brighter AI

Privacy regulations on video data collection worldwide

Understanding the rules and best practices of major regulations in times of processing data for AI and analytics

In cooperation with

KI BUNDESVERBAND

With insights from executives and data privacy experts worldwide, including:

Capgemini · EVOTEGRA · iapp · IBM · IEF · intel · LiangDao · pwc · samasource · SIGNATRIX

Usage of this report

This report is general and educational in nature and is not intended to provide, and should not be relied on, as a source of legal advice. The information and materials provided in the report may not be applicable in all (or any) situations and should not be acted upon without specific legal advice based on particular circumstances. brighter AI cannot be hold accountable for the content's correctness and completeness.

Contents

Introduction

There is no doubt that the ongoing revolution in analytics and artificial intelligence requires enormous amounts of data. In industries from healthcare and retail to automotive and public transport, image and video analytics is one of the key techniques to fuel new digital solutions. Smart stores will be filled with numerous cameras[1] and autonomous vehicles will generate and process Zettabytes of visual data[2].

Meanwhile, events such as the use of facial recognition during Black Lives Matter protests in 2020[3], have raised increasing concerns associated with recording and processing publicly-recorded images. Following a strong backlash from society, companies like IBM, Microsoft and Amazon stopped selling the software to government authorities[4]. While the importance of data privacy for social responsibility increases, regulators worldwide are updating laws to establish clearly defined rules for the digital revolution. For companies, it is important to keep up with the dynamic environment to minimize regulatory risks and to develop future-proof solutions that are trusted by consumers.

In this report, we collect relevant information on privacy laws and best practices to consider when engaging in analytics and artificial intelligence. Building upon experience from data projects all over the world, we summarize key aspects about data protection laws of six regions: the European Union, the United States, China, Japan, South Korea and Brazil. Furthermore, we highlight insights from industry leaders and privacy experts. There exists some skepticism about the impact of regulation on progress in AI and analytics. However, companies increasingly find value in complying and developing responsible, data-driven innovations – as this is not only appreciated by regulators, but also by consumers.

"Four terabytes is the estimated amount of data that an autonomous car will generate in about an hour and a half of driving – or the amount of time a typical person spends in their car each day." [2]

Kathy Winter
Vice President Automated Driving Solutions, Intel

"Data protection and cyber security regulations are the (de)accelerator for realizing autonomous driving and smart city solutions. They must be kept up to date with the digital revolution."

Dr. Yang Ji
CEO, LiangDao GmbH

Overview

Criteria	EU **GDPR**	US **CCPA**	China **CSL & PIS**	Japan **APPI**	South Korea **PIPA**	Brazil **LGPD**
Applicability (entities)	All private and public entities	Companies with • USD 25M+ revenues • Data of 50,000+ consumers • 50%+ of revenue by selling data	All types of organizations and individuals	All business operators handling personal information	Any entity that manages personal information directly or indirectly	All entities and public authorities
Territorial scope	Entities established in EU or offering goods & services to or monitoring the behavior of persons in the EU	Entities doing business in the state of California	*Not specified*, CSL even applies to overseas entities whose activities could risk CII (Art. 75)	Entities established or located in Japan, and providing goods or services to individuals located in Japan	Entities established or located in South Korea, and those processing personal data there	Any entity that processes personal data in Brazil / collected in Brazil, or that supplies goods & services in Brazil
Rights of individuals	• Information • Objection / consent denial • Data erasure • Data access • Rectification • Data portability • Restriction of processing	• Information • Objection (opt-out) and data erasure • Data access • Data portability • No discrimination for exercising rights	• Be informed of rights prior to collection / use of personal data • Request removal or correction of personal data	• Be informed of rights prior to collection / use of personal data • Request deletion or correction • Filing utilization cease request or complaint to PPC	• Be informed of rights and usage of personal data • Request access, correction and deletion of personal data	• Information • Consent denial • Data access • Data correction • Anonymization or erasure of unnecessary or excessive data • Data portability
Data protection officer	DPO required, if: • public authority • large-scale monitoring of individuals • processing special data categories	*Not specified*	PIS requires a person in charge of personal information protection	*Not specified*	Every data handler must install designated DPO	Any organization that processes data will need to have a DPO
Risk/impact assessment	Data Protection Impact Assessment (DPIA) required when project might involve "high risk" to individuals' personal data	Privacy risk assessments are recommended	Security assessment must be conducted if data needs to be transferred outside China	*Not specified*	DPIA required for public agencies in case of data breach (this does not apply to private sector companies)	No specification about when a DPIA is required, but the ANPD can request the controller to perform and provide it
Fines	Up to EUR 20M or 4% of annual global turnover	Up to USD 7,500 per (intentional) violation, plus compensation up to USD 750 per consumer	Up to CNY 1M (EUR 130,000), plus 1–10 times the amount of unlawful gains, plus civil fines for responsible personnel	Up to JPY 500,000 (EUR 4,000) and up to one year's imprisonment	Fines up to KRW 50M (EUR 35,000), plus up to 5 years prison for responsible personnel	Up to BRL 50M (EUR 11.5M), or up to 2% of revenues

