Custobar

The Marketer's Manual to European Data Protection

How to Handle Customer Data Privacy in Consumer Businesses

These days marketers may feel that with all the customer data regulation in place, they should be as well-schooled in marketing technology as marketing, and have a law degree on the side. In the EU, regulation is rapidly developing on many fronts. The General Data Protection Regulation, GDPR, is the most powerful policy, but there are many others in place as well.

On top of EU data protection regulation, there are local, country specific rules and regulations. Applications of GDPR have furthermore raised the question of how personal data can be moved between EU countries and non-EU countries. EU-U.S. data transfers are a special case in point, deeming Google Analytics potentially illegal in the EU. So much so that Austria, France, Denmark, and Italy have already banned Google Analytics.

The genuinely well-meaning regulation that aims to protect personal data has made it truly difficult for companies to provide consumers with relevant and targeted content and marketing communications. With all the data protection regulations and the loss of third-party cookies, both companies and marketing platforms struggle to get and get to utilise customer data. The question that companies face is: How to make my brand appealing to B2C customers?

In our opinion, we should move from a marketer mindset of "how to get as much customer data as possible in order to utilise it in marketing" to a marketer mindset of "how to build trust and a truly meaningful, long-lasting customer relationship". And how to be data regulation compliant and still thrive as a business.

In this white paper, we give clear answers to how your business can get all the benefits of customer data. We also tell how not to be hindered by the loss of third-party data and EU data protection policies in consumer businesses. In short, the answer lies in controlling your own data. The answer is, in other words, first-party data.

Since most of the EU's personal data protection laws and policies are being discussed in scattered webinars that only focus on one regulation at a time, we compiled this guide to give marketers in consumer businesses a comprehensive overall look at the data protection situation by the end of August 2023 with regular updates to this white paper as the regulation evolves.

From Zero to Hero: What a Marketer Needs is 1st Party Data

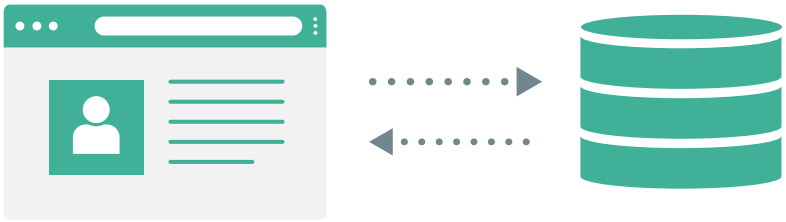
Customer data is at the heart of any and all successful marketing these days. All data is not equal, however. Not as data, not as means for driving sales or enhancing customer experience, and not in relation to data protection issues.

To start, let's define the types of data with an emphasis on first-party data, since it will be the most valuable data for marketers moving forward. Below we will tell you why.

First-party data, also known as 1st party data and 1P data, is customer data that a company collects directly from its customers on its own channels (website, mobile app, etc.). That data is **controlled by the company.** Of course, under GDPR and other regulations, every individual has rights over their data as well.

Companies collect 1st party data directly from consenting customers. **Customer consents** can be becoming a member of the loyalty program or subscribing to the mailing list, for instance. Webshop purchases are also important data sources, since personal data sharing is unavoidable in order to receive the bought items and in accepting the company's Terms and Conditions.

Examples of 1P data include purchase history, website activity, email engagement, interests, behaviours, support calls and sales interactions, customer feedback, etc. **First-party data is of high quality, accuracy, and relevance to your business.**



