bloomreach

Don’t panic!

A marketer’s guide to **customer data security**

Contents

Introduction

Introduction

You've done all of your research, spent hours going through different options, seen an amazing demo, and are finally ready to purchase your customer data platform.

But one last step looms...final approval. Make sure that you are armed with information you need to prove that your CDP is safe and secure.

Our e-book "Don't panic: A marketer's guide to customer data security" will help educate marketers on why security is so important right now and give them the proper tools to help ease the nerves of risk-averse colleagues who may not fully understand the benefits of a CDP.

With data privacy fines on the rise and customers being more concerned about their personal data than ever, privacy and security is no longer something that marketers can put on the back burner. Customer data must be cared for cautiously and steps must be taken to protect companies from security breaches and hacks.

But how? And isn't this somebody else's job?

In 2021, data privacy and security is every employee's job. Especially marketers, who are working with customer data day in and day out.

This e-book takes a deep dive on current governing laws, protecting customer data, how Bloomreach helps keep companies secure, and so much more. It will give marketers the information they need to work appropriately with customer data to ensure they aren't the cause of a data breach or another security issue.

2

Modern Security Standards

Modern Security Standards

Consumers have made one thing clear over the past few years: they want more transparency from companies and control over how their personal data is being collected and stored.

That means, among other things, that the time is now for marketers to begin keeping security in mind in all things they do.

But how do you just begin to "keep security in mind"? You must first have an understanding of what the laws in each part of the world specifically require.

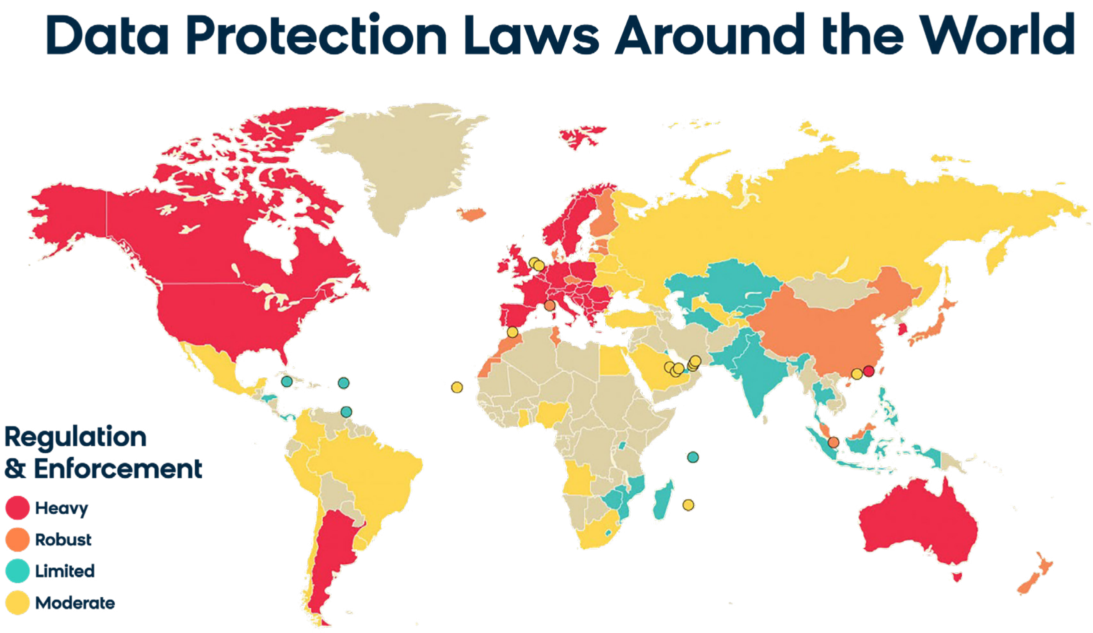


Image credit: TBS News

Why should marketers invest into knowledge about best practices?

Before diving into specific laws in countries across the world, it's important to understand why this topic even matters for marketers.

For years, it was the responsibility of members of the IT team or another department focused only on security to deal with privacy issues.

Those days are over. It is now every employee's job in some way, shape or form to be aware of security and data privacy concerns. This includes marketers.

Why is this the case? A simple case of meeting the demands of customers.

According to the RSA Data Privacy & Security Report, 73 percent of survey respondents are more aware of data breaches compared to five years prior to the survey. Additionally, 62 percent of all respondents said they would blame the company for a breach, not the hacker.

One more eye-opening statistic: 50 percent of respondents said they would be more likely to shop with a company if it could prove that it takes data protection seriously.

Statistics like that make it easy to see why it's time for every employee at your company, including marketers, to be serious about security and data privacy.

Let's also examine a hypothetical situation. A marketer has important individual goals that directly correlate to company success, including helping to raise customer lifetime value, click rates, and conversion rates. Making even the smallest of improvements in those areas helps the marketer's business to generate more revenue.

But what if there is a stumble along the way? A data breach, or some type of incident in which private customer data leaks to a party that it shouldn't? Or even an issue where your company is collecting private information without securing the proper permission to do so. Not only could your business be dealing with fines in the millions, it could also be forced to completely rebuild all of the customer trust it has built up over the years.

All of that hard work done to build a loyal customer base can be gone in the blink of an eye. To ensure you have the knowledge to be in compliance with local regulations, let's dive into our list of laws and regulations. While this list is not exhaustive of all of the laws and regulations of the world, it will give you a good idea of general legal expectations and the surrounding topics of importance.

According to the RSA Data Privacy & Security Report, 73 percent of survey respondents are more aware of data breaches compared to five years prior to the survey.

Additionally, 62 percent of all respondents said they would blame the company for a breach, not the hacker.

bloomreach

GDPR

The General Data Protection Regulation (GDPR) is the legal framework that created guidelines for the collection and processing of personal information from individuals who live in the European Union (EU). Since GDPR guidelines apply to individuals who live in the EU, the regulation applies to any e-commerce store that has customers who live there, regardless of where the website is based. In simple terms, this means that GDPR restrictions must be minded by all websites that attract European visitors, even if they don't specifically have a target audience segment of EU residents.

Specifically, GDPR requires that websites notify visitors of what information is being collected from them when they are browsing the site. Users must explicitly agree to allowing their information to be gathered. There are several other required data-related disclosures from businesses, including mandatory reporting of a data breach.

The regulation came into full effect in May 2018. Since then, many notable companies have received GDPR fines for being in violation of the law, including Google and H&M in 2020.