European Union General Data Protection Regulation

Applicable since

25.05.2018

Supervising authority

Independent Data Protection Authority announced in each member state to provide guidance and handle complaints. The European Data Protection Board ensures consistent application of the GDPR and promotes cooperation among the data protection authorities.

Widely viewed as the global gold standard of privacy laws, GDPR is arguably the most comprehensive and strictest law of its kind.[5] With hefty potential fines of up to €20M or 4% of annual global revenues, its impact on organizations can be severe and since its inception, privacy protection has become a priority on corporate agendas.[6]

While some European companies feel a competitive disadvantage, the regulation applies to all companies operating in any of its member states and worldwide adoption of its principles is evident.[7] Even the controversial ruling of the European Court of Justice making "Privacy Shield", the agreement on data exchange between EU and US, illegal, might eventually speed up international convergence.

"The first years of GDPR were marked by burdensome constraints and terrible user experiences. However, the legislation marks the first time a political system has enforced its fundamental values well beyond its own tech ecosystem, driving user trust and adoption – adherence is already becoming a global competitive advantage."

Clark Parsons
Managing Director, Internet Economy Foundation
Partner, iconomy

Key principles:

Data Minimization Most fundamentally, "personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" (Art. 5, GDPR). Bases for lawful processing can be consent, a contract with the data subject, legal obligations, protection of vital interests of the data subject, public interests and legitimate interest of the data controller (Art. 6, GDPR).

Consent Requirement Consent of the data subject is the most common basis for lawful processing. This consent needs to be "freely given, specific, informed and unambiguous" (Art. 7 & Recital 32, GDPR).

Impact Assessment When processing might result in risks to rights of natural persons, i.e. "using new technologies" such as video analytics or machine learning, data controllers should perform a Data Protection Impact Assessment (DPIA) in order to identify and mitigate potential risks for data subjects (Art. 35, GDPR). When conducting the DPIA, controllers must seek advice of a Data Protection Officer (DPO), who is required for large data-driven companies.

Privacy By Default & By Design Not new as a data privacy concept, with GDPR these are now legal requirements. "By default" means that strictest privacy settings should be the standard and "by design" describes that state-of-the-art technical and organizational measures (TOMs) need to be in place to safeguard data protection. Here, the regulator explicitly recommends to implement privacy-enhancing technologies such as pseudonymization (Art. 25, GDPR).

Processing For Scientific Research Purposes Where personal data are processed for scientific research purposes, i.e. for technological development and demonstration, GDPR should apply to that processing (Recital 159). As Art. 89 further states, processing for these purposes is subject to appropriate safeguards for the rights and freedoms of the data subject.

Enforcement

Until end of January 2020, European data protection authorities have imposed fines of €114 million for GDPR violations.[8]

"It is going to be a slow progress to get the legal certainty regulators need to start whacking companies with higher fines." [9]

Ross McKean
Partner, DLA Piper

Facts & Figures

A member survey by the KI Bundesverband (German AI Association) shows that 75% of polled companies do not experience any disadvantages by GDPR and 16% explicitly benefit from it.

California, U.S.
California Consumer Privacy Act

Applicable since

01.01.2020

Supervising authority

The Attorney General with the power to independently start investigations and actions on alleged CCPA violations.