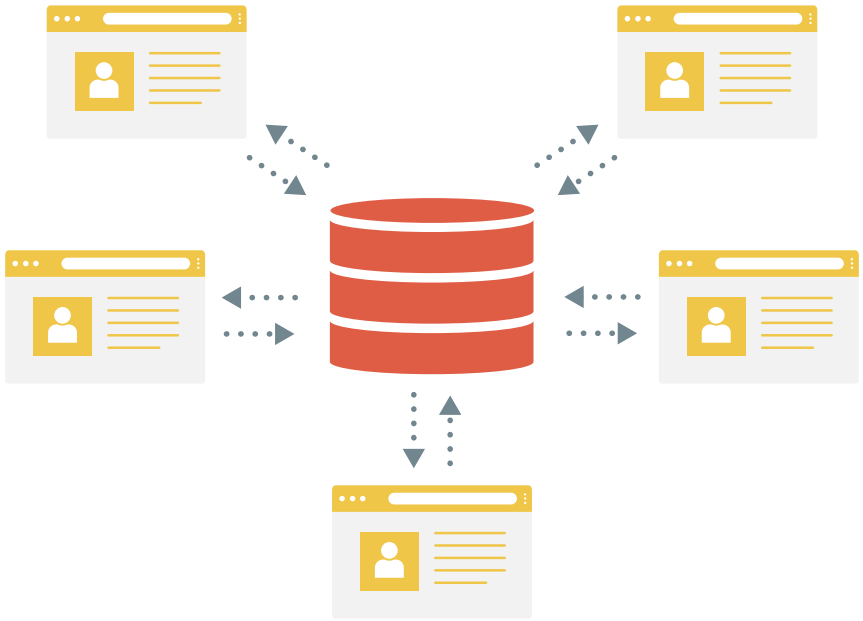
Second-party data is quite insignificant these days, at least in the EU. It is first-party data that is controlled by someone other than your company. It's sold in a private data marketplace and purchased (or legally accessed) directly from the data managers. Data accuracy and reliability are dependent on the data source. An example would be data that media publishers sell to advertisers.

After the purchase of 2nd party data, it is under the same data protection policies as 1st party data. In the EU, under GDPR, customer consent for second-hand data is so-called second-hand consent, which makes the use of 2nd party data impractical and cumbersome. The insignificance of 2nd party data also has to do with the fact that the data is not of good quality.

Third-party data is collected by companies, governments, non-profits, academic sources, etc., without a direct relationship with consumers. This data is obtained by data aggregators, who compile it into single datasets. 3rd party data is shared, bought and sold on data marketplaces and exchanges.

Advertisers purchase 3rd party data through platforms like DSP (demand side platform) or DMP (data management platform), or data marketplaces such as Google. The selling and buying of advertisements and advertising spaces is done programmatically, and 3rd party data acts as the transactions' facilitator. In other words, 3rd party data is not the actual object of the purchase.

There are two notable problems with utilising 3rd party data. Firstly, cookie laws and internet browsers have restricted 3rd party data usage significantly. Secondly, whether data protection regulation was followed in data collection may remain unknown depending on the 3rd party data provider.



You may come across another type of data as well, **zero-party data.** As a data type it's rather new. It may also be confusing, since in many ways it coincides with first-party data. The best way of understanding what zero-party data is may be the way it differs from first-party data:

- first-party data gives you analytics and user behaviour insights
- zero-party data is optional information that a customer intentionally and proactively shares with your company. For instance, how an individual wants to be recognised by a brand, what's their preference centre or what are their purchase intentions.

The four types of data in comparis on with each other:

	First-party data	Second-party data	Third-party data	Zero-party data
Customer relationship	Direct	Indirect	Indirect	Direct
Consent to data collection	Yes*	Yes*	Yes*/Unknown (depends on data provider)	Yes*
Data	Individual	Individual	Aggregate**	Individual
Accuracy and reliability	High	High	Low	High
Data sharing, practical recommendations	No	Yes, but only with trusted partners and not at all in B2C	Yes, with many companies	No

* Note! Data collection and handling may sometimes be based on other criteria than direct customer consent.

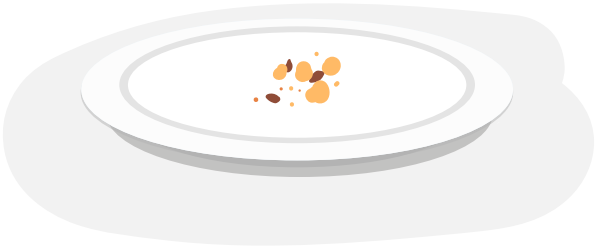
** Aggregate data is usually anonymous in this context. However, it may also be personal data.