It is a good idea for marketers to become fully familiar with GDPR to help their businesses avoid fines and to keep the trust of your customers.

If a marketer is using a customer data platform or preparing to, he or she has access to many customer data points and should be aware of GDPR compliant data collection, storage and deletion methods. This will create a peace of mind for customers and members of the in-house security team.

Collecting website cookies and newsletter opt ins and opt outs is now an essential thing for marketers to track to stay in compliance with GDPR. If customers don't want cookies tracked, don't collect data from them. If consumers opt out of receiving your weekly email newsletter, stop sending it.

Being fully compliant with GDPR is a massive undertaking for a company. It requires full understanding and cooperation from every department, particularly marketing.

Bloomreach has compiled a list of GDPR use cases that will be valuable to marketers.

Bloomreach also goes in-depth with GDPR resources for customers that can help in numerous different situations.

CCPA

The California Consumer Privacy Act (CCPA) is enforced by the office of California's Attorney General and helps to protect residents of California from consumer data misusage. It was the first law of its kind in the United States. CCPA applies to any business in the world that sells the PI of more than 50,000 California residents annually or has an annual gross revenue exceeding $25 million.

The CCPA gives consumers the right to opt out of having their data sold to a third party vendor. It also gives customers the right to request disclosure of previously collected data and the right to request the deletion of collected data.

CCPA also encompasses one of marketing's big buzzwords right now: cookies.

Cookies are considered unique identifiers and are a part of the CCPA's definition of personal information. This means that marketers must know what type (first party or third party) of cookies are being collected by their websites to ensure CCPA compliance.

If your business meets the CCPA compliance thresholds, you are liable for the personal information (including cookies) that you collect through your website from

California residents. Ensure that you are in compliance with CCPA by understanding what type of cookies your website uses and therefore what personal information you are collecting from visitors.

Bloomreach's Customer Data & Experience Platform is perfectly suited to handle CCPA legislation.

This overview of CCPA also helps to clarify specific questions about the law.

CPRA

The California Privacy Rights Act (CPRA) enhances CCPA and will put even more strict privacy guidelines in play once it fully goes into effect on January 1, 2023. It helps to align standards more with GDPR but there are some major differences as well.

One big one? The right to opt out of automated decision-making technology, including "profiling". This is in connection with decisions related to a consumer's work performance, economic situation, health, behavior, location, or other personal preferences. Consumers must now be given the option of "opting out" of sharing the above types of personal data with third parties.

Among other things, the CPRA also introduces "sensitive personal information" as a new regulated data set for marketers to be aware of. Sensitive PI includes race, ethnicity, religious beliefs, genetic data, and other similarly private data. The CPRA also increases the rights of children and requires a new opt-in consent to share the PI of customers under the age of 16 with a third party.

Marketers should be very aware of the specific rules surrounding CPRA opt outs. Opt out rights explicitly extend to the sharing of personal information used for marketing purposes.

KARMA.

This act also establishes a governing body that holds the job of enforcing the guidelines of the act. This governing body can levy fines against businesses for failing to comply. Monetary amounts of fines are similar to CCPA ($2,500-$7,500) but can be increased when the personal information of a minor is involved.

The bottom line here? If you know CCPA, it's time to learn CPRA as well. Enforcement is right around the corner and there are new areas of consumer data that are protected by this new act.

Compare the CCPA and CPRA and learn how your company can stay in compliance.

Here's one more quick look at CPRA for good measure.

LGPD

Brazil’s Lei Geral de Proteção de Dados (LGPD) came into effect in February 2020 and protects the personal data of Brazilian citizens. It is very similar to GDPR in many ways but also differs as well.

Like GDPR, the nation in which a business is housed is irrelevant to this law. If doing business with a Brazilian citizen, you are required to follow the law. LGPD also has many of the same specific data protection points of GDPR including a consumer’s right to access personal data and the right to revoke consent.

One big difference is that there is no written deadline for reporting data breaches. While GDPR requires a report to be made within 72 hours of discovery, LGPD just requires communication to take place in a “reasonable time period”. This certainly leaves more wiggle room for damage control if there were ever an issue.

Another major difference is that LGPD has more strict guidelines in regards to hiring a Data Protection Officer. The law is written as such so that any company who holds the personal data of a Brazilian citizen is required to employ a Data Protection Officer to protect that data.

An important thing for marketers to know about LGPD is that fines are less severe than GDPR fines. While GDPR fines can quickly climb to €20 million, fines generally top out around €11 million for LGPD. While that number is still one to be concerned about, these extreme fines are reserved for major companies that are in violation.

Generally speaking, if marketers understand GDPR, they have a good enough understanding of LGPD to safely operate. The differences between the two laws do not lie in areas that affect marketers every day.

Go in-depth on where these laws are the same and where they are different to ensure understanding.

You can also get a standalone look at LGPD, independent of GDPR.

CPPA

In late 2020, the Canadian federal government introduced the Consumer Privacy Protection Act (CPPA). The bill represents the first proposed changes to Canadian privacy laws in over 20 years. Specifically, the proposed law would strengthen protections for individuals from privacy loss due to failures and limitations of corporate consumer privacy measures.

CPPA would help bring Canada up to speed with the European Union and give it a comparable law to GDPR. This new proposed legislation clarifies the requirements of individuals consenting to sharing personal data and outlines specific information that a business must provide to customers before personal data can be collected.

Monetary fines of up to 25 million Canadian dollars would be in play for organizations who fail to be in compliance. That is on the extreme end, of course. In general, the CPPA would give customers more control over their personal data and more of an influence in how it is collected by companies.

The aligning of privacy laws in Canada and the European Union would be good news for marketers.

Why? Simplicity.

Passage of this law would allow privacy guidelines in Canada to be much more comparable to the EU. Currently, Canadian law is governed by the Personal Information Protection and Electronic Documents Act (PIPEDA), which is over 20 years old and provides very little in the way of modern privacy protection for Canadians.

The uniformity of Canadian and EU law will allow marketers to operate similarly with customers and businesses in each location.

Learn more about the CPPA and how it specifically aligns with GDPR.

3

Security Breaches and Incidents

Security breaches and incidents

In your role as a marketer for your company, you have surely seen the news reports about security breaches or other incidents related to security in your field and others.

Whether it's the leaked customer data, the ensuing process to "clean up" the incidents, or the gaudy fines levied to responsible businesses, it's become blatantly obvious that your company wants to avoid a security breach at all costs.

But what actually happens when there is a security breach or incident? The issue takes place, and then what follows it? What is the process like?