Only introduced this year, CCPA is now the most comprehensive privacy law in the United States and the first to give consumers actual control over how their personal information is used, especially online.[10] Similar to GDPR, its impact is expected to be global, given California's status as the fifth largest economy worldwide (if it was a nation).

While the general purpose of CCPA is clear, some unclear definitions and contradictions with industry-specific regulations are bringing forth numerous debates.[10] Also, there is increasing demand for a country-wide law as other states start introducing privacy bills. [11]

A surprise to many, California is America's frontrunner in data privacy. Recently, the city of San Francisco was the first to ban use of facial recognition technology.[12]

"It's important not to assume that CCPA is 'GDPR Lite' because there are some distinctions that could result in non-compliance. Understanding the difference between the two will allow you to put the controls in place to ensure compliance to both."

Cindy Abramson
Vice President Customer Trust, Samasource

Key principles:

Notice Requirement Before, or at the point of the data collection, businesses are required to communicate the categories of personal information to be collected, the purpose of collection and the consumer's rights. Information should be openly accessible, e.g. on a company's website, and needs to be updated at least annually (1798.100).

"Opt-Out" CCPA does not require explicit consent or registration before collecting, selling or sharing personal information. However, consumers have the option to opt out of recordings – something that is particularly difficult to realize in publicly-recorded videos.

Purpose Limitation Businesses may collect, use or share personal information for business or commercial purpose. While business purpose refers to operational activities including auditing, security, maintenance or R&D, commercial purpose is defined to "advance a person's commercial or economic interest" (1798.140). Due to broad definitions and possibility of dual purposes, a clear distinction is not always possible.[13]

Data Minimization Personal data should be "reasonably necessary and proportionate to achieve the operational purpose" for which it was collected (1798.140).

Data Transfer Cross-border transfer is not restricted by CCPA. Date transfer to third parties and service providers require a written agreement containing certain provisions.[14]

Anonymization & Pseudonymization The CCPA does not apply to de-identified or aggregated information. It is not specified whether the same rules apply to data that has been pseudonymized.[15]

"Consumer protections around data privacy [...] are very likely to be codified in other states and eventually at the federal level. [...] privacy laws are only going to increase in volume and rigor." [15]

Steve Stein, Principal, KPMG Cyber Security Services

Enforcement

CCPA's 6 months grace period finished on July 1st – to this day, there have been no enforcements.[16] However, there are ongoing lawsuits against e.g. Clearview AI, TikTok, Zoom and Walmart.

"If you thought the GDPR was bumpy, the CCPA is going to be a real roller coaster. This is a complex set of new rules, which are still a work in progress." [16]

Reece Hirsch
Partner, Morgan Lewis

Facts & Figures

In a recent survey from KPMG with US consumers, 97% of respondents say data privacy is important to them and 42% consider facial recognition login as a privacy risk.[15]

China

Cybersecurity Law & Personal Information Security Specification

Applicable since

CSL: 01.06.2017
Updated PIS: 01.10.2020

Supervising authority

The Cyberspace Administration of China (CAC), Ministry of Public Security (MPS), Minister of Industry and Information Technology (MIIT)

Despite its focus on lightspeed innovation, data protection is also growing in importance in China, highlighted by first lawsuits for unlawful processing of personal data. In general, China's regulatory landscape around data privacy protection is complex. Companies engaging in video data collection need to work with local partners and should furthermore get dedicated legal advice to avoid potential pitfalls.

The Cybersecurity Law (CSL) is China's legal framework for cybersecurity and data protection that covers personal information protection. It is a high-level law and does not provide practical guidelines.[17] These can be found in the Personal Information Security Specification (PIS), a set of China's de facto data privacy regulations.[17] It provides detailed requirements on the collection and processing of personal information. These two constitute China's legal regime for cybersecurity and data protection.

"In a digitalized society, data security is the guarantee for other forms of security. Without data security, all the products and services based on information technology will lose safety support." [18]

Mo Jihong
Law Professor, Chinese Academy of Social Sciences

Key principles:

Consent Requirement If a product or service collects personal information, the provider shall clearly indicate this, obtain consent from the user (CSL, Art. 22). This means, the data subject needs to receive relevant information including purpose, method, scope and rules of processing (CSL, Art. 41).