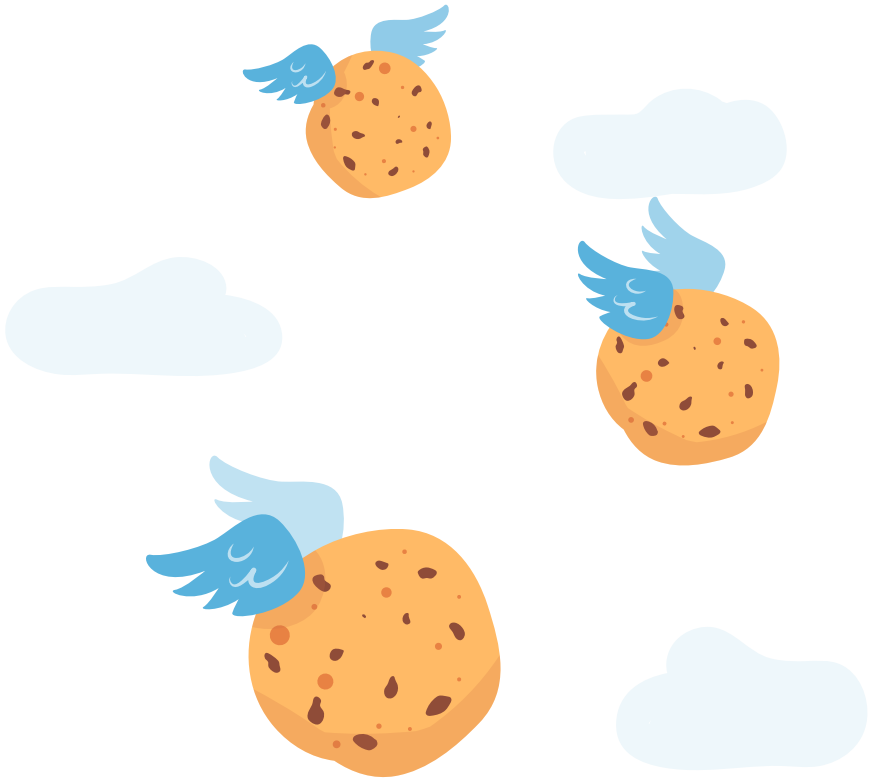
Data Protection in a Cookieless World: Why a Marketer needs 1st Party Data

When we start talking about cookies with any type of data, an important distinction needs to be made: **First-party data is not first-party cookie data.** Any data type discussed above is not cookie data. Some of it may be, but **data types are not cookie types.** Cookies are just one data source among many.

We've become accustomed to cookies being the primary tool for tracking and collecting customer data on the internet. Google is in the process of blocking third-party cookies from Chrome browsers, and Apple has provided consumers with the ability to opt-out of third-party cookies and tracking on its browsers and apps on iOS devices for some time now.

Getting cookie consent from consumers also hugely restricts cookie usage. If a consumer does not consent to cookies, data cannot be collected for marketing purposes.





Cookies are a means to collect data directly from a website visitor's browser, but they are not the only way for consumer data collecting. First-party cookies are one of many first-party data sources. However, data on newsletter subscriptions, loyalty programme memberships, or purchase data does not have to be cookie data. It can be stored via a website's or webstore's backend.

Third-party cookies are on their way out, and cookie data is becoming less and less important in collecting customer data. There are three main reasons for this:

1. Data protection regulations (GDPR in the EU, CCPA in California, and many others, some of which are still in progress) require **explicit consumer consent to cookie data.** According to these regulations, both consent and denial must be equally easy to do on a website. Easy denial of consent has led to a rapid decline of using cookie data, because the availability or the terms of use are not what they used to be.

2. **Browser and operating system manufacturers have started to restrict the use of third-party cookies,** as we already saw with Google Chrome and Apple's iOS14 and newer.

3. **Consumers are becoming more informed** and more concerned with what data is collected about them, how the data is used and stored, and with the overall fact that they have a right to privacy.

When companies no longer get actionable consumer data from third-party cookies, they need to find other ways to convey information about consumer behaviour. That means that Meta and other advertising platforms no longer receive consumer data directly from browsers and mobile applications. The effects are already tangible: marketing campaigns are getting more expensive while their targeting is getting more difficult.

The remedy: first-party data. First-party data can be utilised in targeting marketing communications in the company's own channels as well as targeting ads in advertisement tools. A company's own channels are, for example, email, SMS and push messages, whereas advertisement tools include, among others, Meta, Google Ads, and media companies.

With Meta and Google, there are country specific rules and regulations regarding the need to ask for consumer consent in sharing a company's customer data.