To encourage you to continue your diligence and attention to detail when working with customer data as a marketer, let's break down what a security breach actually looks like from the inside.

So grab your lucky rabbit's foot or put on your lucky socks (just to be safe!) and let's start by imagining a scenario that hopefully never happens to any business you ever work for.

A scary scenario

Your company's Chief Information Security Officer, Compliance Officer, or Data Protection Officer has been notified of a data breach. That individual then gathers additional information about the situation and determines that customer data is involved and there is a risk to your customers.

GDPR now requires the following question to be answered: **is the breach likely to result in a risk to individuals' rights and freedoms?**

Since the controller has already determined there is a risk to customers in our hypothetical situation, the answer here would be yes. If it were no, there would be no requirement to notify appropriate authorities and the breach would just need to be documented internally.

That question now leads to another required question: **is this a high risk scenario for the individuals involved?**

If yes, it is time to take the painful next step of notifying the affected parties (customers, partners, or other employees usually) so they can protect themselves accordingly. If no, the only notification requirement is to notify the competent supervisory authority.

After the proper notifications, it’s time to start picking up the pieces and doing damage control with key stakeholders. It’s also time to potentially invest in better staff training around security or a tool that helps track marketers’ actions to help prevent future issues.

And, exhale. While you hope to never find yourself in that situation, knowing the GDPR-required steps just in case can be nothing but helpful.

GDPR now requires the following question to be answered:
Is the breach likely to result in a risk to individuals' rights and freedoms?

bloomreach

Breaches don't always look alike

For the sake of our scenario, we did not define what the specific breach was. But it is important to note that all data breaches are not alike and cannot be treated as such.

For example, a marketer's laptop might be stolen out of the office over a long weekend. The appropriate response to this incident is largely determined by the contents of the laptop.

Did the laptop contain the personal data or information of customers or employees? Was there no data on the laptop at all? Was there data on the laptop but it was encrypted? The answers to these questions determine how your company must move forward with cleaning up and reporting this incident.

If data on the stolen laptop can be accessed by the thief, the incident needs to be reported to the appropriate parties. If the data is encrypted or was not on the laptop to begin with, just make a record of the incident internally.

Other examples of security incidents or data breaches include: a stolen USB drive, a cyber attack on an online service containing data, a ransomware attack, personal data being sent out accidentally, a direct marketing email being sent in the "to" or "cc" fields so the email addresses of other recipients can be seen, etc. Each of these situations must be handled by following the aforementioned steps in the original scenario.

These situations also must be handled quickly. According to GDPR, the Controller has 72 hours to report the incident to the appropriate authorities if the incident requires reporting. While that might sound like ample time, those 72 hours can go very quickly in a crisis.

Data breaches and/or security incidents can quickly become “all hands on deck” situations as it takes the effort of multiple groups of people to recover all of the necessary information needed to make the 72-hour reporting deadline.

Failing to comply can have serious consequences

What happens if you miss the 72-hour window? Bad things happen. Just ask Twitter.

Twitter was given a $546,000 fine for missing the 72-hour reporting window in January 2019 in an incident that disclosed users' private tweets. The fine was given by Ireland's Data Protection Commission in December 2020.

The main message for marketers in all of this? Be as careful as you can with customer data and do everything possible to avoid a security breach. Doing that, and working with our world-class Customer Data and Experience Platform (CDXP) will help you be as prepared as you can possibly be to combat security breaches and incidents.

bloomreach
The Digital
Experience
Platform
Purpose
for Co

4

Security and the Barrier it Provides to Saas Purchases

Security and the barrier it provides to SaaS purchases

Concerns about breaches and other areas of security are often the reason that marketers find themselves in lengthy discussions late in the sales process educating their colleagues about the importance of a customer data platform.

Why? Because non-marketers often have worries surrounding security and SaaS solutions.

Whether it's your company's CISO, IT Team members, or Data Protection Officer, there are often key stakeholders who might be apprehensive to adopt a customer data platform because of the required responsibility relating to customer data that comes with it.

How can you as a marketer go about facilitating a conversation that helps ease their nerves and gets you the CDP that you need?

Let's find out.

Why the concerns?

First, it's important for marketers to understand that their non-marketing colleagues should not be viewed as the actual barrier to CDP adaptation. You will need to work together with these colleagues once the CDP is purchased and there's no better time to start that process than the latter stages of the sales cycle.

View the situation as an opportunity to see things from their point of view, educate them on your point of view, and help them find the answers they need to their questions about security.

Start by seeing what they might see: a new software platform that might expose the company to potential breaches or incidents and a slew of laws that now must be closely followed. The CDP is also a platform they won't work with daily, so it might be difficult for some to factor its true value into this equation.

Or maybe, there's just a general lack of knowledge and a bit of unnecessary fear.

It's no secret that GDPR fines have skyrocketed lately. However, it is less well known that GDPR compliance can be achieved with proper staff training and a secure software.

It is important to listen to these opposing views and understand any specific concerns. As you know, the benefits of a good CDP are nearly endless for marketers. That's why understanding where your colleagues' concerns come from and helping to mitigate them is so important.

Help me get my CDP!

Alright, enough of the opposing opinion. How can you convince them that a customer data platform is safe, secure, and won't cause the problems many people think it will?

While we can't speak for other CDPs, this is very easy to do with Bloomreach's Customer Data and Experience Platform.

After acquiring the world's first GDPR certified SaaS company in Exponea, Bloomreach has made a commitment to security that few other SaaS companies have. We strive to be transparent about how we protect our clients' data and this has resulted in security and privacy being the highest priority for us in our day-to-day functions.

For any worries about potential breaches or incidents, Bloomreach's commitment to security can be seen through our security certifications that we currently hold:

- ISO 9001
- ISO 27001
- ISO 27017
- ISO 27018
- **ISO 22301**
- GDPR certification
- **SOC 2 (Type 1) Report**

Every employee is an essential part of the defense against security breaches. This includes developers, who receive instructions on clean coding and other important security-related information during their ongoing training.

In regards to concerns about staff training and compliance, Bloomreach can help there as well. The Exponea Academy features a "GDPR Best Practices" course that covers the basics of GDPR, customer data rights, and many other important topics. Having a detailed understanding of the law is the best way to stay compliant with it.

In the face of potential security vulnerabilities, Bloomreach is always improving the platform's security measures and updating with the newest cybersecurity innovations. We are constantly one step ahead of evolving data and regulatory frameworks.

