Embracing the Privacy Era:

GDPR and CRM

ZOHO CRM

zoho.com/crm

Embracing the Privacy Era:

GDPR and CRM

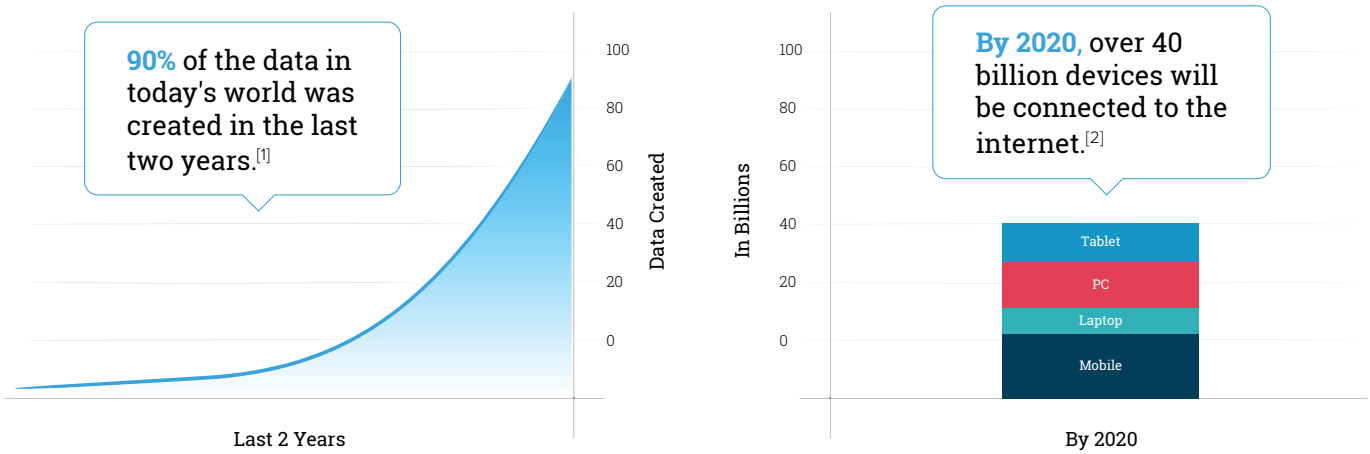
Author: **M.K. Shashank**

Table of Contents

The unending pursuit of customer data

In today's environment, where almost every device is connected to the internet and an untold amount of data is being generated by all these interconnected devices, any piece of customer information that can be found in this ever-expanding volume of data is a godsend for businesses and service providers.

Constant technological innovations have made it so that most of our online activities are documented. Our purchase history and financial transactions are digitized and kept within easy reach. When the power of machine learning is applied to this giant cauldron of customer information, patterns are recognized that help us predict customers' needs and the products/services they'd be willing to spend money on.



What does this mean for the customer?

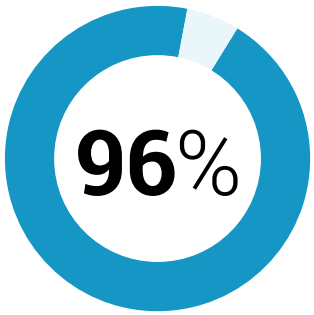
Personalization.

Customers these days crave a personalized experience when a business reaches out to them. Any organization that doesn't capitalize on customer data to provide personalization that suits the needs and tastes of their customers is getting left behind in the race.

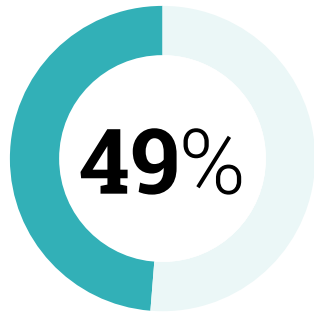
Conflict between personalization and data privacy

Collecting data is the cornerstone for providing a personalized experience to all your customers, but recently the practice has come under scrutiny and data privacy is becoming an issue of concern. A survey conducted by Verint Systems Inc[3]., with over 24,000 participants from all over the world, put the nature of the conflict on display.

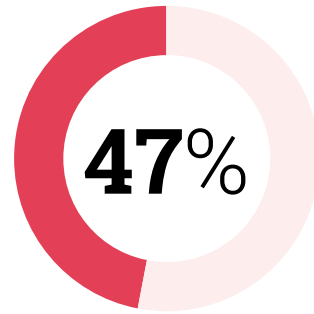
- Personalized service continued to be important. 80% of the consumers liked it when a service was personalized and tailored to their needs.
- At the same time, privacy was a big concern. 89% of the consumers felt it was vital to know how secure their personal information was.
- However, the study also showed these concerns were aligned with the concerns of businesses, which placed emphasis on data privacy (94%), personalization (95%) and resolving customer issues quickly (92%).



of consumers claim the security of their device is important. [4]



However, less than half of them take the proper security measures.



of them aren't sure of how to secure and protect their data.

The importance of data security and privacy

Data security and privacy are often used interchangeably, but they are not the same.
So let's break it down:

- Data privacy revolves around the lawful collection and usage of personal data.
- Data security is having the physical, technical and administrative safeguards in place to protect your customer's data.

Having an advanced security system in place doesn't mean much when the customer loses their say in how their data is being used. Even with the most stringent security system in place, there are chances of mismanagement by employees and third-party processors who have access to sensitive customer data and are unaware of your privacy policies.

There is no shortage of data breaches that put the personal information of millions at risk. A quick glance through the Breach Level Index[6] site gives you an idea of the severity of these attacks.

> 74% of consumers in the United States of America want organizations to be transparent about how personal data is used.[5]

YAHOO!

This breach, which happened in 2013, affected around 3 billion users. Let that number sink in. Every single Yahoo account that existed in 2013 was compromised in the breach and it took Yahoo 3 years to report it. [7]

EQUIFAX

One of the largest consumer credit reporting organizations suffered a breach which left 148 million customers affected. The information stolen included names, addresses, and even social security numbers of Equifax customers. [9]

UBER

This renowned ride-sharing company suffered a data breach in 2016, wherein 57 million users were affected, including drivers and customers. The hackers got ahold of personal information including names, email addresses, and residential addresses. Uber hid the incident and paid a $100,000 ransom to get the hackers to delete the data. The breach only became public knowledge in 2017 during an investigation into Uber's business practices.[8]

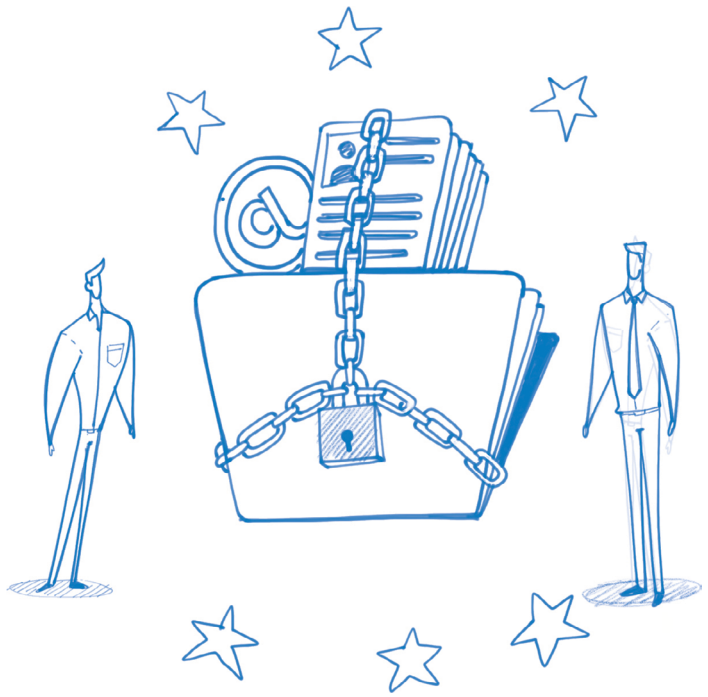
Where there are concerns for data security, concerns for data privacy surely follow because security and privacy are two sides of the same coin.

