Karlsgate

# Evolution of Personal Data Protection

## Guide to Implementing Zero-Trust Data Sharing

## Grow your business while honoring consumer privacy

Successful marketing requires a lot of data. Recognizing customers and serving their needs and preferences better than the competition is just smart business. In fact, consumers who experienced greater personalization were 110% more likely to buy items than planned and 40% more likely to spend more than planned, according to a recent study.[1]

For too long we've relied on sharing Personal Data, or Personally Identifiable Information (PII), across our network of marketing partners to improve performance. In doing so, we've lost sight of the fact that we're unnecessarily exposing customers to identity theft and loss of privacy.

That's not good for consumers nor brands. Consequently, consumer privacy advocates and regulators have stepped in to enforce consumer protections. There's a better way to comply with expanding consumer data privacy laws, honor consumers' right to privacy and improve marketing performance: Zero-trust data sharing.

**GDPR fines as of August 2020**

**343**
incidents

**€490**
million

## What defines Personal Data continues to evolve

Personal Data, what's referred to in the U.S. as PII, has changed dramatically as more Internet-connected devices are being used. It seems that everything we use, from smartwatches to smart home devices to cars, collect data about our every move. Beyond devices, profiling attributes based on various factors enable algorithms to pinpoint individuals with extraordinary fidelity.

### Regulators expand Personal Data definition

It's not surprising that regulators have taken an expansive view of Personal Data that goes beyond traditional PII, like name, address, email, etc., to include these indirect factors.

#### GDPR

"Personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[2]

#### CCPA

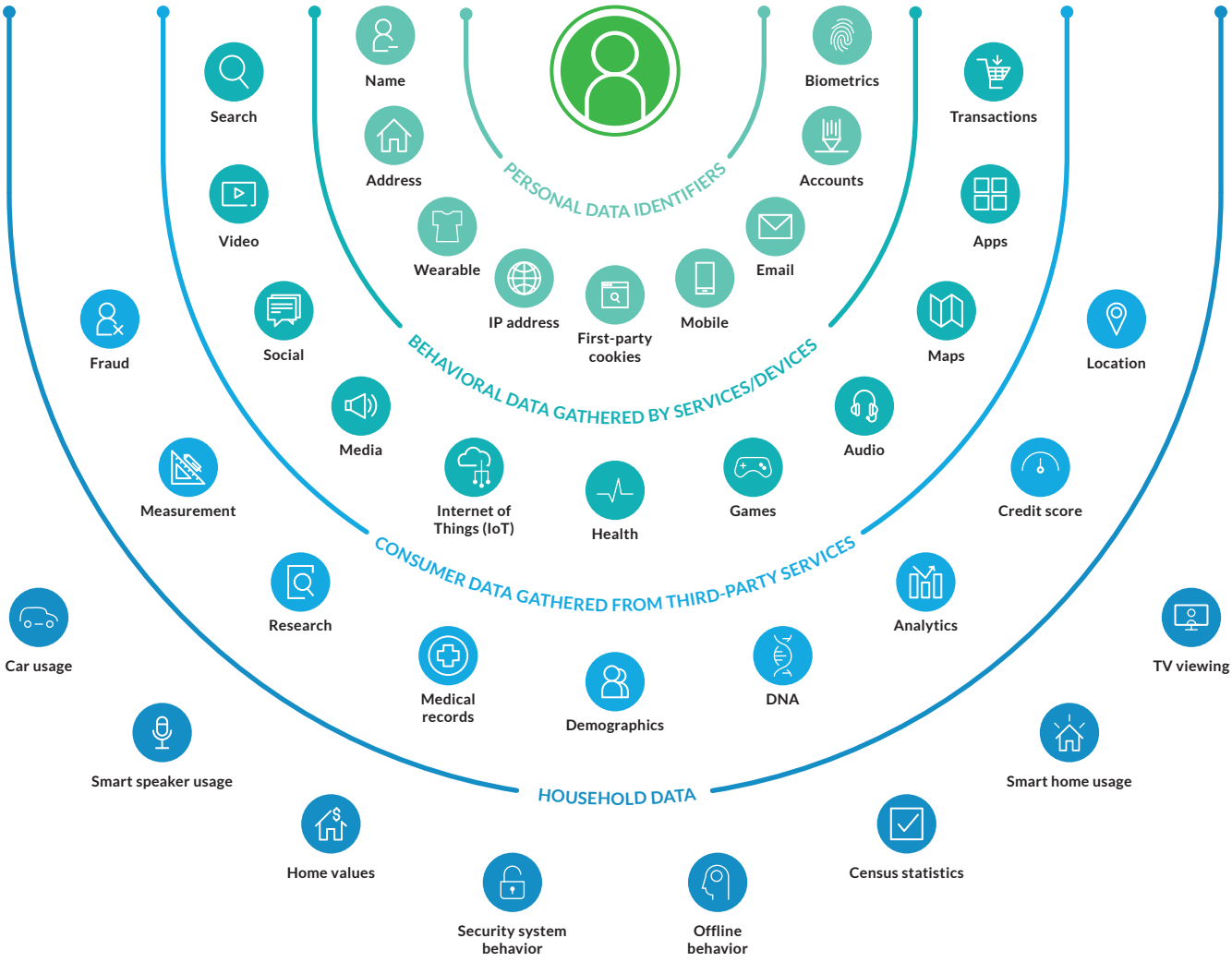
"Personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household.[3]