5

The 90:10 Rule of Properly Training Marketers on Security

The 90:10 rule of properly training marketers on security

As you search the market for the perfect customer data platform for your company, it is essential to not only keep customer data security in mind, but also education and training as well.

The 90:10 cybersecurity rule helps illustrate perfectly why this is so important.

The 90:10 cybersecurity rule is simple: 90 percent of security measures rely on users and other stakeholders while 10 percent of security measures are technical in nature. In other words, 90 percent of security safeguards rely on the computer user to adhere to best practices while the other 10 percent lies with the security features of the CDP.

90% of security measures rely on users and other stakeholders

While only 10% of security countermeasures are technical

To put things in terms of a real-world example…some homeowners have an alarm system on their doors and windows to secure their house. However, if those doors and windows are not completely shut, or the alarm system on them is not activated, these security measures are useless.

This is comparable in many ways to the 90:10 rule and to Bloomreach's Customer Data and Experience Platform.

Just as you might teach a guest how to arm the alarm in your home, Bloomreach is constantly teaching customers how to properly address security concerns when they use the CDXP. Bloomreach offers companies individual consultancy hours for specific security concerns and the Exponea Academy hosts a "GDPR Best Practices" course that aims to change perspectives around and promote compliance with data protection laws.

But why is all of this important to marketers? A strong security program cannot be implemented without properly training marketers on threats, policies, and techniques to protect company assets.

Marketers must begin to understand just how much of the responsibility falls on them to keep customers' data secure.

As you now know, Bloomreach has a world-class platform with top-of-the-line security features. But if important data privacy rules are not followed while using the platform, working with customer data becomes more risky.

This is the illustration of the 90:10 rule that marketers must understand to protect customer data properly. The customer data platform will not do all of the security work for you. Marketers using the software must have an understanding of data privacy laws and work with the data compliantly to achieve an atmosphere of compliance for the company.

Here are three real-life examples where unfortunately compliance amongst marketers was not achieved and a large price was paid:

- In Italy, a £16.7 million fine was given to Wind Tre, a mobile telecommunications operator, for "unlawful direct marketing practices". These practices included creating confusing interfaces for users to give consent, using personal data without the consent of the data subject, and willfully ignoring data protection guidelines.

- Denmark hotel chain Arp-Hansen Hotel Group was fined over £147,000 when it was discovered that it was storing the personal data of over 500,000 people unnecessarily. This is a direct violation of GDPR. This fine was imposed despite there being no record of an actual data breach.

- A £1.24 million fine was levied on German health insurance organization AOK Baden-Wurttemberg in June 2020. It was determined that the company sent marketing messages to 500 people without consent because proper measures were not taken to protect personal data.

The goal of buyers in the market for a customer data platform is to find the best CDP for their company. They're looking for a platform with not only great product capabilities, but with security features that support the outstanding features used every day.

But what also must come along with this purchase is the education and training of marketers to ensure that this software is used in a manner that is compliant with the law. The 90:10 rule emphasizes the importance of this education and training and helps to educate marketers that the responsibility of securely using a CDP will fall on them when the time comes.

90
10

Customers and their Rights with Personal Data

Customers and their rights with personal data

It’s important to understand your CDP will eventually be the home of a massive amount of customer data, if it is not already.

Gartner defines a customer data platform as “a marketing system that unifies a company’s customer data from marketing and other channels to enable customer modeling and optimizing the timing and targeting of messages and offers.”

As the cliche goes, “with great power, comes great responsibility”. It is the responsibility of marketers to care for that aforementioned unified customer data and ensure that customers are afforded all of their rights the law requires when it comes to their data.

But what rights do customers have when it comes to their personal data? Let’s take a deep dive into answering this question so that your company can be prepared if you receive a request related to customer data.

Customer data requests: An overview

Before going into detail about requests, the importance of having a specific process for customers to make these requests must be discussed.

Companies would be best served to have a specific channel (most commonly email) where customers should send requests. This should be communicated to customers through your company's privacy policy so there is no confusion when a customer decides to make a data request.

Companies are responsible for responding appropriately to all requests, even if a customer does not use the correct channel to communicate the request. Requests should be archived with the date they were made.

The General Data Protection Regulation (as well as other governing laws/guidelines) requires that responses are made to customers within 30 days (or 45 under the California Consumer Protection Act) of receipt of the request.

The goal of buyers in the market for a customer data platform is to find the best CDP for their company.

They're looking for a platform with not only great product capabilities, but with security features that support the outstanding features used every day.

bloomreach

What could customers actually be asking your company for?

Right of Access

This type of request generally involves three things: confirmation that you hold an individual's personal data, access to all the data that you hold, and/or other questions related to the gathering and storage of this data.

Customers making this request oftentimes just want to know what personal data your company holds that belongs to them.

Right of Data Portability

This right allows customers to obtain their personal data from your company and reuse it. It essentially allows customers to transfer or move data from one IT environment to another safely. The data should be provided to customers in a way that does not affect its usability.

Right to Rectification

Customers have the right to request that their incorrect or incomplete data be corrected. If there is found to be incomplete or incorrect data on a customer in your system, you must meet the 30-day deadline to correct this if the customer does make this request.

A good practice for certain companies in delicate situations would be to take an extra step to confirm the identity of the individual making the request to ensure the data isn't being manipulated. It is important to log all communication related to requests for rectification in order to avoid potential miscommunications with customers or GDPR issues.

Right to Erasure

Your customers do have the right to have all of their data completely erased from your CDP in certain circumstances.

Generally speaking, you have two options on how to move forward: anonymize the customer in your CDP or delete the individual completely. Deleting completely is the safer option in regards to GDPR.

Unlike the previous rights, this right is not absolute, meaning it does not apply in all situations and you need to always check particular circumstances to determine whether data might be erased.

The right to erasure will definitely apply if a customer's data is no longer necessary for the purpose for which you collected it or you are processing the data for direct marketing purposes and the individual never consented to that.

Right to Restrict Processing

This right essentially gives customers the right to limit the ways that companies can use their data temporarily. This is typically done in lieu of requesting a full erasure of data.

Like erasure, this is not an absolute right and only applies in certain circumstances. When processing is restricted, companies are permitted to continue storing the data in question but cannot use it.

Right to Object

Finally, customers also have the right to permanently stop you from processing their data in certain circumstances.

The absolute right in this case involves individuals' rights to stop their personal data being used for direct marketing purposes. In other cases, customers must show they have a "compelling reason" for a company to stop processing their personal data.