Purpose Limitation Processing personal data is legal if justified, necessary, and for a specific purposes (PIS, Art. 4). The controller further needs to bear responsibility for damage to the lawful rights and interests of the PI subject caused by processing of personal information.[17]

Minimization Principle Only the minimum types and quantity of personal information necessary for the purposes for which the consent is obtained from the data subject should be processed – unless explicitly agreed by the data subject (PIS, Art. 4). After the purpose is achieved, the data should be deleted promptly (PIS, Art. 4).

Cross-border Transfer Personal information generated and collected in China must be stored within (mainland) China. Cross-border transfer underlies specific rules: the data controller should conduct a security assessment and comply with requirements in measures and relevant standards issued by the relevant offices (PIS, Art. 8).

Personal Biometric Information This includes facial recognition features, which is the most common feature in publicly recorded video data, and the data subject must be informed about collection and provide specific consent. Personal biometric data must be stored separately from personal identification data.[19]

Anonymization & Pseudonymization Anonymized data is not considered personal data, and consequently is not subject to privacy regulations (PIS Art. 3). Also, pseudonymization will reduce any risk of non-compliance.[20]

Enforcement

In 2019, the China Cybersecurity Center has penalized 683 apps across industries from e-commerce to banking.[21]

"The promulgation and implementation of the Cyber Security Law not only legally protects the interests the masses in cyberspace, and effectively safeguards national sovereignty and security in cyberspace, but it is also conducive to the application of information technology and the great potential of the Internet". [22]

Zhuang Rongwen
Head of Cyber Security Coordination Bureau

Facts & Figures

In July 2019, Hangzhou safari park introduced facial recognition for annual pass holders and invalidated those whose holders did not register their biometric information by October that year. The park was sued for this action.[23]

Japan

Act on the Protection of Personal Information

Applicable since

New amendment: 30.05.2017

Supervising authority

The Personal Information Protection Commission (PPC) has the right to perform audits and issue cease and desist orders but cannot impose administrative fines.

Originally established in 2003, APPI was the first comprehensive data protection regulation in Asia. The new amendment in 2017 brought the establishment of the Personal Information Protection Commission (PPC), an independent agency that protects the rights and interests of individuals while taking into consideration proper and effective use of personal information.

In 2019, the EU Commission adopted its adequacy decision in respect of Japan, making it the first formal recognition of bilateral and reciprocal adequacy with a non-EU country.

"When Japan created its rules to protect personal information, it took bits and pieces from other countries' laws (...). A balanced approach is healthy — we need to protect privacy but also leave room for innovation." [24]

Jonathan Soble
Communication Lead, World Economic Forum

Key principles:

Publication Of Purpose A business operator handling personally identifiable (PII) information shall publish the purpose of the personal data's utilization before or after acquiring it (Art. 18). The data subject can thus either give consent prior or opt-out subsequently. APPI defines biometric data, which usually is collected in visual data, explicitly as being part of PII.

Data Minimization Personal information shall not be handled beyond the scope necessary for the achievement of the purpose of utilization (Art. 16). The personal information must not be acquired by deception or other wrongful means (Art. 17).

Cross-border Transfer Prior consent of data subject is required unless the foreign country is a country with adequate standards for privacy protection (Art. 24), e.g. the EU.

Anonymization & Pseudonymization Processing of pseudonymized information relieves from the obligation to comply with certain requirements under the APPI, such as demands for disclosure or erasure. Anonymized information can be used beyond the original purpose and can be disclosed to third parties without consent.[24]

Reporting To The PPC Under new 2020 amendments, reporting to the PPC will become mandatory. However, the obligation will be limited to certain breaches only, which involve a substantial risk to individuals' rights and interests.[24]

"Businesses are required to more strictly manage personal information, as their increasingly globalized operations result in more frequent transmission of such data between (Japan and) overseas." [25]

Harumichi Yuasa
Professor, Institute of Information Security Yokohama

Enforcement

PPC concluded that companies, including Mitsubishi Corp., Mitsubishi Electric Corp. and Toyota Motor Corp., managed personal information inappropriately.[26] No penalties have been imposed so far.