## All data is personal

Given the expansive definition of Personal Data, one has to ask: “Is all data personal?” For companies that participate in the consumer data economy, it’s hard to say no. Conservatively, there are three-times the number of behavioral data types than personal data identifiers. Completely anonymous data may be harder to produce or procure given how connected the world is today.

What we do know is that identifiers no longer solely define Personal Data, so businesses have to change the way they collect, process and share insights about consumers.

## The personal data universe



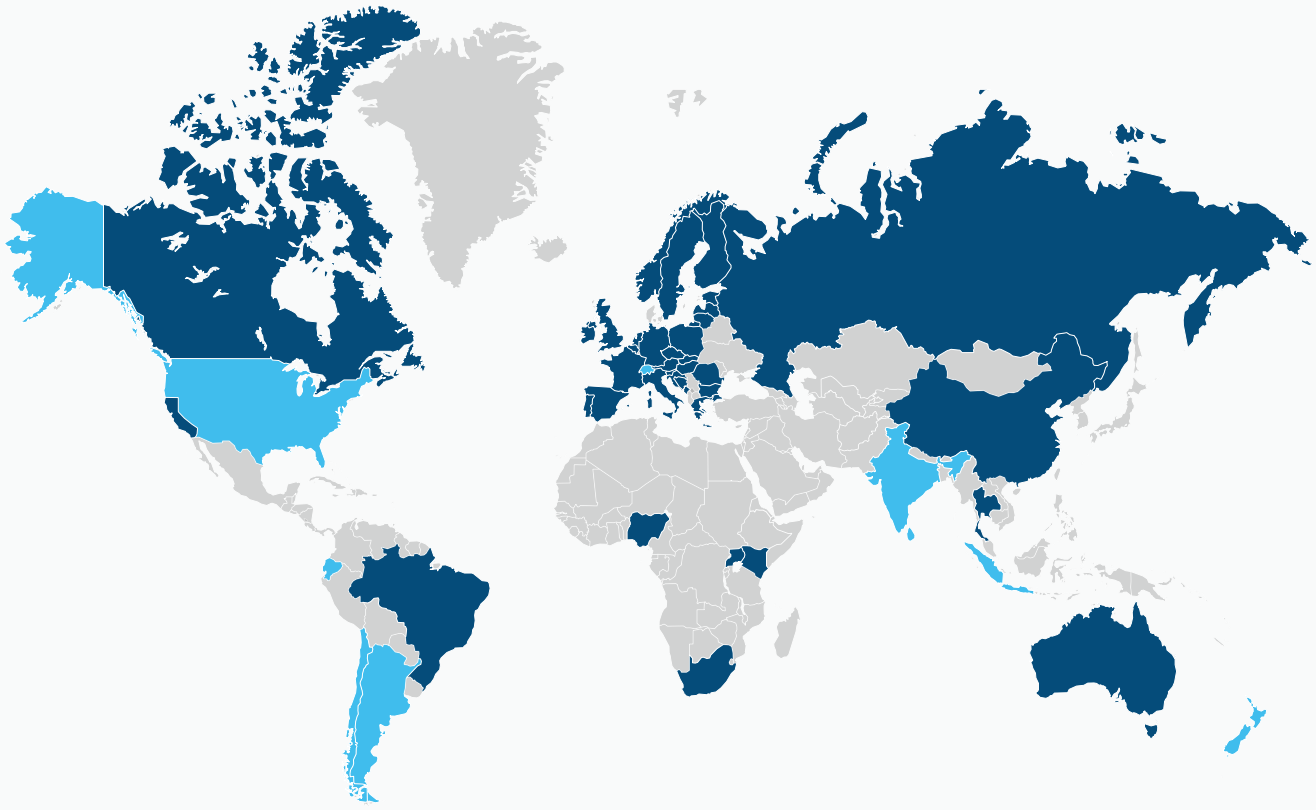
## Consumer Privacy regulation is a global reality

GDPR has been a reality for over a year now, and adoption of similar regulations is accelerating. The California Consumer Protection Act (CCPA) went into effect in 2020 and we'll see significant new privacy laws in some of the world's largest advertising markets like Brazil and India soon.