Concerns for data privacy haven't been unfounded, considering the recent revelation of how Cambridge Analytica[10] leveraged the data collected from over 50 million Facebook users to influence the 2016 US Presidential election. Questions are being raised as to the extent to which data-driven organizations leverage their customers' private data for monetary gains.

> Every day, major organizations across the globe experience 20 data loss incidents on average.[11]

GDPR

To people worried about the security and privacy of their personal information, a privacy regulation like GDPR is a welcome change.



GDPR, or the General Data Protection Regulation, is a landmark piece of legislation aimed at empowering citizens of the European Union with regards to their personal data. With the increasingly complex flow of information across the world, GDPR aims to give EU citizens more direct control over how their personal information is processed and help protect their data privacy.

Why was it introduced?

The previous data protection policy in the EU, called the Data Protection Directive or Directive 95/46/EC, was drafted in the 1990s. There have been significant social and technological developments since then, and there has been an evolution in the way personal data is used.

Another reason for the GDPR's introduction was to harmonize data protection law across the EU. The previous policy, being a directive, did not apply uniformly. National authorities in each member state implemented their own understanding of the directive, resulting in varied data protection compliance requirements across various EU member states.

The GDPR, as the name implies, is a regulation[12]. It is a legally binding rule which has to be enforced across the European Union, and organizations must do their best to abide by it. This will also help in making sure that organizations that are doing business in the EU, or hoping to, face a uniform compliance requirement across the entire region.

Who is affected?

> "Why should I worry about a law that is being enforced in the European Union? My business isn't based there."

That would be a wrong assumption with grave consequences. When GDPR went into effect on May 25 2018, every organization that is established in the EU or that handles the personal data of EU residents fell under the purview of GDPR. So whether your organization is based in the EU or does business with people in the European Union, you are required to demonstrate your compliance with GDPR.

GDPR 101

Customers' rights over their personal data are at the heart of GDPR. The regulation consists of 173 recitals and 99 articles aimed at establishing the privacy standards that every organization handling personal information of EU residents needs to meet.

Before we dive into GDPR, let's take a quick look at the important terms[13] you need to know:

- **Data controller:** Any person or organization that collects and stores the personal data of consumers, and decides how it is processed, is known as a data controller.
- **Processing:** Any act of collecting, storing, organizing, modifying, transmitting, disclosing, using, or erasing personal data of consumers is termed processing. In short, any usage of personal information for reasons other than "purely personal" is considered processing.
- **Data processor:** Any person or organization that processes personal data under the instruction of a controller is known as a data processor.
- **Sub-processor:** When a data processor engages another processor to delegate a part of the processing activity with permission from the controller, the second processor is known as a sub-processor.
- **Data subject:** Any person whose personal data is collected and processed is known as a data subject.

Core data protection principles:

The core principles of GDPR revolve around the lawful collection and processing of customer data under appropriate lawful bases. Article 5[14], which lays down the foundation for the collection and processing of personal data, can be summarized as follows:

- **Lawfulness, fairness and transparency:** Personal data should be processed lawfully and in a transparent manner. Organizations are required to be upfront about why the data is being collected and how it will be used.
- **Purpose limitation:** The purpose for collecting personal data should be explicitly stated and should be legitimate. Processing of personal data should be limited to the purpose stated during collection.
- **Data minimization:** The data collected should be adequate, relevant, and limited to the processing activities.
- **Accuracy:** Steps must be taken to ensure that personal data being processed is kept accurate and updated as necessary without delay.
- **Storage limitation:** The storage of personal data should be limited to the duration needed for the processing activities.
- **Integrity and confidentiality:** All processing activities must be performed with appropriate security measures to prevent accidental loss, damage or destruction of personal data.

Article (6)[15] defines instances when the processing of personal data is considered lawful. These include:

- **Consent:** Consent has been provided by your customer for one or more processing activities.
- **Contract:** Processing is required for contractual obligations or to meet customer requests (example: requesting a quote) before they enter into a contract with you.
- **Legal obligation:** You are obligated to process a customer's data to meet certain legal requirements.
- **Public interest:** You are processing the personal information of your customers in the interest of the general public.
- **Vital interest:** The processing of personal data is required to save someone's life.
- **Legitimate interest:** The processing is necessary for the legitimate interest of your organization and any involved third parties, as long as the processing doesn't breach the privacy of the customer involved.

Article (7)[16] states that if the lawful basis under which the processing occurs is consent, an organization must be able to demonstrate that a customer has consented to the processing of their information. The consent itself should be shown in easy-to-access form and written in clear and plain language.

One of the challenges faced by organizations trying to be GDPR compliant is documenting this consent and making provisions for customers to revise their consent at any moment.

In the GDPR era, organizations are required to be upfront about the purpose for which they collect customer data, while ensuring that all processing activities they perform have been consented to by the customer.

Data subject rights:

GDPR provides a slew of rights to EU residents[17] (data subjects) concerning their personal information.

- **Right to access:** The data subject has the right to obtain confirmation of processing done on their data and to access their personal information.
- **Right to rectification:** The data subject has the right to ensure that their personal information is accurate and updated as needed.
- **Right to erasure:** The data subject can have the organization erase all their personal information without any delay, unless the data is needed on contractual or legal grounds.
- **Right to object and restrict processing:** The data subject can object to the processing of their data and restrict it if they so desire.
- **Right to data portability:** The data subject has the right to obtain their information in a structured and machine-readable format or have their data transferred to another controller if feasible.

Data controller and processor responsibilities:

Data controllers and processors[18] collect, store, and process the personal information of customers. As part of their compliance process, they are required to:

- Have technical and organizational measures in place to ensure all processing activities are done according to regulation.
- Ensure that the measures in place are reviewed and updated when necessary.
- Adopt privacy by design and default.
- Appoint a representative in the EU if they do not have a presence there.
- Ensure a record of all processing activities is maintained.
- Keep the subject's data secure and maintain its integrity.
- If the processor decides to delegate part of the processing activity to another processor, known as a sub-processor, the customer needs to sign a contract with the sub-processor containing the same data protection obligations as the contract with the data processor.

The data controller must have a written agreement with the data processor, and it must specify the following provisions:

Data controller's written instructions:
data processor only processes personal information in accordance with the data controller's instruction unless required by law. If the law requires a processor to disclose the data controller must be duly notifiewd.

Processing details:
This includes the purpose of processing, the duration of data storage, the nature of processing activities, the type of personal data being processed, and the obligations of the data controller.

Duty of confidence:
This is a provision that requires everyone involved in the processing of customer data sign a confidentiality agreement with the data processor.

Security measures:
To ensure the security and integrity of personal information, the data processor must be subject to the same requirements as the data controller.

End of contract:
The data processor is required to delete or return all the personal data to the data controller at the end of the contract, unless the law requires them to retain the data.

Auditing and inspection:
The data processor must agree to undergo audits and inspection by the data controller, to ensure that all processing activities happen in accordance with the agreed-upon contract.

If there is a data breach, the data controller has to notify the appropriate authorities and data subjects affected. The controller is also required to carry out a data protection impact assessment if the processing activity carries with it the risk of compromising the rights and freedom of an EU resident.

If an organization is a public authority, or carries out processing activities which requires the monitoring of individuals on a large scale, it must appoint a Data Protection Officer.