Facts & Figures

Phone manufacturers and carriers have voluntarily cooperated to implement a camera shutter sound to prevent "privacy issues", even though it is not required by law. [27]

South Korea
Personal Information Protection Act

Applicable since

New amendment: 01.07.2020

Supervising authority

The Personal Information Protection Commission (PIPC) consults and resolves personal data-related policies while the Ministry of the Interior and Safety (MOIS) is responsible for investigation and enforcement.

Originally established in 2011, South Korea's Personal Information Protection Act (PIPA) is one of the world's strictest privacy regulations.[28] Like the GDPR, it protects privacy rights from the perspective of the data subject, and it is comprehensive, applying to most organizations, even government entities.[28]

The law aims at enhancing the right and interest of individuals and further realizing the dignity and value of the individuals (Art. 1). In early 2020, the Korean National Assembly passed amendments to its data privacy laws to streamline regulatory supervision and supposedly to reach adequacy decisions from the EU Commission to facilitate data flows.

"Issues on data privacy have gained notable traction in recent years in South Korea and, perhaps reflecting this phenomenon, relevant laws and regulations have been amended frequently."[29]

Haksoo Ko
Professor, Seoul National University School of Law

Key principles:

Personal Information Protection Principles Personal information needs to be collected for specific and lawful purposes and not used for further incompatible purposes. Further, PI needs to be accurate and held securely and collectors are quired to publicize their privacy policy and to make personal information anonymous wherever possible (Art. 3).

Consent And Choice The data subject has the right to consent to or reject processing of personal information, to be informed of it as well as to elect the scope of consent, to confirm processing, to access, correct and delete the personal information (Art. 4). However, no consent is needed within a scope that is "reasonably related" to the original purpose of collection (Art. 15).

Pseudonymization & Anonymization: Anonymized information is considered as non-personal information and thus not subject to the PIPA (Art. 58). Pseudonymized data can be processed without the consent of the data subject for various purposes, including "commercial purposes such as the development of data-based, innovative technology, products, and services".[30]

Specifications On Visual Data "Visual data processing devices" are defined as devices that are installed permanently to take pictures of persons and/or things and/or to transmit them (Art. 2). In public places, they can be installed only for the purpose of prevention of crime and fire, or if related to traffic (control) information (Art. 25). Here, visible notice about a) the purpose of installation and location, b) the range of its operation and duration, c) info (name and contact) of company or person in charge is required. PIPA explicitly states that visual data processing devices shall not be handled for other purposes than the initial one (Art. 25)

Enforcement

Kim Jin-Hwan, DPO of Hana Tour Service Inc, was found guilty of violating PIPA and imposed a penalty of KRW 10 M (EUR 7,000) against him and additional fines of KRW 327.25 M (EUR 232,750) against the company.[31]

Facts & Figures

A survey by Ipsos showed that only 9% of South Koreans agree that the use of AI and facial recognition by the government's "should not be allowed under any circumstances in order to fully guarantee everyone's privacy at all times", compared to 19% in Japan, 18% in China and 16% on a global average.[32]

Brazil
General Data Protection Act

Applicable from

16.08.2020
(enforcement will be delayed due to COVID-19)

Supervising authority

The National Data Protection Authority (ANPD) will have the authority to issue regulations and procedures related to personal data protection and supervise and issue sanctions for violations.

The General Data Protection Act (in Portugese "Lei Geral de Proteção de Dados", LGPD) shall bring clarification to the Brazilian legal framework related to personal data by replacing some and supplementing others of the 40+ existing federal regulations. It shall regulate the treatment of personal data of all individuals in Brazil and forms the country's first comprehensive data protection regulation.

LGPD was planned to take effect in February 2020 but the entry into force was pushed back to August 2020. When COVID-19 hit the country, Senate tried to delay its implementation until May 2021 and sanctions until August 2021. To date, there is no decision.[33]

"We see LGPD as an opportunity for the sustainable development of the country whilst ensuring that fundamental rights and data-driven innovation may coexist in an environment of transparency and trust." [34]

Fabricio Lira
Head of Data and Artificial Intelligence, IBM Brasil

Key principles:

Requirements For Processing Personal Data LGPD states ten legal bases, including consent, but also "for the protection of credit, including as provided in the pertinent legislation" (Ch. 1, Art. 7). LGPD is thus the first and to date only privacy law to contain a specification to empower financial institutions to use data for credit evaluations. Moreover, biometric data, i.e. depiction of faces in camera recordings, is declared sensitive personal data and here, consent of the data subject shall be the legal basis for its collection and processing (Art. 11).

