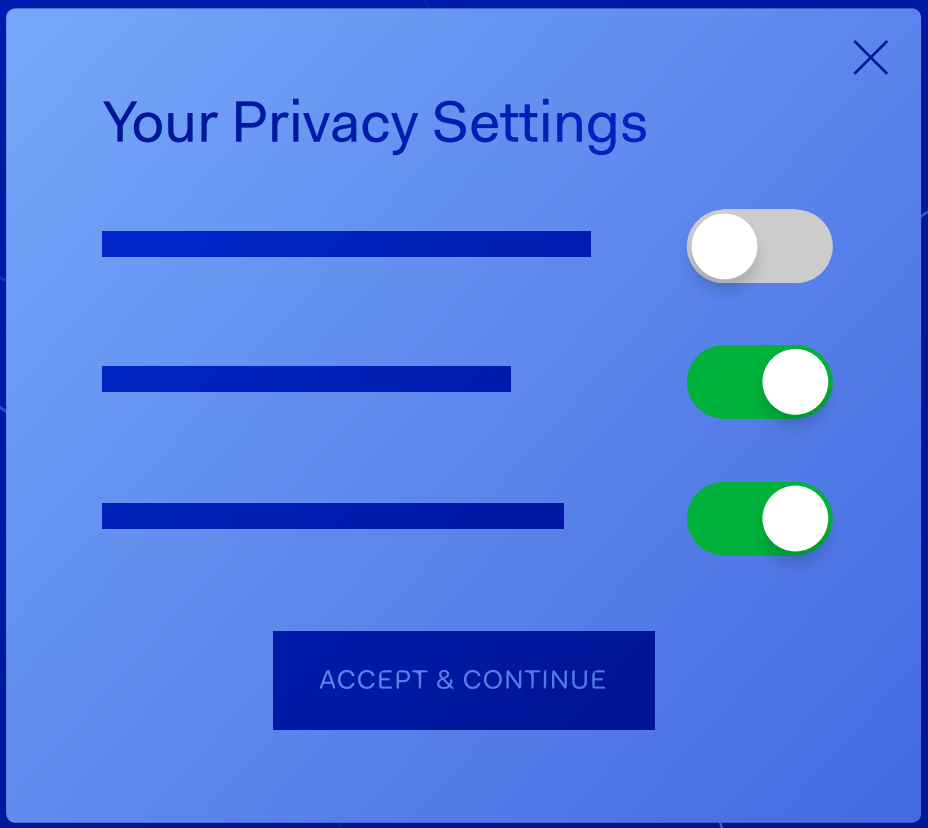
Auth0

mylife digital

Consent Management as a Competitive Advantage

You can build trust if you're prepared to be more transparent



Following in the footsteps of GDPR, the California Consumer Privacy Act (CCPA) takes effect on 1 January, 2020 with enforcement beginning on 1 July, 2020. Whilst many UK businesses brace for a shuddering blow, some are shrewdly viewing data privacy as a competitive advantage, using consent management to build trust and stimulate innovation.