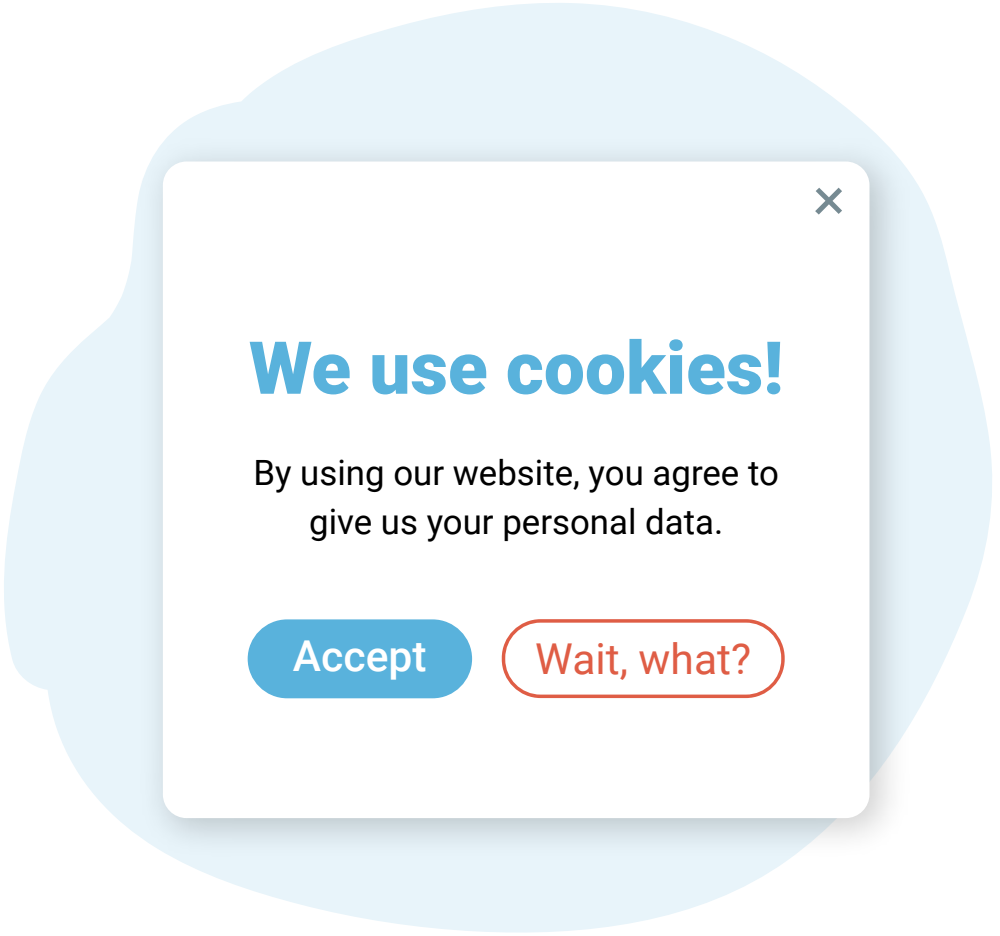
Consumer businesses need a customer data platform (CDP) such as Custobar to collect, manage and utilise their customer data for targeting and personalising communications to their customers. The platform also offers invaluable granular insights into what each audience is interested in, what actions they take, where they live, and beyond. To learn more, **read our CDP whitepaper.**

Between Cookieless and Cookie-filled Worlds: Cookie Laws and Consent Policies

Cookies are unique identifier codes of website users. They are generated by web servers and sent to web browsers, where they are stored for predetermined or indefinite periods of time. They may also only be stored for the length of a single session that a consumer visits a website or webstore.

Cookies inform websites about their users. They indicate that users have returned to a particular website. They also help personalise a website's user experience, and are used for tracking a website's user's visit. **For marketers, their importance lies in the customer data they convey, which is used for targeting, for instance.**

There are many types of cookies, and they are used for a variety of purposes. First-party and third-party cookies were already mentioned above (not to be confused with first-party data or third-party data!), but there are also session cookies, persistent cookies, authentication cookies, and tracking cookies, among others.



Stricter data protection regulation has had an impact on cookie policies. Website and mobile app visitors have the right to choose what cookies they allow.

In cookie compliance, the most commonly used are "Accept all cookies" or "Accept only necessary cookies". By accepting, a website visitor agrees to the storing of all categories of cookies. Rejecting some or all categories of cookies usually requires the website visitor to make a number of consents, some of which may be quite confusing. At least they do nothing to enhance the website's user experience.

Strictly Necessary Cookies are essential for the website to function. They deliver security and enable core site functionalities. Strictly Necessary Cookies are always active, and they are never used to track individuals across websites.

Functional Cookies are required to remember a website visitor's choices, for example language preference or browsed products, to provide the user with a more personalised experience on future visits.

