020-07-06
40 Leader League; "Interview with Fabricio Lira (Head of Data and Artificial Intelligence – IBM Brasil)"; 2020-06-19
41 PK Advogados; "Main Points of the Brazilian General Data Protection Law – LGPD"; 2019-05-07
42 IAPP; Renato Leite Monteiro; "The new Brazilian General Data Protection Law — a detailed analysis"; 2018-04-15
43 Amnesty International; "New poll reveals 7 in 10 people want governments to regulate Big Tech over personal data fears"; 2019-12-04
44 Wired; Alex Lee; "The European Court of Justice has ruled that Privacy Shield is invalid"; 2020-07-16
45 Financial Times; Song Jung-a & Kang Buseong & Edward White; "A warning from South Korea: the 'fantasy' of returning to normal life"; 2020-06-20
46 Washington Post; Geoffrey A. Fowler; "Black Lives Matter could change facial recognition forever — if Big Tech doesn't stand in the way"; 2020-06-12
47 Forbes; Zak Doffman; "Hong Kong Exposes Both Sides Of China's Relentless Facial Recognition Machine"; 2019-08-26
48 The Atlantic; Adrienne Lafrance; "Who Owns Your Face?"; 2017-03-24

brīghter AI



brighter AI

brighter AI entwickelt Anonymisierungslösungen für Bilder und Videos, die mit Analytik und KI kompatibel sind. Das Berliner Unternehmen verfolgt die Mission, jede Identität in der Öffentlichkeit zu schützen.

Weitere Informationen unter www.brighter.ai

KI Bundesverband

Der KI Bundesverband vertritt die Interessen von KI-Unternehmern gegenüber Politik, Wirtschaft und Medien, um ein aktives, erfolgreiches und nachhaltiges Ökosystem in Deutschland & Europa aufzubauen.

Weitere Informationen unter www.ki-verband.de

© 2020 brighter AI