Privacy laws will cover half the population's data by 2022

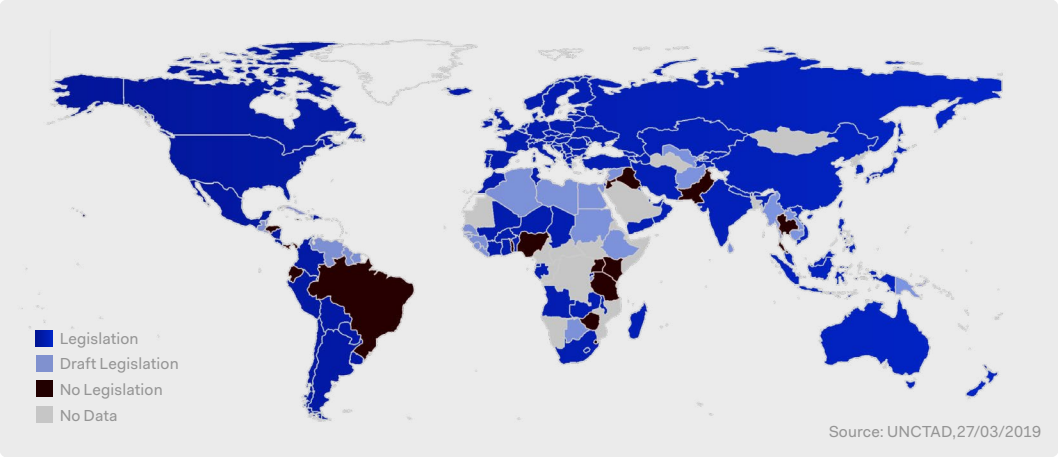
We have created more data in the past three years than in the entire history of the human race.[1] But as data volume has grown, so too has data misuse. The General Data Protection Regulation (GDPR) sparked a global shift in how (and when) organisations start thinking about what data they collect, where it's stored, and how it's processed.

As of 2019, data protection and privacy laws cover 58% of the world's countries and another 10% of countries have draft legislation in progress.[2] With the CCPA on the horizon, consent and preference management is top-of-mind – but it doesn't have to keep you up at night.

Consent under GDPR vs. CCPA

Consent is one of the six lawful bases for processing personal data, set out in Article 6 of the GDPR.[3] The UK's data protection authority, the Information Commissioner's Office (ICO), defines GDPR-compliant consent as "giving individuals genuine choice and ongoing control over how you use their data, and ensuring your organisation is transparent and accountable." [4]

1 PwC, Data the new Smart
2 United Nations Conference on Trade and Development (UNCTAD), Global Cyberlaw Tracker
3 Information Commissioner's Office, Lawful basis for processing
4 Information Commissioner's Office, Why is consent important?



Graphic 1: As of 2019, data protection and privacy laws cover 58% of the world's countries and another 10% of countries have draft legislation in progress.[2]

In practice, individuals must be able to easily give and withdraw their consent (i.e. not buried in complex terms and conditions) for you to process their data for a specific purpose. The purpose should describe how you process their data, who it is shared with, how you contact them, and – most importantly for business intelligence – what is added to their data and why. We'll explore the issue of adding data, often called 'profile enrichment', later on.

As a best practice, consent should be refreshed regularly. If you have any doubt that a customer's consent is still valid, refresh it.

CCPA has a great deal of overlap with GDPR, with the additional provision that individuals have the right to stop businesses from selling their information to third parties. "Note the definition of sale in the CCPA is wide enough to include sharing personal information (PI) for non-monetary consideration, such as for preferential product placements in a store. The definition of sale could also cover sharing PI collected via cookies or similar technologies with a company in exchange for enhanced services, such as sharing PI with an advertising network, which might pool the PI collected across a number of client websites in order to better target ads," explains *CIO UK*.[5]

5 CIO UK, *The California Consumer Privacy Act and EU businesses - Another hurdle in race for compliance?*

However, unlike GDPR, the right to 'opt-out' under CCPA only applies when "a business sells personal information relating to Californian consumers."[6] For more information, the International Association of Privacy Professionals (IAPP) also offers a primer on GDPR-compliant consent and how it differs from CCPA.

87% of consumers likely to exercise right to 'opt-out'

Consent puts consumers in control of their data, but businesses are understandably concerned about its impact on their operations. If you resell data collected from free apps like Facebook or Google, or just want to collect enough data to provide the best user experience, you've felt the seismic shift caused by data privacy regulation.

"Research predicted that some organisations could lose up to 75% of their marketable database under GDPR, but our conversations have indicated that, in many cases, this could be considerably more," says J Cromack, co-founder and Chief Innovation Officer at Privacy UX company, MyLife Digital.

The outlook on CCPA is equally grim. Recent BritePool and Annenberg Research showed that 87% of consumers said they would exercise their opt-out rights.[7] However, one year after GDPR came into effect, only 13% of people had acted to restrict the use of their personal data.[8] This should be encouraging to companies preparing for CCPA and other local regulations.