Performance or Analytics Cookies provide aggregated statistical information, that includes the number of page visits, page load speeds, time spent on particular pages, browser and device preferences, etc. They are used to improve a website's performance and design.

Targeting or Marketing Cookies are used to deliver and target advertisements.

The cookies that are used on a particular website must be found on the website's Cookie Policy.

Despite the importance of **cookies** for companies and service providers (and marketers!), they are governed by both the GDPR and the ePrivacy Directive. The need for regulation comes from the fact that although cookies in and of themselves are harmless, **they can potentially identify a website visitor without consent and therefore contain data that can be considered personal.**

While the GDPR is the most comprehensive data protection legislation in the EU, it is **the ePrivacy Directive (EPD) that is known as the "cookie law".** It both supplements and, in some cases, overrides the GDPR in relation to cookie policy. The ePrivacy Regulation (EPR) will eventually replace the EPD, building upon it and expanding its definition. In the meanwhile, there are country-specific interpretations about how to ask for cookie compliance.

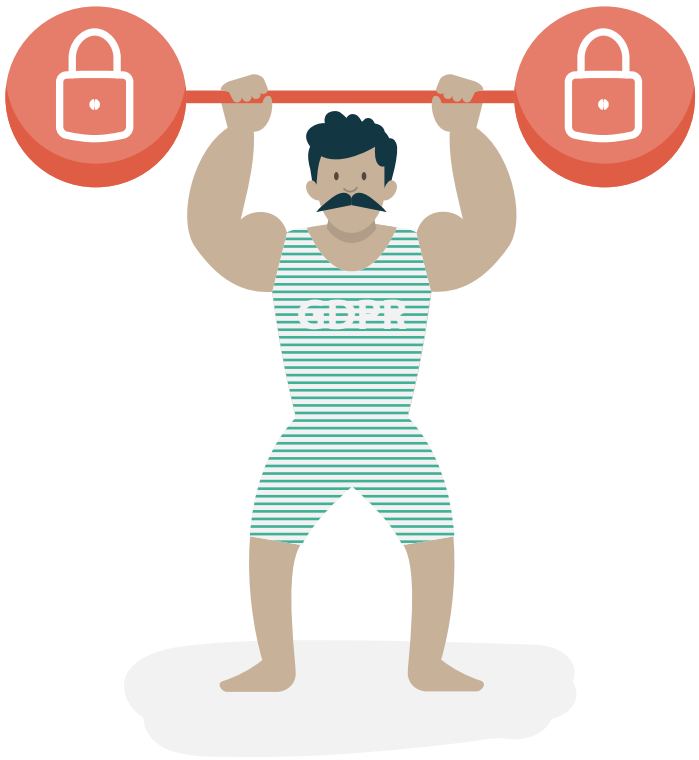
What is true throughout Europe, despite the varying policies and practices from country to country, is the severity with which necessary and unnecessary cookies are treated. **Marketing and analytics cookies are not necessary. Any system that has been dependent on third-party cookies no longer receives the amount of customer data than before. Furthermore, the data does not convey as much information as before.**

A Customer Data Platform (CDP) such as Custobar will continue to collect versatile customer data, because it is not dependent on cookie data.

The use of 3rd party cookies is restricted not by law or policy, but by browsers and manufacturers, especially Apple. Laws and policies require the consumer's explicit consent.

GDPR, the Toughest Privacy and Security Law in the World

The General Data Protection Regulation, GDPR, is the culmination point of the European Commission's major modernisation process of the data protection framework. Most marketers no doubt still remember May 25th of 2018, which was the deadline for being GDPR compliant.



GDPR was brought about by the EU to give its citizens more control over how their personal data is used. The law governs the way in which companies and organisations within the EU can use, process, and store personal data, that is, information about identifiable, living people.

There are 7 key principles of GDPR:

- Lawfulness, transparency, and fairness.
- Only using data for the specific lawful purpose that it was obtained, the most lenient of which is legitimate interests.
- Only acquiring data that is strictly needed.
- Ensuring the accuracy of first-party data.
- Storage limitations.
- Integrity and confidentiality.
- Accountability.