If GDPR is anything to go by, all are likely to have a significant impact on advertising. Marketers will have to grapple with further restrictions on their ability to access the data they rely on for their digital marketing campaigns – not only for targeting, but also for measurement.

### WFA global privacy map

An overview of data protection and privacy regulation, focused on key ad markets – not an exhaustive list of all legislative developments in all countries around the world.[4]



Regulation in place/due to come into force

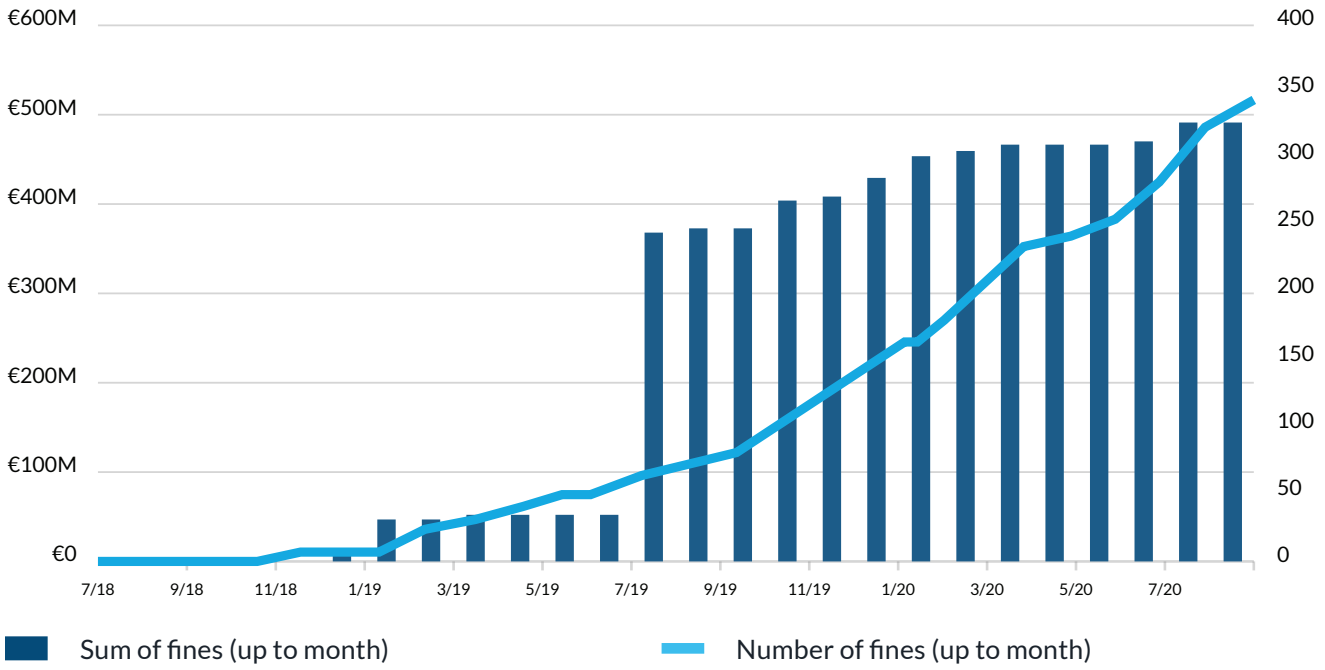
Regulation under discussion

## Non-compliance is having real financial consequences

Besides the risk to brand reputation and the cost of recovery from a data breach, companies are now facing regulatory fines for non-compliance with GDPR and CCPA personal data protections.

### GDPR fines

GDPR fines are administered by the data protection regulator in each EU country. The administrative fine structure has two tiers. Less severe non-compliance fines are up to €10 million or 2% of a company's annual revenue. More serious cases have fines up to €20 million or 4% of annual revenues. To date, cumulative fines levied for GDPR non-compliance have reached more than €400 million.[5]




### CCPA Fines

California's CCPA went into effect on January 1, 2020 and enforcement by the California Attorney General (AG) started on July 1, 2020.