Lost marketing data isn't necessarily bad news either. "Many of those contacts were probably lost already as they were not actively engaged.

6 Fieldfisher, CCPA Blog Series, Part 3: *Confused over opt-out rights? You're not alone.*
7 Adweek, *87% of Consumers Would Opt Out of Ad Targeting Under CCPA Terms*
8 TrustArc / Ipsos, *GDPR Consumer Survey*

"Research predicted that some organisations could lose up to 75% of their marketable database under GDPR, but our conversations have indicated that, in many cases, this could be considerably more."

J Cromack
co-founder and Chief Innovation Officer, MyLife Digital

So, what this allows is a concentrated effort to put the customer at the centre of everything. To improve the quality of your customer data and build a strong foundation from which you can engage your database," says Cromack.

Consent is central, but not centralised

Multiple stakeholders, including Marketing, Data Governance, Risk, and CRM managers, rely on consumer consent to meet their goals, but there's rarely a single database to pull from. The reality is most businesses collect and store data in silos, with duplicate records that cannot be merged within a single database, let alone across multiple.

For example:

- Consent records may be stored against one or more of these duplicate records and regularly contain conflicts.
- Reading the different records takes manual intervention because there is no common taxonomy.
- Linking consumers' consent and preferences to external systems like an Email Service Provider (ESP) or Customer Relationship Management (CRM) can be complex.

Yes, data privacy has created a new normal. But when you look at the opportunities to build your trust and brand reputation with customers, there are plenty of reasons to be optimistic.

57% of consumers more likely to spend with compliant brands

The ICO offers a nice summary of consent as an advantage: "Getting this right should be seen as essential to good customer service: it will put people at the centre of the relationship, and can help build confidence and trust. This can enhance your reputation, improve levels of engagement, and encourage use of new services and products. It's one way to set yourself apart from the competition."[9]

Recent research proves it. As organisations increase transparency, people trust more, and are more willing to spend their money with compliant brands:

- One in three people (34%) trust companies and organisations to store and use their personal data, up from one in five in 2017.[10]
- The majority of UK consumers (57%) are more likely to do business with brands that demonstrate GDPR compliance, with a badge or seal.[11]

Graphic 2: The majority of UK consumers are more likely to do business with brands that demonstrate GDPR compliance, with a badge or seal.

10 Information Commissioner's Office, *ICO trust and confidence report 2019*
11 TrustArc / Ipsos, *GDPR Consumer Survey*

But we still have a long way to go. "Consumers still don't fully trust organisations with their data but want a highly-personalised experience. It's a real paradox. We need to empower individuals in new ways to obtain the data the business needs, while respecting their right to choose what they share," said Cromack.

Treat your data as a liability

If you want to engage your customers in a mutual value exchange, first ask yourself, "What data do I actually need?" You must have a legal basis for collecting any kind of personal data under data privacy regulations. Collecting more or less than you actually need can have negative consequences, from poor user experience to credential stuffing attacks.

Here's an example: A company wants to set up a geofence to improve the user's experience when they visit a physical shop. They want to know adoption rate (how many people are using the app in the store) and conversion rate (whether a person used the app and then went to the store within a certain time period).

The company could collect and store all of the following data in a single record for the user:

- GPS location
- Nearby WiFi
- Nearby Bluetooth
- IP Address
- Unique ID of the device
- User ID
- Items searched
- Timestamp

But this is far too much information for two simple questions. The company would achieve the exact same result by collecting just two data points: the user's last login and the geofence boundary. Learn how this works in our blog about a security-minded approach to data design.

Resist the urge to collect data because you might need it in the future. Consumers don't want to share their location with a Solitaire app where there's no clear benefit. However, they will trade data for value – even first-party data, if you empower them to do so.