Individual rights granted by the GDPR:

- Right to be informed of how your data is being processed.
- Right to access this data.
- Right to rectify incorrect data.
- Right to erase data.
- Right to restrict processing of personal data.
- Right to data portability. This means that a business will need to put in place a system by which it can quickly and easily compile all the personal data it holds on an individual and make it securely accessible to them. The Custobar Customer Data Platform (CDP) is one good system for this.
- Right to object to your data being processed.
- Rights relating to automated decision-making, including processing.

The lawful basis for processing personal data is important to identify under GDPR. These reasons are acceptable:

- Consent
- Contract
- Legal obligation
- Vital interests
- Public task
- Legitimate interests

For marketers in online businesses, for instance, this means that getting personal information from the consumer should in principle be consensual. **While personal data cannot be collected just for the fun of it, an existing customer relationship is a valid and acceptable reason.**

Although the General Data Protection Regulation applies to individuals, companies and organisations that handle personal data within the EU, countries outside the EU are also under the same regulation when:

- They supply goods or services to the EU.
- They process data about citizens residing within the EU.

Data processing and data transfers from the EU to other countries, 'Third Countries' under GDPR, especially to the U.S., has been and continues to be a pain point. The controversy over Google's Analytics being illegal is a case in point. The reason for the pain point is that many European companies use the products and services provided by American high-tech companies. The Hubspot Marketing Automation software is a good example. Even if these companies store their consumer/customer information in the EU, their access to that personal information has been deemed problematic.

The situation is that **there are no legal agreements about EU-U.S. data flows currently in effect**, not since the EU-U.S. Privacy Shield was brought down in July 2020. The EU and the U.S. have agreed "in principle" on a data transfer deal to replace the defunct Privacy Shield, but there is no knowledge about how long the current legal uncertainty will persist. Until then, Standard Contractual Clauses (SCC) regulate data transfers between EU and non-EU countries.

The "New Deal for European Consumers", a.k.a. The Omnibus Directive

On 7th January 2020, **the Omnibus Directive** (Directive (EU) 2019/2161) came into effect. The EU Omnibus Directive, also known as **the Enforcement and Modernisation Directive**, needed to be brought into action by 28th May 2022 in all EU member states.

The EU Omnibus Directive is part of the EU's New Deal for Consumers initiative. The initiative's objective is to strengthen the enforcement of EU consumer laws and modernise EU consumer protection rules in light of market developments. The directive, on the other hand, aims to bring digital content, goods, and services into the scope of consumer protection legislation.

Put simply, the EU Omnibus Directive gives consumers more rights while placing more restrictions on businesses for consumer protection. The main idea is to **bring all digital transactions under consumer rights that have earlier only been applicable to traditional products and services.**

The EU Omnibus Directive is a new directive that significantly changes four existing consumer protection directives:

- The Consumer Rights Directive (2011/83/EU)
- The Price Indications Directive (98/6/EU)
- The Unfair Contract Terms Directive (93/13/EEC)
- The Unfair Commercial Practices Directive (2005/29/EC)

Under the directive, consumers can exercise traditional consumer rights when they buy digital goods, services, and content. **For consumer businesses, the directive means following a strict set of standards in listing and marketing their digital offerings.** Businesses that are not compliant with the directive are liable to a fine.

Here are some of the most important requirements that the new directive brings about:

The **new consumer rights** expand consumer rights to digital transactions. These rights include the right to withdraw within 14 days and the right to receive necessary pre-contractual information. An **exception** to these rights occur when a consumer provides personal data that is given due to a legal requirement or processed solely to supply the digital content in question.

There are a whole host of **new restrictions on businesses.** They include restrictions on price manipulation and transparent pricing, increased online marketplace transparency for consumers about their rights, prohibition of fake reviews, and regulating the conversational AI, speech-based assistants, and chatbot interaction between consumers and traders.

For consumers, the EU Omnibus Directive means more protection against and remedies for unfair business practices, such as overly aggressive marketing or fake reviews. Consumers should also be able to make better choices in online marketplaces.

With the new directive, businesses need to review and renew their terms and services, pricing processes, and transparency practices.

Europe Is On Its Way to ePrivacy Regulation

The ePrivacy Regulation (ePR or EPR) was originally intended to come to pass together with the GDPR. However, the negotiations of the ePrivacy Regulation are still ongoing.