The request can be in regards to all of a customer's data or just a certain portion of data held by your company. It can also relate to a specific purpose or reason you are processing the data.

7

Owning Customer Data in a Cookieless World

Owning customer data in a cookieless world

The days of relying on third party cookies and third party tracking to supplement marketing campaigns are over.

In response to the aforementioned legislation, Safari, Chrome, and Firefox have each updated their tracking prevention for businesses and users in 2021.

The cliff notes? Cookie-based tracking is a goner. Campaign cookies in certain browsers are now limited to a 24-hour life span, much less time than any marketer wants. Others in different browsers can last up to seven days. Cookies can no longer be relied upon for what they used to be.

As the “cookie crumbles”, how can you take ownership of your customer data? How can a customer data platform help you deal with these changes and better shape your company’s future?

Great questions. Let’s explore.

Own your customer data so it doesn't own you

Safari's Intelligent Tracking Prevention, Mozilla's Enhanced Tracking Prevention, and Google's Privacy Sandbox are the main culprits as to why marketers have lost the benefits they once had with cookies.

But the funerals for third party cookies and third party tracking weren't overly sad ones. While responsible marketers could use that information effectively, there was too much power held by irresponsible marketers thanks to that data. Future users of these browsers should have far less concerns about being surveilled without granting companies' permission to do so.

A response to different worldwide legislations, ITP, ETP, and PS are their respective parent companies' attempts to give an increased sense of security to browsing users.

One thing has been made clear: companies need to take responsibility and own all collected customer data. Previously, businesses could rely on pixels and trackers to reliably measure conversions, purchases, and other actions customers took on their website.

That reliability is gone now. No longer will your campaigns be able to identify a purchase that happened more than seven days after the ad click (or 24 hours in some browsers).

That means your campaign performance will suffer. Facebook recently shared that costs per conversion can go up more than 150% for campaigns that lose access to the conversion data.

Where ad platforms conveniently offered businesses ready-to-purchase segments before, they will now need to develop a different analytics strategy. As a result, companies will no longer be able to afford not collecting, storing, and securing customer data themselves.

And the best way to collect, store, secure, and effectively use that customer data than with a customer data platform.

Having a good CDP is more important than ever

If a brand is going to completely own its customer data, it should not be on its own in doing so. It needs a customer data platform to assist in compiling, storing, and enriching that data.

A core feature of any good CDP is a single customer view. This is the place where all customer interactions with your brand are recorded. This is also the place where you should have the information that was previously tracked by third party trackers.

But that's not where it ends. You can also connect a CDP to your internal systems, for example a retail loyalty system. This will allow you to measure the impact of your marketing even on offline customer behavior.

As advertising giants adapt, you are able to share the conversion data with them in new ways.

One example is the Facebook Conversions API. With a CDP, you can use these new tools to optimize campaigns even for conversions that don't happen on your website, such as store visits or predicted purchases.

Maybe most importantly, a good CDP can also ensure that your data is stored in a secure manner and respects customers' privacy consents. With GDPR fines soaring, the time is now for businesses to begin taking extra special care of collected customer data.

We're hoping it's obvious that now is not time to mourn the crumbling cookie. It's time to take decisive action and develop a data strategy that will enable you to succeed in the post-cookie world.

Bloomreach is the right choice for a post-cookie world

But you don't just want any CDP.

Bloomreach's Customer Data and Experience Platform is the highest rated Customer Data Platform according to independent review site G2. The CDXP will allow you to unify all of your customer data and deliver top notch customer experiences, all with a single solution.

With the cookie reduced to mere crumbs, it's time for your business to get our top notch CDXP that is safe and secure.

Bloomreach’s Six Guiding Principles that Will Help Secure Customer Data

Bloomreach’s six guiding principles that will help secure customer data

Customer data protection should be prioritized more than ever in 2021.

With data breaches on the rise and non-compliance fines ballooning, the time is now for businesses to start paying more attention to securing collected customer data.

But how? To help, Bloomreach has created six guiding principles that will help your company keep customer data secure and stay out of harm’s way in the eyes of the law.

Without further ado, it’s time to HOLD’EM Secure.

6 Privacy Principles – Hold’em Secure

Honesty	Be clear about what you collect and why.
Obedience	Seek your customers’ consent and respect their requests.
Legality	Stay within legal limits.
Defense	Defend data from anyone and anything.
Exactness	Maintain data accurately and keep it up to date.
Minimization	Keep only what you need.

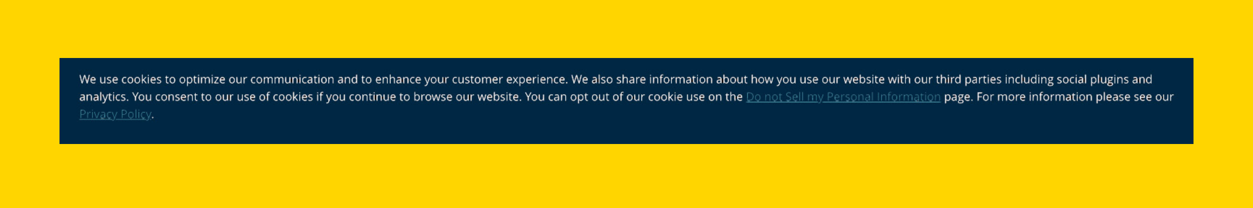
The acronym that illustrates the above six principles will help guide your company with customer data security and help it to avoid any potential consequences with governing laws. Let's look deeper at each statement.

Honesty

Be clear about what you collect and why. A simple principle that can have severe consequences when not followed.