Data security:

Data controllers and processors[19] may need to ensure that personal data is pseudonimysed and encrypted, based on the magnitude of risk involved with the exposure of such data. They must maintain confidentiality and integrity of personal information during processing activities.

Data controllers and processors must have a standard RTO (Recovery Time Objective) in place and have the ability to restore access to personal data in the event of a technical or physical incident.

They should also have a procedure to regularly test and evaluate the effectiveness of their technical and organizational security measures and policies.

Price of GDPR violation

Any organization found violating GDPR can incur a fine of up to 20 million Euros or 4% of its global annual turnover for the preceding financial year (whichever is higher). The price of non-compliance is high, even for a large multinational organization.

A Survey by **MarketingSignals.com** which involved around 1,000 UK workers, revealed the following:

17% stated that they still don't know what benefits GDPR offers.

Top 5 ways in which businesses are non-compliant with GDPR

35%

said that they still send marketing emails to customers without express consent.

31%

said that they have data of customers who haven't agreed to have their data stored.

27%

haven't secured the data that they have from ransomware attacks.

22%

evealed that they have a more drawn out process for customers choosing to opt out when compared to their opt-in process.

14%

have privacy-friendly choices that aren't visible to users.

When the law came into effect on May 25th 2018, it didn't take long for the hunt to begin. Austrian privacy activist Max Schrems, who was always critical of how companies coerced customers to fall in line with their data collection policies, filed complaints against IT behemoths Google and Facebook.

The complaints are aimed at the practices of all large tech companies that offer free services and in return leverage customer data for their profit. Three complaints worth €3.9 billion have been filed against Facebook, and another filed against Google is worth €3.7 billion. While the European Data Protection Authorities have promised to work with their Irish counterparts for the complaints as the EU headquarters of Facebook and Google are based in Dublin, we will have to wait to know how the latest privacy tug-of-war will end.

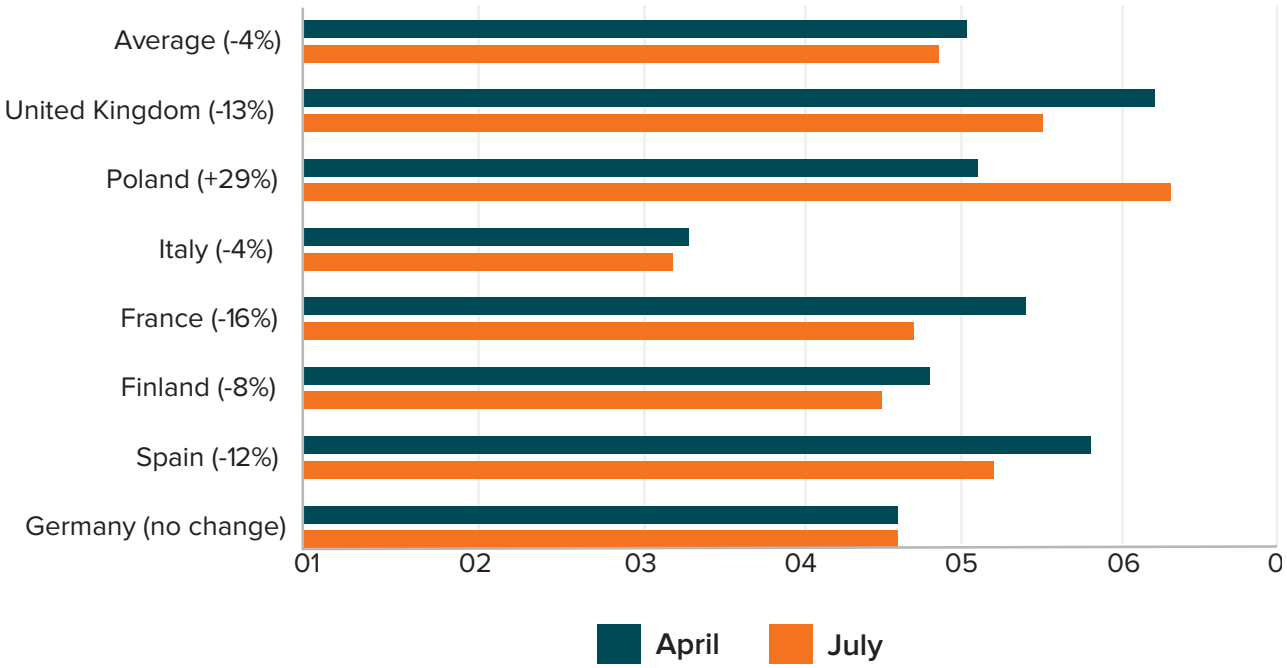
The impact of GDPR

Post the implementation of the GDPR, there have been a lot of changes in how organizations deal with personal information in all their business avenues. Let's take a look at 3 changes that became evident after GDPR enforcement began:

Reduction in the use of third-party cookies on websites:

One of the most important impact of the GDPR is the sudden drop in third-party cookies across websites in the EU. News sites from across seven countries (Finland, France, Germany, Italy, Poland, Spain, and the UK) were studied[20] before and after the enforcement of GDPR. The number of cookies set on these sites has dropped by around 22%.

There has also been a drop in sites containing third-party social media elements (such as a button to share to Facebook or Twitter), from 84% in April to around 77% in July 2018.



Contextual vs. personalized targeting for ads:

After GDPR, organizations are uncertain about relying too much on personalized targeting for ads. With so much uncertainty surrounding the use of personal information to tailor ads, there is a resurgence in targeting ads based on what a customer is looking for in a page. This could also be a result of the dramatic fall in the number of cookies used on EU websites.

With a drop in third-party data available to business due to difficulty in obtaining consent from users to use their data for personalized targeting, organizations are returning to contextual targeting for ads. In a

survey of 500 marketing decision makers conducted by ad tech firm Sizmek[21], around 77% stated that GDPR will make it harder to have personalized ads, and around 80% said that they would be scaling up contextual ads over the next 12 months while trying to maintain personalized ads where possible.

Andrew Frank
VP and Distinguished Analyst
Gartner for Marketers [23]
Gartner

> Rather than lament over what we can no longer do with personal data, let's see how much further we can get with non-personal data, like contextual information[22] and circumstantial data about time, place, weather, and so forth. In the rush toward audience buying and people based marketing, a lot of valuable data and analysis might be getting overlooked."

Blocking EU visitors from websites: a sensible strategy?

Over 1,000 news sites have blocked access for EU visitors. However, this is not limited to news sites. Gaming websites and internet platforms have also declared that they will no longer be serving EU customers. Many organizations do not wish to put themselves through the gruelling effort of ensuring that all of their processes comply with the obligations placed upon them by GDPR. They are unsure what risks it would entail to allow EU visitors to access their sites, and are content to wait until the regulators figure everything out. While this may seem sensible, it is not good in the long run.

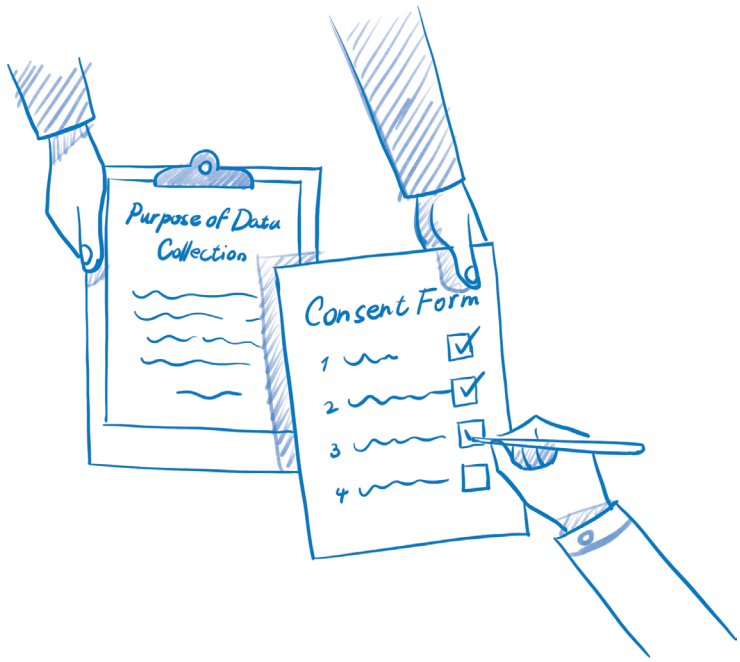
What seems like a very appealing solution will eat into your revenue and interfere with the growth of your business. The EU is a huge market, and it's worth going the extra mile to ensure your organization is GDPR-ready and equipped to serve customers from that region. Being GDPR-ready also helps increase consumer trust and brand loyalty in this privacy-conscious era.