General Principles For Data Processing Need for data minimization, accuracy, storage limitation, security, lawfulness, fairness, accountability, purpose limitation and transparency on the use of personal data.[35] Further, the LGPD explicitly forbids processing personal data for discriminatory purposes.[36]

Privacy By Design & By Default The law defines the adoption of practices guaranteeing privacy and data protection rights as mandatory in the design of services, products and business models. Also, privacy controls, especially online, should be the most protective by default and the data subjects should be able to "opt-in".[36]

Pseudonymization & Anonymization LGPD states that personal data should be pseudonymized or even anonymized whenever possible (Ch. 2, Art. 7). Anonymized data is not considered personal data and thus specifically excluded from LGPD's application, except when the process of anonymization has been or can be reversed (Ch. 2, Art. 12)

Enforcement

LGPD is not enforced yet and sanctions will not be feasible before August 2021.

"For IBM, privacy is a matter within the context of trust and transparency before being an obligation to comply with local laws." [34]

Fabricio Lira
Head of Data and Artificial Intelligence, IBM Brasil

Facts & Figures

A survey by YouGov shows that almost 83% of Brazilians think governments should do more to regulate technology companies' control over people's lives online. [37]

Way forward

Looking into privacy regulations of different markets and how industry leaders approach them, it becomes apparent: In our globalized world, data collection and AI projects are increasingly borderless, while privacy laws are inherently not.

However, states are trying to harmonize privacy regulations, not only to facilitate data transfer for multinational companies, but also to give equal rights to all people. At the same, it is inevitable that constitutional, societal and economic differences lead to variations across the globe. Furthermore, the EU's recent ruling on "Privacy Shield" has shown that formerly adequate measures to align protection efforts between countries can be quickly overturned.[38] Thus, a global perspective on compliance will stay relevant.

Most privacy regulations are defining personally identifiable information rather broadly and miss specific guidelines on video data. But looking at recent developments, this year's mega topics have been significantly accompanied by discussions around "visual" data privacy: COVID-19 has accelerated growth in leveraging CCTV footage for video analytics[39] and protests in Hong Kong and the US sparked intense discussions about the use of facial recognition technologies and its dangers.[40,41]

Already in 2017, The Atlantic asked "Who owns your face?" [42] As such, it is evident that the protection of visual PII is not a new topic – but evolving as fast as the opposing technology itself. Currently, South Korea's PIPA is the only regulation in our report that is specific here, but only on visual data gathering devices that are installed permanently in one place. As our research shows, regulations are constantly being adjusted to new developments and thus, it seems likely that this changes in the future – given the rise of the public opinion that our face is one of the most sensitive personal identifiers that needs additional protection. The ban on facial recognition in San Francisco seems to be a starting point.

"There is still considerable work to do before we can begin to imagine a future where privacy laws are 'harmonized'. (...) Many countries in the Asia Pacific region have taken inspiration from the (...) GDPR, by either adopting, or planning to adopt, similar or more stringent regulations." [25]

Deloitte

"Your face is yours. It is a defining feature of your identity. But it's also just another datapoint waiting to be collected. At a time when cameras are ubiquitous (...), faces are increasingly up for grabs." [42]

Adrienne LaFrance
Executive Editor, The Atlantic

In summary, when it comes to the collection and processing of video data in public, companies are moving in a sensitive, volatile and fragmented regulatory environment. Laws and agreements are constantly updated and not yet aligned across the globe. While societal concerns increase, there is still significant acceptance when it comes to security and safety, as seen during the COVID-19 crisis. Additionally, the "Nothing to hide argument" (that even has its own Wikipedia article) continues to be common.

Accompanied by the regulatory and societal discourse, the tech industry's attitude of "speed over caution" is changing and more companies embrace concepts such as "privacy by design" in order to benefit from rightfully collected data and consumers' trust.