Consumers will trade data for value

Co-creating experiences with customers is a powerful way to improve your value proposition and increase your revenue. One option is profile enrichment, the process of adding data to a user's profile by using third-party APIs like Clearbit or FullContact, or social providers like Facebook or Google. By consenting to profile enrichment, users receive a personalised experience and offers, which may boost their engagement.

If you'd like to enrich user profiles, you must inform consumers how their data will be used and name any third-parties. Often this requires additional consent, since users may not have given you certain data or defined how you can use it.

Third-party data won't disappear completely, but it shouldn't be your sole strategy. "As the unpermissioned data market diminishes, it will become increasingly critical for marketers to invest in building and maintaining their own first-party data assets," says London publisher Raconteur.

"As the unpermissioned data market diminishes, it will become increasingly critical for marketers to invest in building and maintaining their own first-party data assets,"

— Raconteur

It's possible to enrich a profile with data from users themselves, known as 'progressive profiling.' Progressive profiling is a technique for asking a few questions each time the user logs in to build up a profile over time.

For example, the first time someone logs in, you might ask for:

- Their name
- Their email address
- Their password

At second login (or at purchase), you might ask for:

- Their address
- Their birthday
- Their phone number

At third login, you might ask for:

- Their company
- How many people work for them
- Their industry, and so on.

Of course, you can't possibly ask users every single thing you want to know. Progressive profiling is best used as a companion to profile enrichment. It's a powerful tool for increasing signups by shortening registration forms and helps build trust with consumers by involving them in personalisation.

Whitbread, owner of the UK's leading hotel chain, Premier Inn, is using these tactics to add value to both the company and its customers. "[When] people come to the website direct, we ask them to enter their registration or their details. Obviously, everybody's on different social media platforms. The ability to opt-in and do progressive profiling, all those kind of things that Auth0 is already offering us is something that we want. We've found that the more people that we have sign up to accounts, their average booking value increases," said Danny Goodwin, former digital delivery manager at Whitbread.

Taking it a step further, you can blend progressive profiling with progressive consent from MyLife Digital to create a compliant audit trail demonstrating the correct privacy notices have been shared to collect additional data.

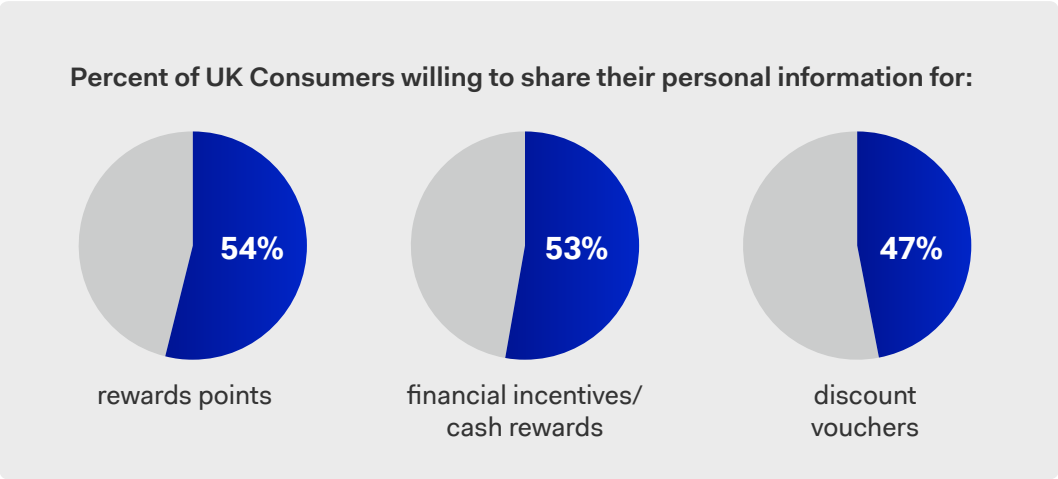
54% of UK consumers would trade data for rewards

Most people said they would exercise their 'opt-out' rights under CCPA, but it's a very different picture when you introduce rewards.