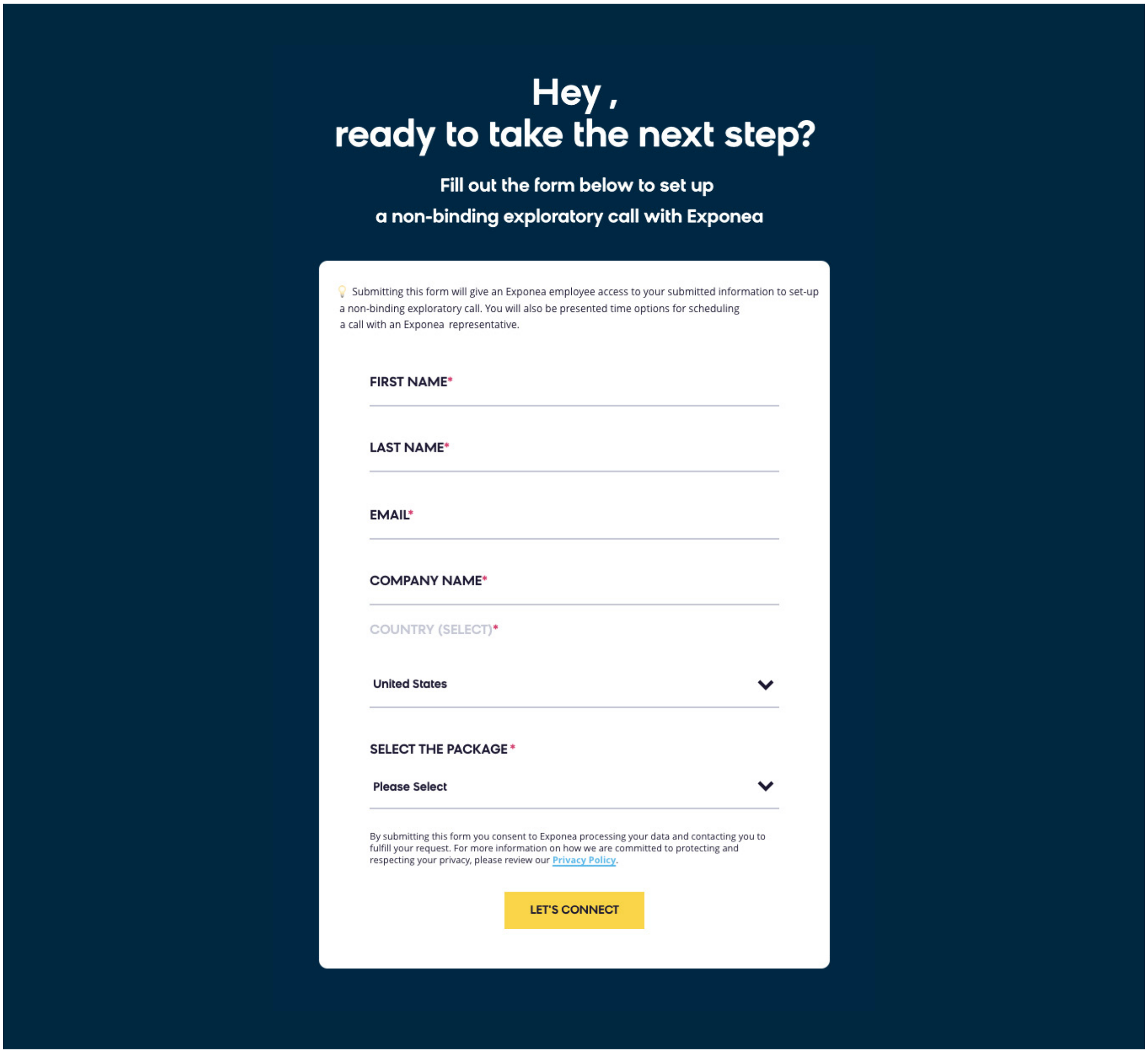
To be specific, be clear about the personal data you are collecting from your customers, how you are collecting, and why it is necessary for your company to obtain it. Honesty truly is the best policy when collecting customer data.

How can this be done? Maybe most importantly, when asking customers to accept or decline cookies. It is important to clearly communicate the purpose of your website's cookies, who else you will be sharing the collected information with, and exactly how a customer can opt out of being tracked.



We use cookies to optimize our communication and to enhance your customer experience. We also share information about how you use our website with our third parties including social plugins and analytics. You consent to our use of cookies if you continue to browse our website. You can opt out of our cookie use on the Do not Sell my Personal Information page. For more information please see our Privacy Policy.

The same principles apply when collecting information for the purpose of taking a next step with your company.



Hey ,
ready to take the next step?

Fill out the form below to set up
a non-binding exploratory call with Exponea

💡 Submitting this form will give an Exponea employee access to your submitted information to set-up a non-binding exploratory call. You will also be presented time options for scheduling a call with an Exponea representative.

FIRST NAME*

LAST NAME*

EMAIL*

COMPANY NAME*

COUNTRY (SELECT)*

United States ⌄

SELECT THE PACKAGE *

Please Select ⌄

By submitting this form you consent to Exponea processing your data and contacting you to fulfill your request. For more information on how we are committed to protecting and respecting your privacy, please review our Privacy Policy.

Best practice is to only collect necessary information for the next step to take place. It is also best to be forthright about what steps will happen for customers when they complete the required or suggested actions.

All in all, it’s just best not to be sneaky. Penalties can be severe if caught.

Google was fined $56.6 million in 2020 because it “should have provided more information to users in consent policies and granted them more control over how their personal data is processed”. A steep price to pay for not being forthright about data collection methods.

Obedience

Seek your customers’ consent and respect their requests. Online success is all about consent.

The goal is not to figure out ways of tracking, targeting, and marketing to your customers without their knowledge. The goal should be to offer your customers an experience worth giving you all of the necessary consent to get that experience.

Make them love the personalisation and they will be happy to provide the data. Truly a win-win scenario.

Things can be bad for companies who are not obedient. Amazon France was given a $42 million fine in 2020 for tracking users without prior consent.

Legality

Stay within legal limits.

While the law differs in different corners of the globe, it basically requires the same thing of every company: take precious care of your customers' data.

One important thing to remember: even though your company is not headquartered or located in the country enforcing a particular law, it can still be held accountable for following that law. This is because the internet connects the entire world with just a few clicks and your company very well may have customers from countries with strict data protection laws.

It's best to have an understanding of these laws and govern your internal actions accordingly. You can end up receiving a fine like Marriott did if not.

Marriott was fined £99 million for failing to comply with multiple GDPR rules.

Defense

Defend data from anyone and anything.

To borrow a sports cliche: "the best offense is a great defense". True in athletic competition and true in customer data collection as well.

How, exactly? Well, in this case, defense is protecting your customer data and offense is the many marketing campaigns that you can carry out once you have healthy customer data.

The marketing campaigns are useless without ample amounts of legally obtained customer data. Therefore, everything starts with customer data and it must be protected as such.

Protecting customer data is easy with Bloomreach's Customer Data and Experience Platform. The CDXP securely compiles siloed customer data from every corner of your company so that you can connect with customers via marketing automation techniques that meet them at whatever stage of the customer journey they are at.

The risks are high if your defense of data is not up to par. British Airways received a £183 million fine for failing to put enough security measures in place.

Be clear about what you collect and why.

A simple principle that can have severe consequences when not followed.

Exactness

Maintain data accurately and keep it up to date.