As a way forward, organizations that engage in analytics and artificial intelligence projects should consider: It is not all or nothing. Privacy regulations and innovation should be seen as an unsolvable dilemma, but as a chance. Data protection laws are not a "showstopper" for projects in computer vision and machine learning. (Also not desired by the law makers!) Based on the increasing public interest and potential sanctions, it is not advisable to turn a blind eye to it or look for loopholes. Instead, insights from leading companies show that it is possible to embrace privacy frameworks for the legitimate use of data to develop sustainable innovation in line with laws and social responsibility. This requires staying up to date, hiring specialized employees and constantly improving safety measures. When done properly, this fosters trust and minimizes reputational or monetary risks – without a negative impact on leveraging data-driven technologies.

"We work with computer vision and we take privacy very seriously. Our clients appreciate this added value to our product because it offers the perfect combination of security and innovation. In the end, it becomes a competitive advantage to treat privacy as an integral part of product design."

Christoph Schwerdtfeger
Head of AI and Co-Founder, Signatrix

"Organizations need to promote a data protection and privacy mindset among employees and integrate advanced technologies to boost data discovery, data management, data quality, cybersecurity, and information security efficiencies. Firms that take these actions proactively – and view data protection and privacy regulation as an opportunity – will secure a significant competitive advantage." [43]

Capgemini

"The members of the German AI Association are committed to ensure that artificial intelligence is used in the sense of European and democratic values. Of course, this also includes the protection of individuals when processing their personal data. We believe that AI-based innovations and data protection are not mutually exclusive."

Daniel Abbou
CEO, KI Bundesverband

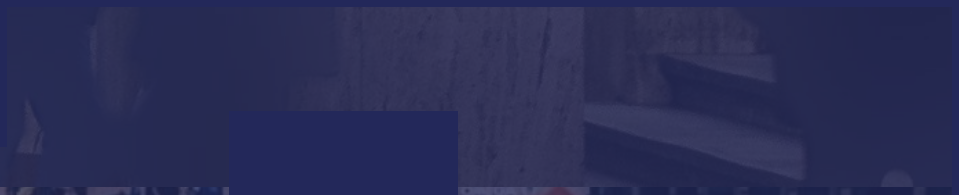
Abbreviations

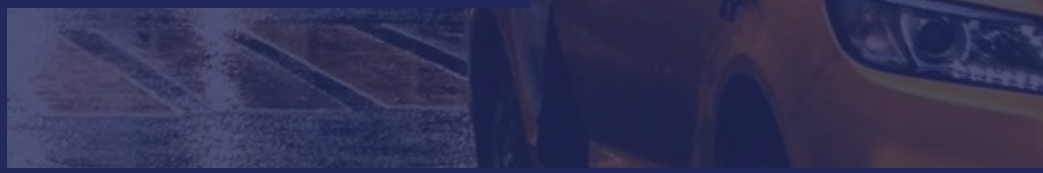
AI	Artificial Intelligence
ANPD	National Data Protection Authority
APPI	Act on the Protection of Personal Information
BRL	Brazilian Real (currency)
CAC	Cyberspace Administration of China
CCA	China Consumers Association
CCPA	California Consumer Privacy Act
CII	Critical Information Infrastructure
CSL	Cybersecurity Law
CNY	Chinese Yuan, Renminbi (currency)
DPIA	Data Protection Impact Assessment
DPO	Data Privacy Officer
EUR	Euros (currency)
GDPR	General Data Protection Regulation
IAPP	International Association of Privacy Professionals
JPY	Japanese Yen (currency)
KRW	South Korean won (currency)
LGPD	General Data Protection Act (in Portugese “Lei Geral de Proteção de Dados”)
MIIT	Minister of Industry and Information Technology
MOIS	Ministry of the Interior and Safety
MPS	Ministry of Public Security
PI	Personal Information
PII	Personally Identifiable Information
PIA	Privacy Impact Assessment
PIC	Personal Information Controller
PIPA	Personal Information Protection Act
PIS	Personal Information Security Specification
PPC / PIPC	Personal Information Protection Commission
R&D	Research and Development
TOM	Technical and Organizational Measures
USD	United States Dollar (currency)