The California AG will enforce the CCPA and has the power to issue non-compliance fines. The CCPA also provides a private right of action which is limited to data breaches. Under the private right of action, damages can come in between $100 and $750 per incident per consumer. The California AG may enforce the CCPA in its entirety with the ability to levy a civil penalty of not more than $2,500 per violation or $7,500 per intentional violation.

### The ROI of Regulatory Compliance

Now that regulators have started to levy fines for non-compliance, data privacy and security teams have a basis for judging investments in data protection. While internal policies and procedures must be updated to protect data internally, companies need to move quickly to implement better practices for protecting data that is shared with partners.

## Zero-trust: Ushering in the Protected Data Age

The Protected Data Age represents a new data sharing paradigm – one where the protection of information is not derived from the assurances of trading partners but is inherent in the manner of sharing the data itself.

The goal should be a Zero-trust approach where data privacy and security are built into the data sharing process. Three basic data sharing strategies will help organizations succeed.

START

### Implement Zero-trust data sharing

Work with a technology partner who has privacy-by-design data integration that protects you, your customers and your data partners. The partner should have the ability to match data sets without ever exposing or sharing Personal Data to themselves, you or your partner. **The partner should support the following capabilities:**

| NEUTRAL FACILITATION | DIFFERENTIAL PRIVACY | PSEUDONYMIZATION | ANONYMIZATION |
|---|---|---|---|
| Data partners don't share encryption logic | Random secret provided by each transaction participant | Some or all of ID replaced with pseudonym | One-time ephemeral matching key |

STOP

### Match files with discoverable IDs

You can't control how Personal Data is used once you lose custody. This is the biggest issue we face in the data ecosystem. Using secure FTP and APIs don't address the fact that you're still sharing discoverable IDs. The problem is that clear text transfers, hashed/pseudonymized identifiers and clean rooms are all susceptible to re-identification, retention and persistence. **Ask your partners for Zero-trust data sharing:**

| NO | NO | NO |
|---|---|---|
| transfer of identity data custody | disclosure, retention or persistency of identities | possibility of re-identification |

CONTINUE

### Seek consumer insights from their best source

Companies should revisit their data acquisition strategies to seek partnerships that can provide more relevant, timely and accurate consumer insight data. Leveraging a Zero-trust data sharing approach frees companies from the risks that comes with traditional data sharing. **Once you've embraced the Protected Data Age, you can look for data in unexpected places:**

| CHANNEL PARTNERS | TECHNOLOGY PARTNERS | DATA PARTNERS | AFFILIATE PARTNERS |
|---|---|---|---|
| No longer need to be protective of customer data | No risk of exposing your customers | No risk of re-identification | No risk of retention or persistency |

## A partner for the Protected Data Age

Karlsgate solves the biggest issues with sharing insights about people. Karlsgate Identity Exchange™ eliminates the need to use unprotected personal identifiers to conduct commerce. This reduces many of the risks that negatively affect personal privacy rights protection without inhibiting the use cases for data sharing.

Karlsgate Identity Exchange is a privacy-by-design data sharing platform that eliminates transferring or disclosing any Personal Data. Using patent-pending Cryptoidentity™ to map identities, it eliminates the need for trust in data sharing partnerships.

**No Capacity for Identity Discovery**
Matching is 100% deterministic preventing acquisition of data on individuals not previously present in a participant's data set.

**No Personal Revelation**
Triple-blind matching logic creates an undecipherable key for all transactions in which the input function cannot be deduced from the output.

**No Residual Constancy**
Single-use, random values mixed into the identifier ensures that no single participant can derive a stable or predictable output from the hashed values.

**No Identifying Granularity**
Individual identities are protected using limiters negotiated between partners but with an absolute minimum value of 30.

Karlsgate

Karlsgate is an innovative data integration company. Through the Karlsgate Identity Exchange, we empower data owners, brands, publishers, agencies and technology companies to share consumer insights freely without exposing consumer identities.

Learn more about us at karlsgate.com or contact us at info@karlsgate.com.

1 The Next Level of Personalization in Retail. BCG-Google, Business Impact of Personalization in Retail Study–Consumer Survey, U.S., 2019, Boston Consulting Group, 2019.
2. GDPR Article 4.1.
3. Cal. Civ. Code § 1798.140(o)(1).
4. World Federation of Advertisers (WFA) Global Privacy Map, June 2020.
5. GDPR Enforcement Tracker, CMS Hasche Sigle Partnerschaft von Rechtsanwälten and Steuerberatern mbB.