The page speed of certain US sites also demonstrates website owners' ambivalence about serving EU customers. The US version of USA Today had an average load time of 9.9 seconds after GDPR enforcement, but versions in UK, France, and Germany loaded in 0.42, 0.75, and 0.51 seconds respectively. This is mainly attributed to the site dropping ad servers, Google services and analytics, and social media plugins. Ad rates have seen a 10% rise in the US and a simultaneous drop in the EU.

GDPR and CRM

Customers are the lifeblood of any organization, and their data drives your organization to offer a better and more personalized experience in every interaction. At the center of any data driven organization you can find great CRM software.

CRM systems are used to collect and store different types of information from customers, depending on the organization's needs. With the expanded definition of personal information under GDPR and the varying degrees of security that information is subjected to, combined with the slew of rights for EU residents that came with GDPR, a CRM system that helps you address these concerns will be your greatest asset.



Gartner[24] predicts that by 2022, poor privacy management in CRM procedures will lead to major sanctions for companies that fail to comply with GDPR.

How can CRM help you meet GDPR requirements?

Leading CRM providers have redesigned their software and introduced new features to aid organizations on their compliance journey. So it is paramount that you thoroughly evaluate your current CRM software to see if it helps you do the following:

- Track the source for all personal information.
- Document the lawful basis for processing all personal information stored in the system.
- Address the various rights of EU residents under GDPR.
- Provide selective access to sensitive information only to those employees who require it.

GDPR requires privacy by design, which means that privacy must be a core part of the design and functionality of a product. So choosing a CRM that has in-depth privacy and security measures built into it is a necessity in the GDPR era.

How Zoho CRM can ease your GDPR compliance journey

Zoho as an organization has always valued the privacy of our customers. As a data processor for our customers, we've designed Zoho CRM to ease the compliance process, in order to let you close deals smarter, better, and faster without having to constantly worry about GDPR.

We've thoroughly analysed the regulation to bring you multiple enhancements that let your organization collect, process, and store your customer data in accordance with GDPR.

Enabling GDPR compliance in Zoho CRM

The GDPR features can be enabled at the drop of a hat, by navigating to the Compliance Settings section under the Users and Control tab in the Setup menu. Enabling the compliance settings won't affect any processes that you have already set up.

These features have been designed to help ease your compliance journey by assisting you on three fronts:

- Data collection
- Data processing
- Data subject rights

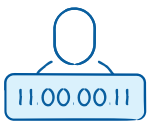
Let's take a quick look at how you can leverage Zoho CRM, and address the GDPR requirements, at these three different stages of your data cycle.

Data collection

GDPR demands that personal information collected from data subjects should be limited to what the data controller needs to deliver its services, and if additional information is requested, a legitimate need must be demonstrated.

If you're planning to rely on consent for processing, the consent must be explicit– your data subjects must take a deliberate action (such as clicking the checkbox; pre-ticked checkboxes do not qualify). Controllers are also expected to be transparent about the duration for which the data will be processed.

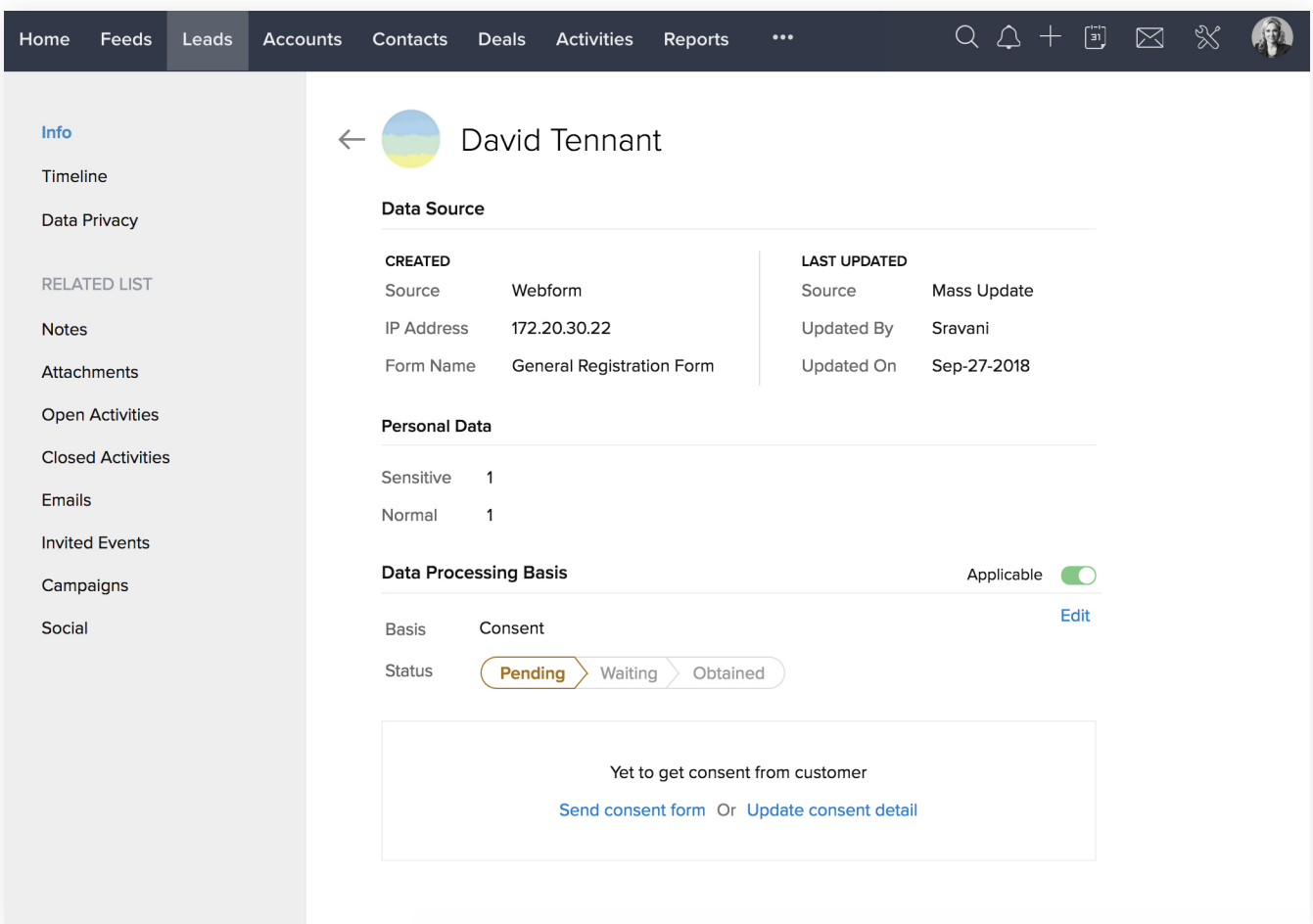
Zoho CRM web forms can be completely customized to help you restrict your data collection to the smallest amount of personal information that is required to deliver your service to a customer. This combined with the other GDPR features helps you stay compliant when you gather personal information from your prospects.