References

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 Future of Privacy Forum; Marianne Varkiani; “Comparing Privacy Laws: GDPR v. CCPA”; 2019-12-18
11 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
12 The Guardian; Veena Dubal; “San Francisco was right to ban facial recognition. Surveillance is a real danger”; 2019-05-30
13 Clarip; “What is a CCPA business purpose or commercial purpose?”; 2018
14 Ernst & Young LLP; “The California Consumer Privacy Act: Overview and Comparison to the EU GDPR”; 2018
15 KPMG; “The new imperative for corporate data privacy”; 2019-07-29
16 The Verge; Kim Lyons; “No one is ready for California’s new consumer privacy law”; 2019-12-31
17 DLA Piper Blog; “China: Important clarifications and changes to china’s data privacy standards”; 2020-03-24
18 XinhuaNet; ”Data security legislation significant to national security: expert“; 2019-04-15
19 CMS Legal Services EEIG; Nick Beckett; “China publishes new specification on personal data security”; 2020-03-11
20 The Law Reviews; Hongquan (Samuel) Yang; “The Privacy, Data Protection and Cybersecurity Law Review – Edition 6 CHINA”; 2019-10-23
21 South China Morning Post; Celia Chen; “China punishes 100 apps for breaches of personal information as consumer anxiety rises over privacy”; 2019-12-09
22 China Daily; “The head of the Cyber Security Coordination Bureau of the State Internet Information Office answers questions”; 2017-05-31
23 The Guardian; Michael Standaert; “China wildlife park sued for forcing visitors to submit to facial recognition scan”; 2019-11-04
24 The Japan Times; Jonathan Soble; “How COVID-19 has shown us that society needs resetting”; 2020-06-29
25 Deloitte; “Unity in Diversity”; 2019-07-12
26 Japan Times; ‚Panel warns over 30 firms that got Japan job-seeker data from scandal-hit Recruit Career“; 2019-12-05
27 Japan Times; Akky Akimoto; “Google Glass may shatter Japan's 'manner' mode”; 2013-05-15
28 IAPP; Alex Wall; “GDPR matchup: South Korea's Personal Information Protection Act”; 2018-01-18
29 Brussels Privacy Hub; Haksoo Ko & John Leitner & Eunsoo Kim & Jong-Gu Jung; “Structure and enforcement of data privacy law in South Korea”; 2016-10
30 Lee&Ko Legal; “Major Amendment to the Personal Information Protection Act Passed by National Assembly”; 2020-01
31 Hunton Andrews Kurth LLP; “South Korean Court Imposes Personal Liability on Privacy Officer for Data Breach”; 2020-01-09
32 Ipsos; “Global public opinion on government use of AI and facial recognition”; 2019-09-11
33 Morrison & Foerster LLP; “Clarity at Last? We Will Soon Know When the Brazilian LGPD Comes into Effect”; 2020-07-06
33 Leader League; “Interview with Fabricio Lira (Head of Data and Artificial Intelligence – IBM Brasil)”; 2020-06-19
35 PK Advogados; “Main Points of the Brazilian General Data Protection Law – LGPD”; 2019-05-07
36 IAPP; Renato Leite Monteiro; “The new Brazilian General Data Protection Law — a detailed analysis”; 2018-04-15
37 Amnesty International; “New poll reveals 7 in 10 people want governments to regulate Big Tech over personal data fears”; 2019-12-04
38 Wired; Alex Lee; “The European Court of Justice has ruled that Privacy Shield is invalid”; 2020-07-16
39 Financial Times; Song Jung-a & Kang Buseong & Edward White; “A warning from South Korea: the ‘fantasy’ of returning to normal life”; 2020-06-20
40 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
41 Forbes; Zak Doffman; “Hong Kong Exposes Both Sides Of China's Relentless Facial Recognition Machine”; 2019-08-26
42 The Atlantic; Adrienne Lafrance; “Who Owns Your Face?”; 2017-03-24
43 Capgemini Research Institute; “Championing Data Protection and Privacy”; 2019-10-14

brīghter AI





About brighter AI

brighter AI provides leading image & video anonymization solutions that are compatible with analytics and machine use cases. The company's mission is to protect every identity in public.

For more information visit www.brighter.ai

About KI Bundesverband

The German AI Association represents AI entrepreneurs' interests towards politics, business and media to build an active, successful and sustainable AI ecosystem in Germany and Europe.

For more information visit www.ki-verband.de