A second poll from Britepool and Annenberg Research allowed participants to select an additional option: 'Reward Me for My Personal Information'. In this poll, 21% selected the new option, and the number of people who said 'do not sell my personal information' dropped by 30%. "Our takeaway from the research is that people are distrustful of the internet...and they want three things: information, control, and rewards," said Britepool COO Bob Perkins on *Adweek*.[12]

Indeed, more than half (54%) of UK consumers would be willing to share their personal data for rewards points, followed by financial incentives/cash rewards (53%), and discount vouchers (47%), according to OnBuy.[13]

12 Adweek, *87% of Consumers Would Opt Out of Ad Targeting Under CCPA Terms*



Graphic 2: The majority of UK consumers would trade data for rewards

Fewer consumers (16%) were willing to trade data for personalised rewards or recommendations. However, 87% of consumers in an Accenture study said it's important to purchase from a brand or retailer that 'understands the real me'.[14] The reality is likely somewhere in between: personalisation that is within reason and delivers real value.

"We are seeing more and more that people are willing to engage in trade-offs, as long as they're getting something valuable in return. It's up to companies to strike the right balance and then guard that data with their life so they don't lose the trust they've worked so hard to build," said Martin Gontovnikas, VP of Marketing at Auth0.

Nearly four in five people (78%) felt companies should be held responsible for lost or stolen information in the event of a data breach, according to the ICO.[15]

Make consent management work for you

Whilst it's not impossible for internal teams to solve these challenges themselves, there are tools available that ultimately save on cost and

13 Small Business, *More than half of UK consumers will share personal data for reward points*
14 Accenture, *2019 Consumer Pulse Survey*
15 Information Commissioner's Office, *ICO trust and confidence report 2019*

resource. It's the classic build vs. buy equation we explore with our customers and prospects every day.

Gartner forecasts privacy regulations will drive at least 10% of market demand for security services through 2019, including identity and access management (IAM).[16] Identity solutions like Auth0 control access, the point at which consent must be obtained or verified. We offer out-of-the-box features and last mile customisations to help you build trust with your users and secure their data with the latest technologies like breached password detection and multi-factor authentication. Although Auth0 does not provide consent management solutions directly, a natural benefit of Auth0 is integration with best-in-class consent management platforms like MyLife Digital.

Is buying a consent management solution right for you? Ask yourself these questions:

- Is building your own consent management tool going to add to your core proposition or be a distraction, taking priority away from other value adding processes?
- Do you have the domain expertise in-house to ensure you can build this in line with the forever changing and relevant regulations?
- Will building your own consent management tool provide you with a competitive advantage?
- Can you ensure that the project will deliver required capabilities? Is it likely to have scope reduced to meet budget / time constraints? (Phase 2 hardly ever happens!)
- Do you have the budget to maintain the consent management function as an ongoing cost centre?
- Have you the experience, resource, cost and capabilities to continuously develop the tool as new guidance regarding consent and best practice emerges?

16 Gartner, *Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019*

About Auth0

Auth0, the identity platform for application builders, provides thousands of enterprise customers with a Universal Identity Platform for their web, mobile, IoT, and internal applications. Its extensible platform seamlessly authenticates and secures more than 2.5B logins per month, making it loved by developers and trusted by global enterprises. The company's U.S. headquarters in Bellevue, WA, and additional offices in Buenos Aires, London, Tokyo, and Sydney, support its customers that are located in 70+ countries.

For more information, visit https://auth0.com or follow @auth0 on Twitter.

About MyLife Digital

Trusted data, powering positive outcomes

MyLife Digital, through its market leading Privacy UX platform Consentric, rebalances the management of personal data between organisations and individuals, building consumer trust.

The company strives to facilitate transparency between the data owner and those who wish to use it, for whatever purpose, helping everyone do the right thing, with the right data.

MyLife Digital recognises its ethical responsibility as a custodian of personal and proprietary data, by implementing privacy by design into all systems and processes.

For more information, visit https://mylifedigital.co.uk/.