Data source tracking

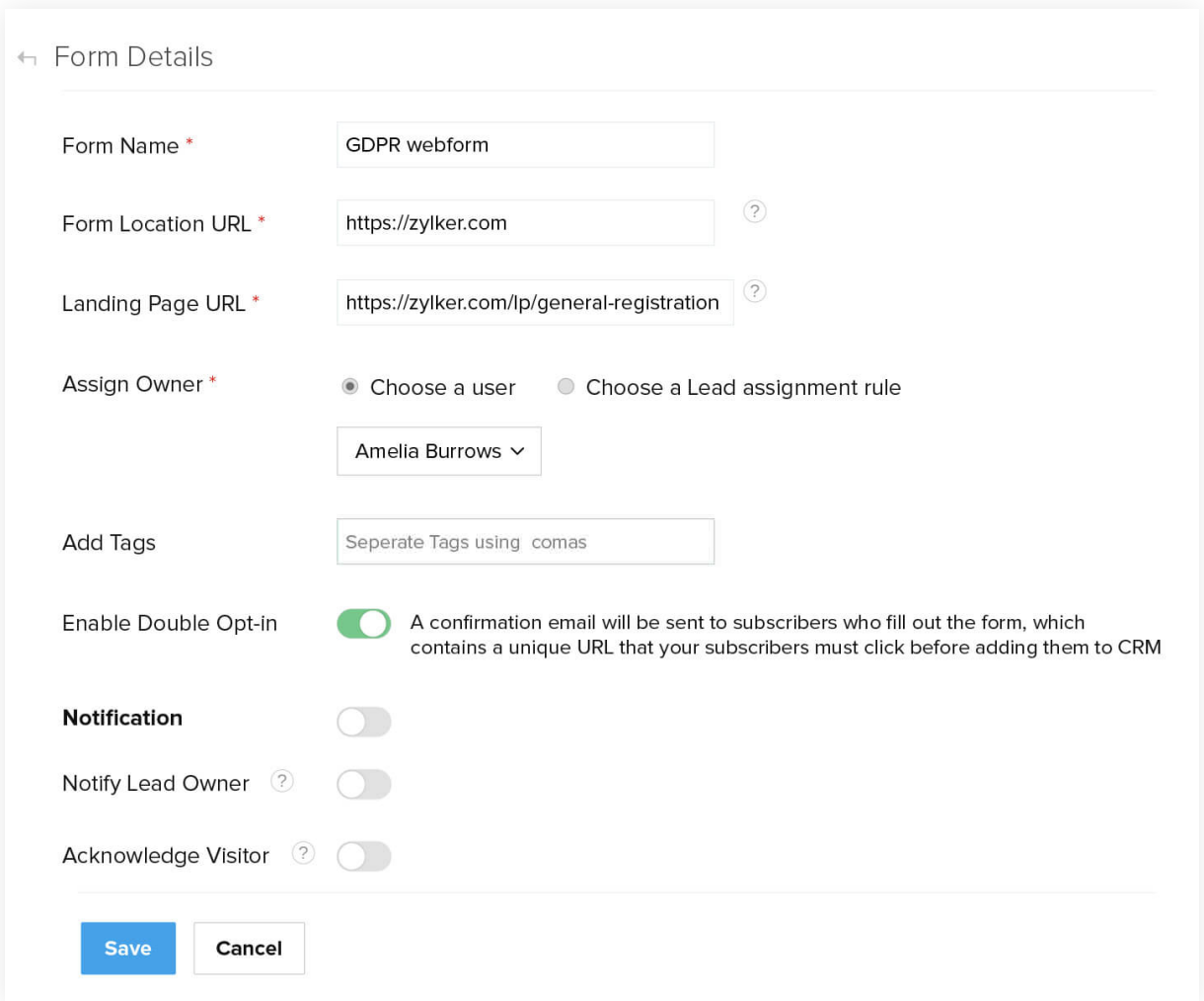
Data subject information can be pushed into Zoho CRM from multiple sources, including direct sources like web forms and indirect sources such as imports, UI, APIs, and third-party integrations.

The source of each piece of data, and additional details like the URL and IP address for web forms, will be documented in the Data Privacy tab of the record details page. When the record is updated, the source from which the update came is documented as well.



Double opt-in mechanism

Double opt-in is one more compliance feature which you can use when setting up web forms. Any time a data subject submits their information through a web form, a double opt-in email is sent to them to confirm their registration or signup.



A double opt-in mechanism is not mandated by GDPR, but it is a best practice nonetheless. By having every prospect double opt-in, you eliminate the possibility of someone accidentally or maliciously signing up to your mailing list using an email that is not their own.

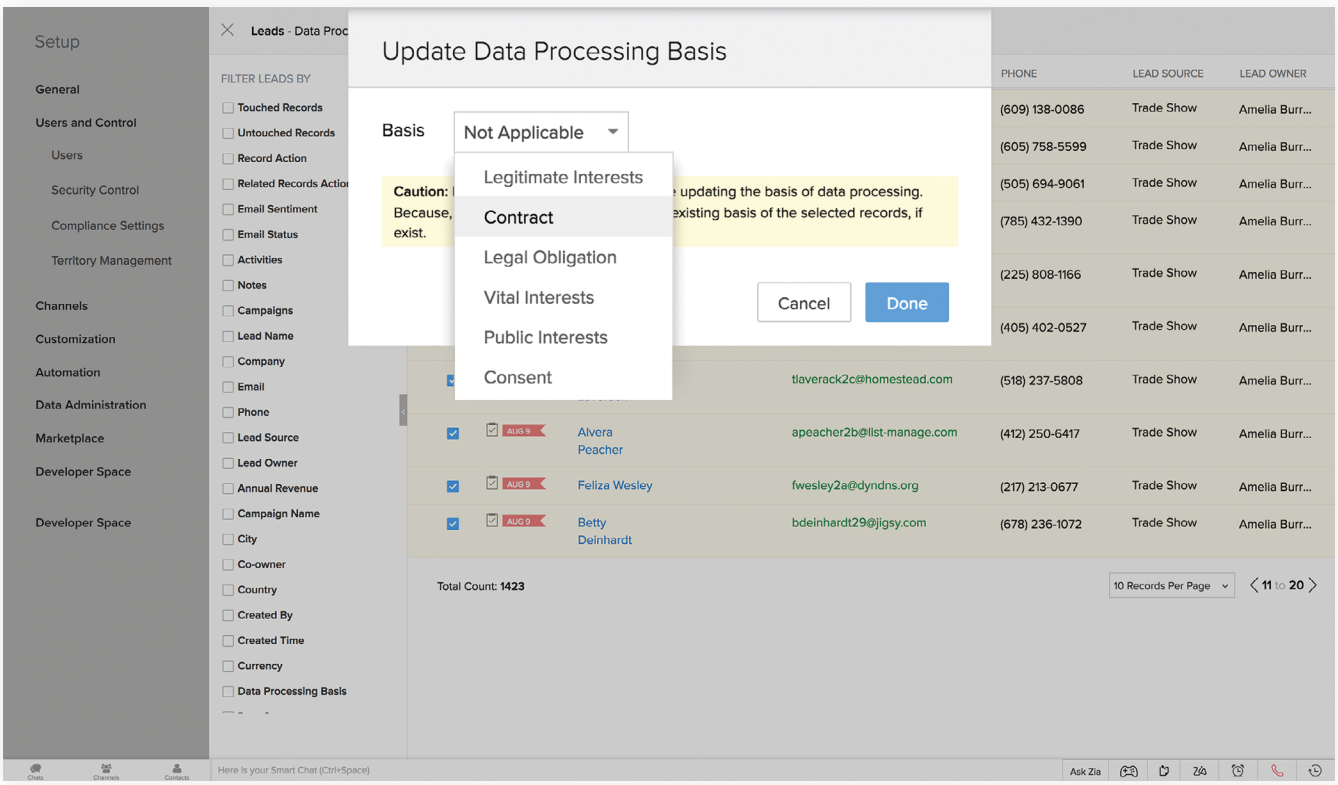
This leads to a clean and healthy mailing list composed of people who want to receive email communication from your organization, which results in better open and click-through rates.