According to the European Commission, the Regulation on ePrivacy "aims at reinforcing trust and security in the digital world." The regulation for ePrivacy rules for all electronic communications proposal is from 2017, and it includes:

- The regulation's applicability to **new players** in electronic communications service providers, such as WhatsApp, Facebook Messenger, and Skype.
- **Same level of protection** of their electronic communications for all consumers and businesses in the EU.
- **One single set of rules** across the EU, which is good news to all businesses.
- **Guaranteed privacy for communications content and metadata** (data that describes other data, such as location, creation date, and author).
- **Streamlined cookie laws**, which will be more user-friendly and clarify instances when consent is not needed.
- Unsolicited electronic communications will be banned. **Protection against spam** covers email, SMS and automated calling machines. Marketing callers will be required to display their phone numbers or use a special prefix indicating a marketing call.
- Regulation **enforcement** will be the responsibility of the same data protection authorities that are in charge of the compliance with the GDPR rules.

While we wait for the ePrivacy Regulation to come into effect in 2024 at the earliest, the ePrivacy Directive (ePD or EPD) is largely responsible for gaining access to and storing consensual consumer information on users' devices. That makes EPD, or its Article 5 to be more precise, the current "cookie law".

European privacy and data protection laws are made up of both the GDPR and the ePrivacy Directive. The difference is, that the GDPR applies only to the processing of personal data, while the ePrivacy Directive regulates electronic communication even when it concerns non-personal data.

The main difference between the current ePrivacy Directive and the upcoming ePrivacy Regulation is, apart from the obvious content differences, that a directive must be incorporated into national law by the EU countries, whereas a regulation becomes legally binding throughout the EU when it comes into effect.

There is much regulation and legislation concerning cookies and digital direct marketing that vary from country to country.

On 23rd April 2022, the European Parliament and Council of the EU also reached a provisional political agreement on the Digital Services Act (DSA). Together with the Digital Markets Act (DMA), which reached political agreement on March 25, 2022, the DSA and the DMA form a single set of new rules known as the Digital Services Act package. The package will be applicable across the whole EU, and it has two main goals:

1. To create a safer digital space protecting the fundamental rights of all digital services users.

2. To establish a level playing field to foster growth, innovation, and competitiveness, both in the European Single Market and globally.

The Digital Markets Act (DMA) especially defines clear rules for large online platforms and marketplaces, such as Google, Amazon and Meta. The Council of the European Union stated in their press release on March 25, 2022, that the DMA "aims to ensure that no large online platform that acts as a 'gatekeeper' for a large number of users abuses its position to the detriment of companies wishing to access such users."

Business Success That is Unhindered by European Data Policy

With all the data protection and privacy rules and regulations concerning consumer data that consumer businesses need to comply with, it might be scary and quite confusing to continue with collecting customer data and using it for targeted and personalised omnichannel marketing. Including third-party marketing platforms such as GoogleAds and Facebook.

However, it doesn't need to be rocket science. **Follow these three steps to ensure your (data-protected) commercial success:**

1. Build a trustworthy and meaningful bond with your customer so that your customer feels comfortable providing your business with their personal information and gives their consent for using that data.
2. Be sure to provide actual added value for your customers in exchange for having and using their data, for example via loyalty programs.
3. Collecting, using and storing first-party data that your company owns into Customer Data Platforms (CDPs) like Custobar is the best practice in complying with the existing and preparing for the upcoming data protection legislation.

Tatu Kuivalahti
CEO Custobar

About Custobar

Custobar is a Customer Data Platform (CDP) and marketing automation tool that combines data from all customer touch points: purchases from both online store and physical locations, browsing data, mobile app transactions, customer service tickets etc. Custobar offers the easiest user interface in the market for business users to understand their customerbehaviour and build marketing automations. Custobar also provides comprehensive and real-time integration APIs for agile integration with other systems.

Custobar was founded in 2014. The company is based in Helsinki. Custobar's unique sales and marketing platform is already in use in more than 11 countries across Europe and the US by retailers and other consumer businesses.

Custobar

VISIT CUSTOBAR

Glossary

1P data/1st party data

First-party data is information that a company collects directly from its customers. It is company (and consumer in question) governed data that is available for marketers. First-party data reduces the need for any other type of data.

3rd party cookies

Third-party cookies are files that store information on the website visitor's computer. Third-party cookies are being phased out because their usage violates privacy concerns and regulatory laws. The loss of third-party cookies is best leveraged with a first-party data strategy.

CCPA

The **California Consumer Privacy Act** of 2018. It is a data protection law regulating the way businesses worldwide are allowed to handle California residents' personal information. The CCPA was made effective 1st January 2020. It is the first law of its kind in the U.S.