Your company is responsible for the actions that happen after data has been collected. Wrong data can have a wide variety of negative consequences.

For example, a wrong salutation in an email lowers your chances of being a loved brand. But a consent management issue can earn you a multi-million dollar fine by the data protection authorities.

You should sanitize your mailing list regularly, not use unlimited time consents, and assess your data structure before trying a new use case. Testing your website and systems from time to time on your own is also good practice.

According to GDPR, customers have the right to request that companies update their personal data when they believe it might be incorrect. But waiting for a customer to make this specific request is not best practice when you have a hunch that data needs to be corrected.

Italian telecommunications operator TIM was fined €27.8 million in 2020. One of the reasons for the fine was improper management of consent lists.

Minimization

Keep only what you need.

Customers are going to shop with brands that they can trust. Do not “spy” on your customers by collecting masses of useless data.

Instead, collect the necessary data to personalize their experience and explain to them the reasoning behind why the data needs to be collected.

Knowing that a person is a millennial, likes nice shirts, and makes a new purchase every month has the same value for you as knowing that the person was born on a certain date, takes photos of their nice shirts on their private Instagram, and gets their salary paid on the first day of every month.

But for the customer, keeping the second set of personal information private makes all the difference in the world.

Additionally, there is no reason to keep data once you have no use for it. Not only are you risking a data leak, the data will likely not be as useful for you in the future as you might think.

Customers’ behavior changes quickly so what might have been relevant last year might not be relevant this year. Make some analysis of the data, keep the statistics, and once you are done, dispose of the data in a secure way.

Danish furniture company IDDesign received a fine of nearly €150,000 for possessing the personal data of customers for a longer time than was necessary.

Don’t let this happen to your company.

How Bloomreach's SmartSecure can Protect your Company from Security Breaches

How Bloomreach's SmartSecure can protect your company from security breaches

A data breach is something that your company wants to avoid at all costs.

Data breaches have serious consequences and their effects can linger long after the incident. They can also be a huge financial burden to companies.

In fact, a data breach on average costs affected companies £3.5 million when all is said and done.

Bloomreach understands the value of data privacy and security and has created a solution that will ease the nerves of any stakeholder with a vested interest in those important topics.

Let's be sure to start here: the CDXP is secure on its own.

The goal is to be transparent in how we protect our clients' data and this has resulted in security and privacy being held to the highest priority in day-to-day business functions.

That said, the CDXP is a very powerful tool. With great power, comes great responsibility. Large datasets and complicated data structures can be put at risk if they are not used as they are supposed to be.

SmartSecure is a monthly security assessment of your account that searches for common vulnerabilities and bad application usage practices. Once per month, a report that details the aforementioned things is sent to key stakeholders at your company to help mold future best practices when using the CDXP.

The report also includes recommendations on how to improve and mitigate risks or incidents.

SmartSecure will help you mitigate dangerous risks such as data leakage or loss and help completely avoid bad data practices and poor data management.

The increased layer of security of collected customer data will result in an even further elevated level of trust between your customers and your business and will lead to enhanced customer loyalty.

Specifically, the monthly compliance report will cover:

- Authorization settings
- Logs of activity where personally identifiable information was accessed
- Suspicious logins
- Usage of GDPR features
- Suggested usage of other features

Remember that £3.5 million average data breach fine? SmartSecure will help your business steer clear of GDPR and other issues with compliance.

Who is SmartSecure for?

Any current CDXP user or future user can benefit from SmartSecure. But which individuals at these companies would actually benefit?

- **Your company's leadership.** When you aren't using the platform every day, you are less familiar with how the CDXP works. SmartSecure is an excellent security blanket (pun intended) for company leaders so they can be confident in those who use the platform inside their company and be reassured that the platform is being used as intended.

- **DPOs, CISOs, and other security operations team members.** If you ask these folks if they would like a second set of eyes to help monitor activity, most would say yes without hesitation. SmartSecure will help save these employees time and help to prevent problems in the future by mitigating common risks.

- **Marketers.** SmartSecure will introduce guidelines and best practices to avoid bad usage and potential incidents for the marketers at your company.

SmartSecure checks data, projects, and campaigns to ensure compliance. Data checks include private data, data structure, and data exports while project monitoring includes access management and account management. Campaign checks will help ensure GDPR consent.

9:41
bloomreach
The Dig
Experie
Platf
Purp
for C
Powering 25% of All US & UK
eCommerce Experiences

10

How Proper Consent Management can Help Manage Customer Data

How proper consent management can help manage customer data

Whether it's for your customer data platform or a similar tool, it is important to have a comprehensive consent management plan that is easy for your customers to understand and compliant with necessary laws and regulations.

Keep reading for everything you could possibly need to know about consent management and how it will affect your company in 2021.

What is consent management?

Consent management is a system or process for allowing customers to determine what personal data they are willing to share with a business.

It has become so important worldwide because of the lawful requirement for websites to obtain user consent for collecting data through cookies while browsing. Businesses all across the world are now responsible for collecting and managing customer consent.

Exponea breaks things down into three consent categories that make up consent management: general consent, consent, and legitimate interest. These must be considered before embarking on marketing campaigns or email communication efforts.

What consent management really boils down to is this: it is a process that guides compliance by informing users about data collection and usage practices. A good consent management process logs and tracks consent collection so that companies do not need to worry about being in compliance with worldwide laws and regulations. It also of course facilitates the collection of consent.

What is the difference between consent and preference management?

While consent management and preference management might sound the same, there are very distinct and important differences between the two. Both are critical parts of creating a privacy first and customer-centric strategy but it is important for businesses to understand the difference between the two concepts.

Marketers ask for customer consent in the consent management process to do things like collect, store, and process personal data. The data is then of course used for marketing campaigns like retargeting and email campaigns.

Consent collection is also commonly known as "subscribing" or "opting in" to receiving communications from a company. If customers no longer want to hear from a company, they would change their "opt in" to an "opt out" and revoke consent for marketing communications.

Consent management governs this collection of customer wishes and ensures that companies are staying compliant by not contacting customers who do not wish to be contacted any longer.

While it might sound similar, preference management actually refers to giving users the ability to make choices about the frequency of communication, topics, and which channels they'd like to receive communications on.

While preference management is important, consent management is the topic at hand and it is important to understand when you must collect consent from customers.

When should you use consent management?

According to GDPR, consent is one of six lawful bases to process customer data.