Data processing

Information provided by a data subject can only be processed under one of the six lawful bases. GDPR places significant emphasis on the fact that all processing activities must be carried out securely to ensure that personal information is not exposed.

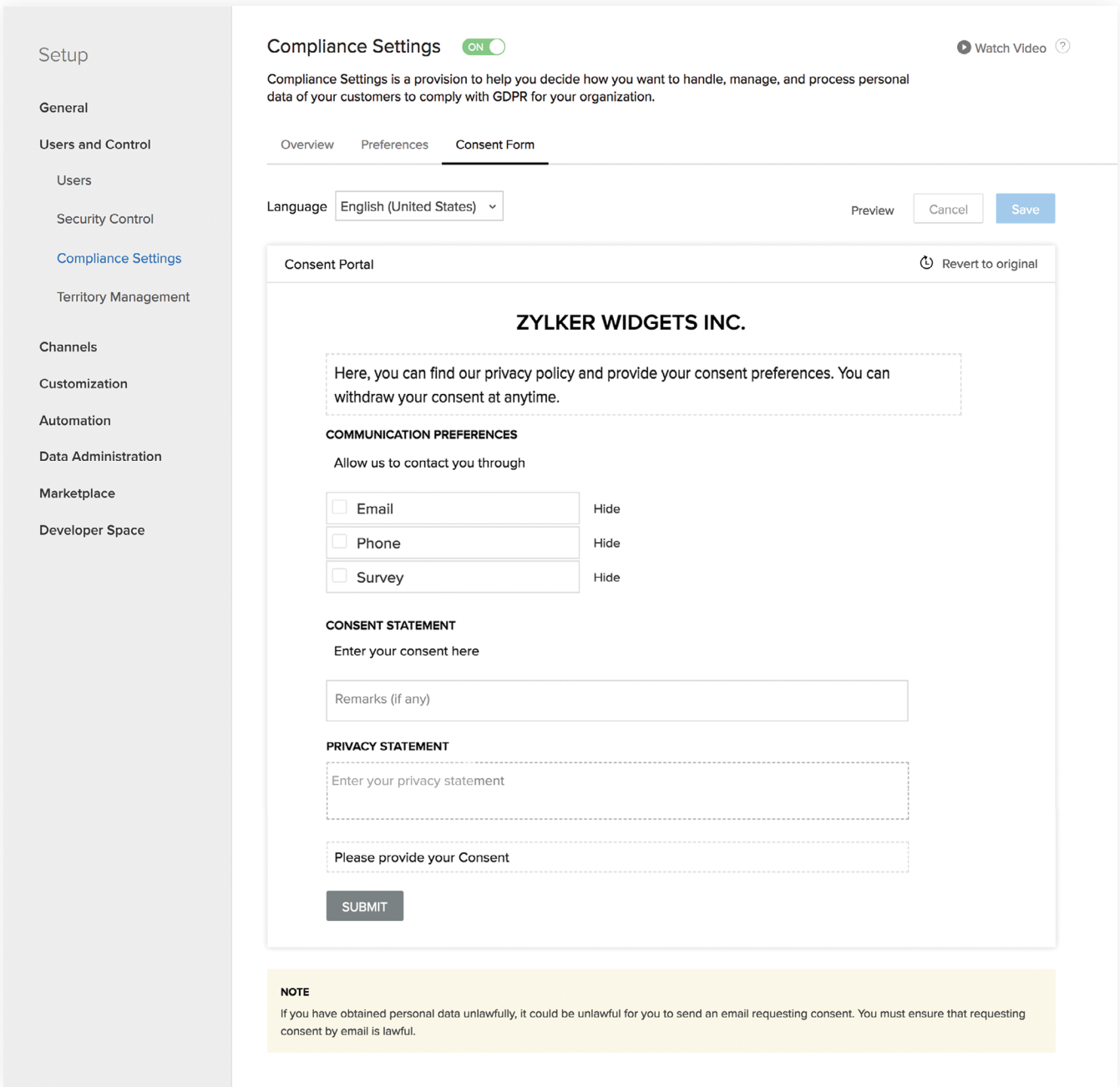
Choosing the lawful processing basis

Once personal information has been collected, the next step is to ensure that the information is processed under one of the six lawful bases. You can manually update the data processing basis for your customer records, or use workflows with custom criteria to automatically update records' data processing basis as they are added.



Consent form

Consent is one of the cornerstones of GDPR. The execution of any processing activity now depends on the consent provided by the data subject, if consent is the lawful basis used. In order to demonstrate compliance, it is mandatory that a data controller get consent and be able to provide proof of consent when required.



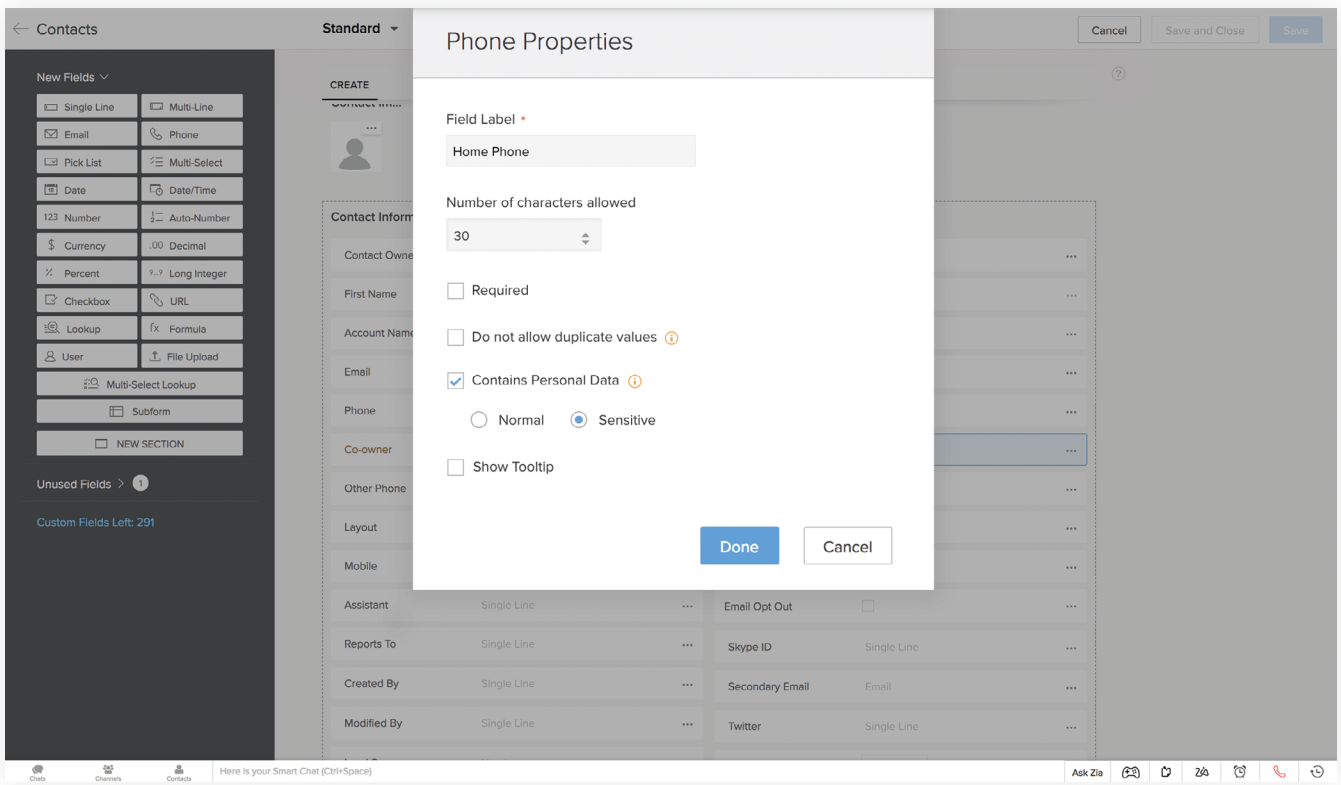
The consent form in Zoho CRM, which can be customized, allows controllers to get explicit consent for:

- The purpose of data collection.
- The data subject's preferred communication channel.

Consent from data subjects, whether in writing or orally obtained (through email or telephone) can be attached to the form using the Attachment option. Once the data subject has submitted their consent, it's stored under their record details page. This also helps the controller understand their actionable items from the data provided. For example, if a data subject has indicated that their preferred channel of communication is email, then they cannot be contacted through any other means in Zoho CRM.

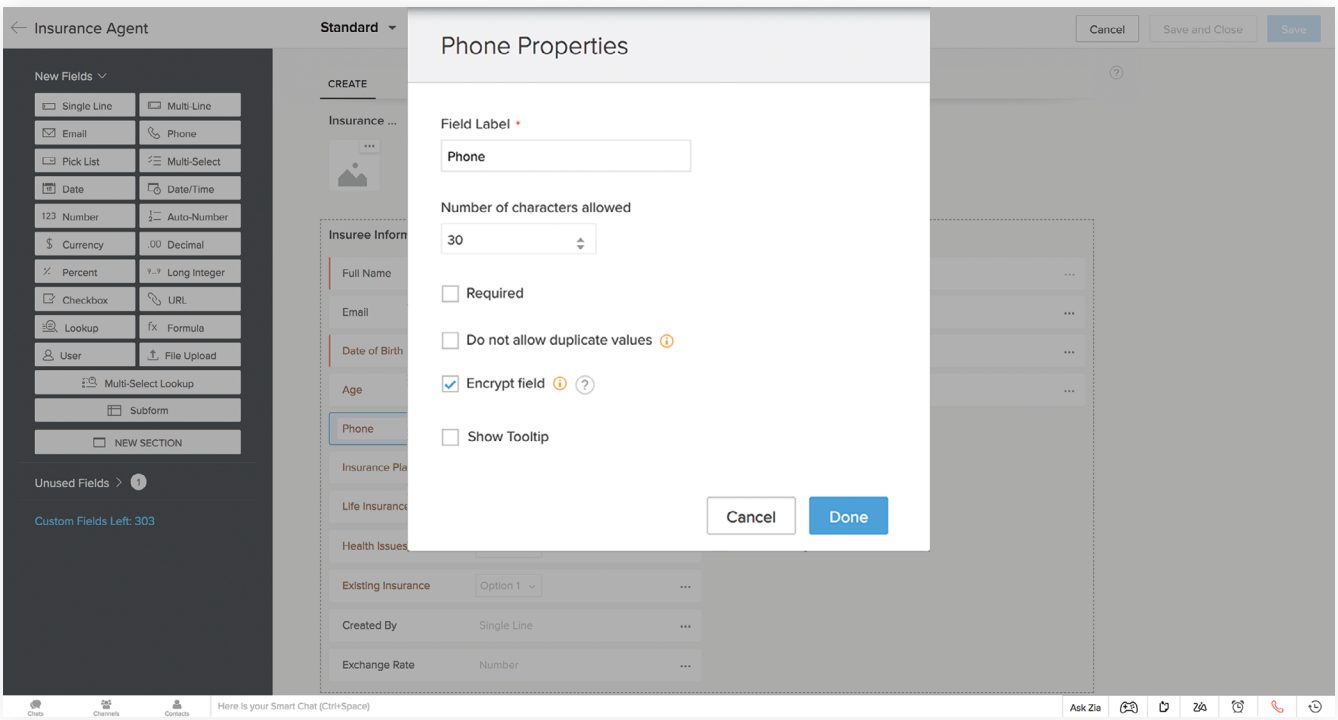
Marking personal fields

Data controllers can mark fields containing Personally Identifiable Information (personal fields) and indicate whether they contain sensitive information or not. The controller can also choose to restrict these fields from certain processing activities such as exports, APIs and connected services.



Encryption At Rest (EAR)

Enterprise users have the option of Encryption At Rest for personal fields. Zoho CRM uses a strong and robust security mechanism, AES, to encrypt and decrypt sensitive data. Apart from protecting data during transit, Zoho CRM secures data stored in servers using the AES-256 protocol and prevents data from being leaked or lost if you've enabled EAR.