CDP

A **Customer Data Platform** is a system designed to collect and combine customer data from all sources and marketing channels into one unified profile of each individual customer. These profiles can then be used for customer segmentation and targeted and personalised omnichannel marketing campaigns. A CDP relies heavily on first-party data and is thus the best martech tool to battle both the 3rd party cookie loss as well as all the rules and regulations on personal data protection. To learn more about what a CDP is, read our CDP whitepaper.

DMA

The European Commission adopted a proposal for a **Digital Markets Act** on 15th December 2020. The proposal addresses the negative consequences arising from platforms that act as digital "gatekeepers" to the internal market. These platforms, such as Google or Meta, are considered to have the power to act as private rule-makers and function as bottlenecks between businesses and consumers.

DMP

Data Management Platforms collect, organise and activate first-, second-, and third-party data from various online, offline and mobile sources. That way they resemble Customer Data Platforms (CDPs). And just like CDPs, DMPs also use the data they collect to build detailed cus-

tomer profiles that drive targeted advertising and personalisation initiatives. The **main difference** is that **CDPs use primarily first-party data**, whereas **DMPs mostly use third-party data**. The latter already partly is and will be unavailable with the loss of third-party cookies. Also, DMPs deal with **customer profile and transaction data**, not personal data as such in the way **personal data is used and processed in CDPs.**

DSA

The European Commission and the European Parliament reached consensus on the **Digital Services Act** on April 23, 2022. The DSA establishes accountability standards for online platforms regarding illegal and harmful content, such as disinformation. When it will come into force, even as early as 2024, it will have a significant impact on every social network, search engine, and online marketplace that does business in the EU. Together with the Digital Markets Act (DMA), it creates the Digital Services Act package.

DSP

Demand Side Platforms are automation aided types of software via which advertisers can buy advertising. Once an advertiser has uploaded creative, set up targeting, and defined a budget for the campaign, the DSP makes bids that fit the advertiser's criteria on its network of publishers' sites and mobile apps. Some DSP examples are Meta Ads Manager, Amazon Advertising Platform (AAP), and BrightRoll.

EPD/ePD

The **ePrivacy Directive** regulates cookie usage, data minimisation, unsolicited email marketing, and other data privacy aspects. The full official name is "Privacy and Electronic Communications Directive 2002/58/EC". It was passed in 2002, and amended in 2009. Like other EU directives, it is not a binding law. Directives are instructions to EU member countries to create their own legislation in alignment with the directives. ePD will be replaced by the ePR in the future.

EPR/ePR

The **ePrivacy Regulation** will regulate the use of electronic communications services within the EU. It will replace the ePrivacy Directive (ePD). Its difference from GDPR is that it regulates electronic communication even when it concerns non-personal data, whereas GDPR only applies to the processing of personal data.

GDPR

The **General Data Protection Regulation** (EU) is the regulation in EU law on data protection and privacy in the European Union and the European Economic Area (EEA). It is an important component of EU data protection law and of human rights law. The GDPR's aim is to enhance an individual's

control and right over their personal data. It also addresses the transfer of personal data outside the EU and EEA areas. The GDPR became enforceable on May 25th, 2018.

Omnibus Directive

The Omnibus Directive, also known as part of **the New Deal** for EU consumers and more officially as the "Enforcement and Modernisation Directive", expands consumer protection laws in the EU to keep up with changes in the market. The Omnibus Directive extends traditional consumer rights to include all digital transactions. In practice, the directive means the right to withdraw from a transaction within 14 days, the right to receive vital pre-contractual information, and protection from fake online reviews. The directive has been in effect in national legislation since 28th May 2022.

Privacy Shield

The EU - U.S. Privacy Shield was a legal framework for regulating transatlantic exchanges of personal data for commercial purposes between the EU and the U.S. However, it was invalidated on 16th July 2020, because U.S. law gives U.S. authorities the right to collect personal data about EU data subjects (identifiable individuals) without adequate safeguards.

SCC

SCCs are **Standard Contractual Clauses**. There are two standard sets of contractual terms and conditions to consider under the GDPR: one for the processing of personal information between data controllers and data processors, and one for the transfer of personal information outside of the European Union (so-called Third Countries).

This whitepaper has been written to the best of our knowledge, but it should not be considered a substitute for professional legal advice.

Publishing Date: 30th August 2023

Contact: www.custobar.com, info@custobar.com