In most situations, the most optimal way for a business to process customers' data is to obtain consent. However, should that not be an option, GDPR does allow five other ways for a business to process customer data. They are:

- **Performance of contract.** If your business is providing a good or a service to a customer, for processing of customer's data that you need for the performance of such a contract, the contract is the legal basis you rely on rather than consent. For example, if a customer orders a t-shirt from your e-commerce store, your business will need the customer's address to deliver the t-shirt and complete the order process. The customer does not need to explicitly consent to the processing of delivery data as the contract in place covers it.

- **Performance of public tasks.** Authorities performing duties that are within their everyday job descriptions do not need to comply with these consent management standards when they carry out tasks in the public interest or exercise official authority. However, unless you work for the government, the police, a hospital, or a school, it is likely this basis does not apply to you.

- **Legitimate interest.** This basis involves some gray areas. Your company may process customer data without consent when there is a "genuine reason" to do so. What that specifically means is up for legal interpretation and has already been debated in court.

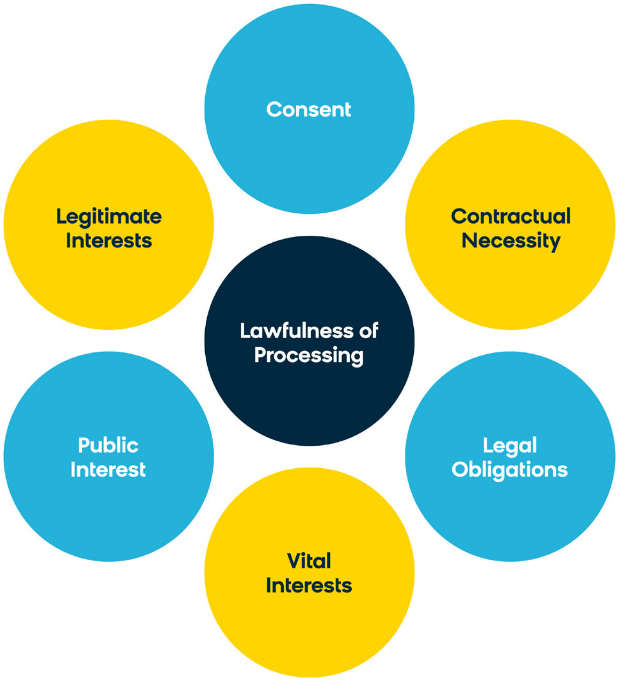
- **Vital interest.** If processing customer data is essential in the act of saving someone's life, such processing is legally mandated under GDPR. Again, this does not apply to your everyday e-commerce business.

- **Legal obligation.** This basis applies when processing a particular type of data is legally mandated. An example here would be criminal records.

While preference management is important, consent management is the topic at hand and it is important to understand when you must collect consent from customers.

GDPR Lawfulness Personal Data Processing

Legal grounds and lawful basis - processing lawful it at least one of legal bases below



Consent

The consent of a data subject to the processiong of his/her personal data

Contractual necessity

Processing is needed in order to enter into or perform a contract

Legitimate interest

There is a weighed & balanced legitimate interest where processing is needed and the interest is not overriden by others

Legal obligations

The controller is obliged to process personal data for a legal obligation

Public interest

Public authorities and organizations in the scope of public duties and interest

Vital interests

Public authorities and organizations in the scope of public duties and interest

Many of these bases do not apply to typical e-commerce stores. Any business that is not referenced amongst the above exceptions lands right back where we started this discussion: it must obtain consent to legally process customers' data.

Why does consent management matter?

The million dollar question. Quite literally, for some companies.

Consent management can seem like a big hassle and additional work that can be alleviated if the consent management process is just ignored, right?

Ignore consent management at your own risk. GDPR fines have skyrocketed over the past year as customers have begun to care much more deeply about businesses having their personal data.

GDPR fines can reach £20 million or 4% of the annual global turnover of a company for certain infractions. Here are two examples of GDPR fines that could have been avoided if these business had a better consent management plan in place:

Companies won't just feel the pain of these incidents financially. The "clean up process" from a GDPR fine includes not only fixing the issue a company was fined for, but also earning back the trust of customers who now see the affected brand in a negative light.

That process is easy for some customers and difficult for others. Take the necessary steps of having a reliable consent management program in place to avoid potentially large fines and the decreased customer loyalty that may come with those fines.

Consent management and compliance

Now that you know that it can be disastrous to not be in compliance, how specifically can your business stay compliant with GDPR when it comes to consent?

Article seven of GDPR outlines all of the required conditions for consent and lays out exactly how companies are to stay compliant in this regard.

Here is a brief summary of article seven to save you some technical reading:

- When collecting and processing a customer's data based on consent, your company must be able to prove that the customer has consented.

- If the customer's data consent is given in a written declaration that also concerns other matters, the request for consent must be presented in a manner that is easily distinguishable from the other matters.

- The customer has the right to withdraw consent at any time. This will have no effect on the lawfulness of processing prior to consent being withdrawn. The withdrawal of consent should be as easy as the collection for customers. If consent is given with one click, customers should be able to take it away with one click as well.

- When assessing whether consent is freely given, utmost account shall be taken of whether the performance of a contract is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

As the law changes, and new regulations pop up in different corners of the world, the consent process will change as well. That's why it is so important to have a partner like Exponea, the world's first GDPR certified SaaS company, on your team keeping you up to date on all things consent management.

Conclusion

Conclusion

This e-book touched briefly on a lot of topics that it is important for marketers to have a working knowledge of.

What's more important is that you have the right team in your corner helping to make sure that you are taking proper care of customer data and doing all you can to avoid security breaches.

Bloomreach's commitment to security is unrivaled in the CDP space. Need proof? Exponea, a Bloomreach company, was the world's first GDPR certified SaaS company and holds top security certifications to ensure that our customers have full protection when using our platform.

If you are ready to see the CDXP in action, watch our short demo video and see how you can compliantly turn your customer data into marketing magic.

bloomreach

About Bloomreach

Bloomreach is the leader in commerce experience™. It's flagship product, brX, is the only digital experience platform built specifically for brands, retailers and B2B companies who want to grow their revenue online while delivering each of their customers a premium, personalized commerce experience. brX combines content management capabilities with market-leading commerce-specific, AI-driven search, merchandising and personalization in one flexible, API-first next generation platform.

Bloomreach serves over 500 global brands including:

BOSCH M&S next PUMA Virgin EXPERIENCE DAYS

For more information, visit Bloomreach.com, follow us on Twitter @Bloomreach_tm and on LinkedIn.

FIND OUT MORE

bloomreach