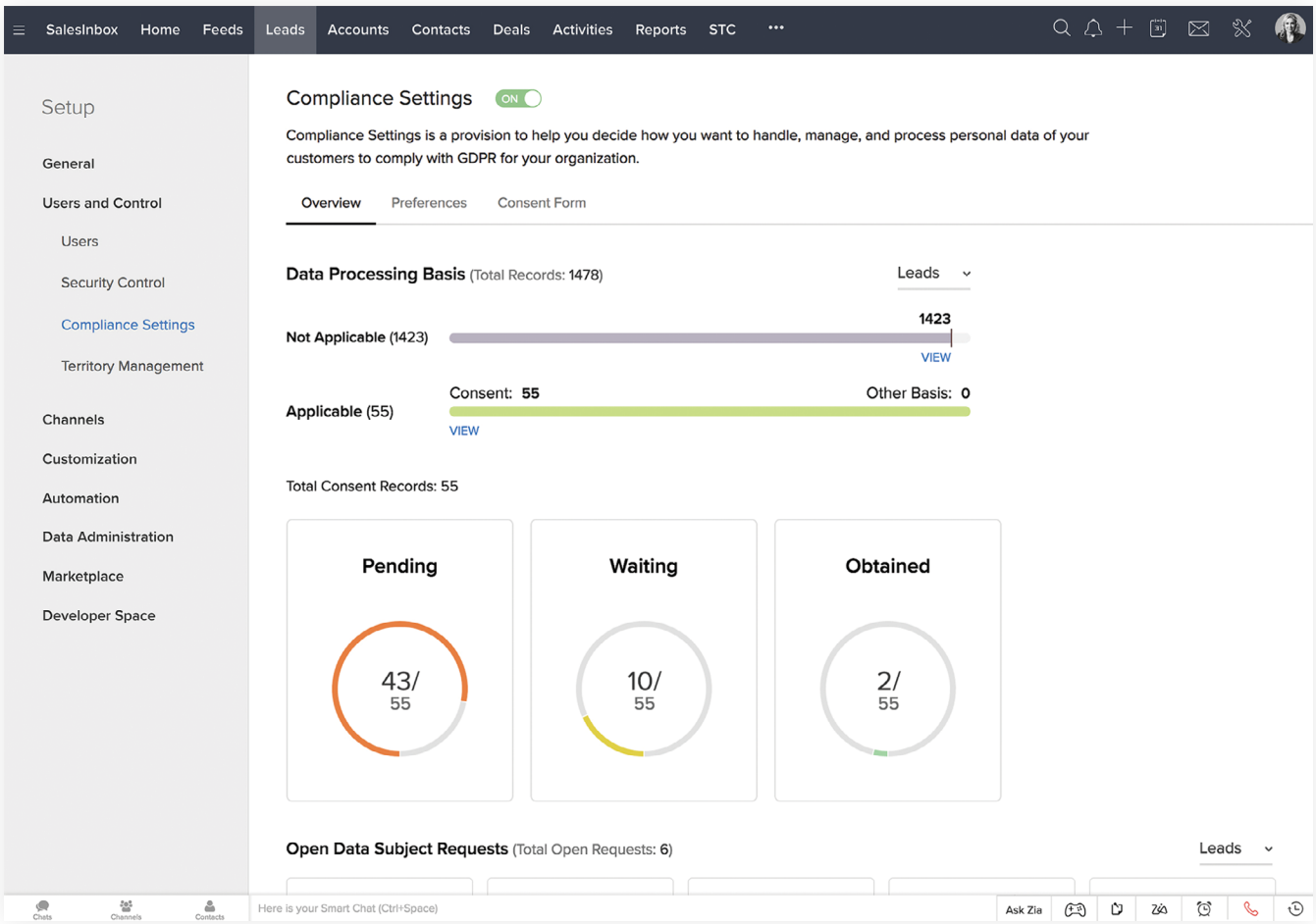


Audit log and timeline

The data controller can monitor their sales team's activities with audit logs, so they can track who did what and when with respect to a data subject's information. For example, all record deletions and modifications done by their users will be automatically audited to create a history of processing activities for accountability.

Consent management

The consent management system helps the controller keep track of the consent status of their data subjects. The system helps users identify data subjects who have yet to provide consent and mmediately send them an email with the consent form link. Consent can be obtained through web forms, a consent form, the customer portal, or offline methods like email or phone calls.



Data subject rights

GDPR comes with a slew of rights which EU data subjects can exercise at any time, and which must be addressed by the data controller within a month's time. The data request management feature in Zoho CRM lets the controller keep track of all data requests so that it's easier to address them promptly.

The various data requests raised are also maintained under each data subject's record details page, so that the controller can see any pending requests.

Data subjects can exercise their rights through the consent form, the customer portal, or offline methods like email and phone calls. Zoho CRM helps controllers insert a data request link in any email template being sent to customer, and address other data requests through the following options:

Access

Zoho CRM's email feature allows the controller to create a template incorporating the required customer information through merge fields, which can be sent to data subjects who exercise their right to access. Data subjects can also access their information through a customer portal (Enterprise edition).

Rectify

When a data subject exercises their right to rectify, their information can be exported and sent to the subject to be corrected and then updated. Data subjects can also rectify and update their information themselves through customer portals (Enterprise edition).

Export

When a data subject exercises the right to portability, their information can be exported, attached to an email, and sent in a machine-readable CSV format, all without being downloaded to the controller's device.

Stop Process

Once a data subject exercises the right to stop processing, their information will be locked, preventing further processing. If the data subject exercises this right through the data subject request link, their records will be locked automatically. CRM users will not be able to edit or share the records, run macros on them, or send the user automated emails through workflows. The request can also be added manually if the data subject exercised their right through an email or a phone call. A stop-processing request can be created under the Data Subject Request section of the Data Privacy Tab. Once the request is created, clicking the Lock button will lock the record to prevent further processing. When the data subject has agreed to let you process their data again, you can unlock it from the Data Privacy tab.

Erase

Once the right to be forgotten is exercised, the data subject's information can be locked for the retention period defined in the data controller's terms of service. After that point, the data controller will have the option to delete the data subject's information. Once it is deleted, all records that have the data subject's email will be moved to a block list to prevent the re-entry of the same data.

Choose Privacy. **Choose Zoho.**

"We have expanded the GDPR-style rights to our users globally. Whether the EU regulation is applicable where they are or not, our users across the world can request us to remove their personal data or know what data is there in our systems about them."

Sridhar Vembu
CEO, Zoho Corporation

At Zoho, we've always maintained a high standard when it comes to our users' rights to data privacy and protection. Over the years, we have demonstrated our commitment to data privacy and protection by meeting the industry standards for ISO 27001 and SOC 2 Type 2. Zoho Corporation participates in and has certified its compliance with the EU-U.S. Privacy Shield Framework, with respect to transfer of data to the U.S.

Zoho has never sold customer information for advertising, or made money by showing them other people's ads, and we never will. This has been our approach for almost 20 years, and we remain committed to it. GDPR is another opportunity for us to deepen our commitments towards the security and protection of personal data to build stronger ties with our customers.

Read more about our security practices and infrastructure at https://www.zoho.eu/security.html

For sales enquiries, write to us at sales@zohocorp.com

About the author:

Shashank works as a Product Marketer for Zoho CRM. He is an avid gamer and an artist with an ingrained curiosity about our cosmos. GDPR keeps him awake at night better than a hot cup of coffee ever could.

Reference

[1] . https://www.statista.com/statistics/512650/worldwide-connected-devices-amount/

[2] . https://www.slideshare.net/MichaelBeatty/ibm-cloud-storage-cleversafe

[3] . https://www.verint.com/digital-tipping-point/

[4] . https://newsroom.intel.com/news-releases/new-mcafee-survey-reveals-42-percent-consumers-take-proper-security-measures-protect-new-gadgets/

[5] . http://www.pewinternet.org/2015/05/20/americans-views-about-data-collection-and-security/

[6] . https://breachlevelindex.com/top-data-breaches

[7] . https://www.reuters.com/article/us-verizon-yahoo-breach/data-breach-victims-can-sue-yahoo-in-the-united-states-judge-idUSKCN1GO1TL

[8] . https://www.nytimes.com/2017/11/21/technology/uber-hack.html

[9] . https://www.consumerreports.org/credit-bureaus/equifax-data-breach-was-bigger-than-previously-reported/

[10] . https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

[11] . https://prod.demand.intelsecurity.com/verifyThanks?docID=000292c31a94769ee41654e7f7343363&region=us&_ga=1.12946999.1660561146.1484749798

[12] . https://europa.eu/european-union/eu-law/legal-acts_en

[13] . https://eugdpr.org/

[14] . https://gdpr-info.eu/art-5-gdpr/

[15] . https://gdpr-info.eu/art-6-gdpr/

[16] . https://gdpr-info.eu/art-7-gdpr/

[17] . https://gdpr-info.eu/chapter-3/

[18] . https://gdpr-info.eu/chapter-4/

[19] . https://gdpr-info.eu/art-32-gdpr/

[20] . https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2018-08/Changes%20in%20Third-Party%20Content%20on%20European%20News%20Websites%20after%20GDPR_0_0.pdf

[21] . https://www.sizmek.com/

[22] . https://digiday.com/media/personalization-diminished-gdpr-era-contextual-targeting-making-comeback/

[23] . https://www.gartner.com/marketing/expert/andrew-frank.html?_ga=2.45843428.1769514339.1535373355-359735365.1533878318

[24] . https://www.gartner.com/doc/3832563

Sales Enquiries

USA
+1 877 834 4428
+1 615 671 9025

UK
+44 (20) 35647890
+44 8009177225

INDIA
+91 (44) 71817070
+91 (44) 71817000

FRANCE
+33 805542462

SWEDEN
+46 201408150

NETHERLANDS
+31 707007083

GERMANY
+49 8000229966

ITALY
+39 (0) 287103737

SPAIN
+34 918368598

AUSTRALIA
+61 2 80662898

ZOHO CRM

sales@zohocorp.com | www.zoho.com/crm | www.zoho.eu/crm