ClickDimensions

Permission, Privacy and Security: Top Questions and Best Practices

With a full suite of features that includes web tracking and email marketing, the ClickDimensions marketing automation solution evokes a number of questions from our prospects, customers and partners surrounding permission, privacy and security. And rightly so. While these respective tools have the power to deliver valuable insights and provide an effective communications channel, when used improperly, they can have a negative impact on organizations and their audiences alike.

In the following pages, we have gathered some of the most common customer questions we receive related to these issues along with our best practices for addressing them.

Permission

What is permission-based marketing?

Permission-based marketing means that your prospects and customers have directly granted your organization permission to market to them. In email marketing, this means that they have opted in to be on your list. This opt in can be in the form of a subscription sign-up form on your website, a paper form at your place of business, or even a conversation you have in person or on the telephone with someone. Giving a recipient an opportunity to unsubscribe or opt-out is important, but your marketing is not permission-based if you didn't first get their consent.

How do I get someone's permission before adding them to my marketing list?

There are many smart strategies for acquiring subscribers; most involve offering something of value to individuals in exchange for their contact information. For example, offering an eBook in return for completing a form, conducting a contest with an entry form, or hosting a webinar or event that requires registration. Something as simple as adding easy-to-find email sign up boxes throughout your website can help tremendously in list-building efforts. Social media is also a great place to build your lists, either by promoting giveaways or content downloads. At ClickDimensions, we get a lot of mileage and new names on our lists from our content marketing efforts such as eBooks and webinars.

Can I use purchased lists?

It may be tempting to purchase a list of email addresses from a third-party; however, most of these lists are not reliable, and the recipients on the list have not opted-in to receive your emails. Third-party lists are often purposely seeded by ISPs with fake email addresses whose only purpose is to catch

spammers. Third-party lists also frequently contain out-of-date email addresses that will cause your bounce rate to go up. Purchasing lists is such a bad practice that ClickDimensions does not permit the use of third-party lists at all, whether purchased, rented or borrowed.

What is ClickDimensions' policy regarding permission-based marketing?
ClickDimensions' terms of service require that all of our customers adhere to permission-based marketing practices.

Privacy

How does web tracking work?
Modern browsers are not designed to give away your personal information. Barring a bug, hack or hole, companies like Microsoft, Google, Apple and Mozilla are not in business to tell websites who you are. So, to determine who you are, tracking technologies need some method of creating a link between you and your browser (or your computer). This link is typically what is referred to as a cookie. A cookie is traditionally a text/HTML file that is placed in your browser and includes a unique identifier that is meaningful only to the site that placed it. With each visit you make to that website, the site can look for the cookie and check its identifier against the website's database to see if you have visited before.

Site-specific tracking

If, during one of your visits, you tell the website who you are by completing a form or clicking on a link in an email sent from the site, then the unique identifier in the cookie can be associated with your personal information (i.e. your email address) so that each time you return to the site, you will be recognized. We refer to this type of tracking as site-specific because the site you are visiting has determined who you are through only your interactions with their site, and without help from other sites. In order for site-specific tracking to be responsibly employed, organizations using it should practice permission-based email marketing so that visitors identified through email link clicks must have signed up for those emails on the site or otherwise given their explicit consent to receive them.

Multi-site tracking with universally unique identifiers (UUID)

An alternative method of tracking is through the use of cookies containing universally unique identifiers (UUID) that are shared across multiple websites. In some cases, advertising solutions place cookies on your computer so that ads served to you on various websites can be tailored to your specific demographics and interests. There are two ways that cookies can accomplish this. Either the cookie can contain anonymous information indicating the visitor's demographics and interests (e.g. information that indicates only that the visitor is male, 35 – 55 years old and a sports fan) or the cookie can contain personally identifiable information (PII) so the site can know the exact identity of the visitor. The latter is accomplished by placing a UUID in the cookie so that other sites can read that identifier and reference a shared database that tells the site exactly who the visitor is, along with all the information that it and the collaborating sites have collected about the visitor. So, if you visit site A and identify yourself by providing personal information and then site A shares that information with site B, then site

B knows who you are even though you have not identified yourself to site B. Multi-site tracking can be enriching for the user when it does not involve PII such as what is available through the use of UUIDs. However, to visit a site, share with it your personal information and then have it share that personal information with other sites is an invasion of privacy unless you are aware it is happening, agree to it, know exactly what information it is sharing about you and to which sites your information is being shared.

What kind of cookies does ClickDimensions use?
ClickDimensions uses first-party HTML browser cookies in our web tracking technology. This means that visitors to sites using our web tracking technology are easily able to set their browsers to reject cookies and are easily able to delete cookies set by us and others.

ClickDimensions never stores any information in a computer's Flash local shared objects area, also known as Flash cookies.

How do I notify my website visitors about tracking?
Some countries and jurisdictions require websites to notify visitors about the types of tracking technologies used on the website and by the website owner. ClickDimensions has developed an example script that will show an alert to a website visitor to notify them about tracking. You can use this sample script by copying it to your own website and modifying the language that is contained in the script. You can view the example notification and download the JavaScript file here.

NOTE: ClickDimensions does not make any warranty about whether or not the use of this script or our website analytics conforms with your regional privacy laws. ClickDimensions provides a technology that we believe is respectful of individuals' privacy, but it is up to the end user to implement the technology in a manner that conforms with applicable laws in your jurisdiction.

Security

Does ClickDimensions store any of my customers' data?
Your customer and lead data is stored safely and securely in your CRM system, not in ClickDimensions. The exceptions to this are:

a) Email addresses of recipients. In order to accurately record deliveries, opens, clicks, bounces, etc., all email marketing platforms must store this information.

b) The ClickDimensions profile management feature stores a small amount of data to make it possible to pre-populate a web form that an email recipient visits by clicking a link in a ClickDimensions email.

Is the connection between ClickDimensions and my CRM secure?
If you register your CRM using an address that starts with HTTPS, then our connection to your CRM will always be securely encrypted using the SSL certificate you installed on your CRM website (or the one used by Microsoft for CRM Online). Note that self-signed SSL certificates are not supported.

How does ClickDimensions connect to my CRM?
ClickDimensions communicates with your CRM using only Microsoft-documented methods to connect to CRM's web services. ClickDimensions

does not communicate or connect to SQL Server, Active Directory, or any other server or network applications. All of our functionality is delivered through Microsoft's SDK (Software Development Kit) methods for Dynamics CRM. Microsoft has also designated the ClickDimensions solution as Certified for Microsoft Dynamics (CfMD). For detailed information on ClickDimensions connectivity, you can read more here.

Who has access to ClickDimensions servers?
ClickDimensions' application is entirely hosted in Microsoft Azure in Microsoft data centers. As such, physical access to the servers and network resources that host the ClickDimensions application is restricted to Microsoft personnel. ClickDimensions personnel do not have physical access to these resources. See Microsoft's Azure Trust Center for more information.

Remote access to the production environment is restricted to ClickDimensions' Chief Technology Officer. The ClickDimensions application production environment is a separate network from ClickDimensions' internal operations network. Therefore, ClickDimensions employees, such as developers and technical support individuals, do not have access to the ClickDimensions production application.

Where are the Microsoft Azure data centers located?
The ClickDimensions application is hosted separately in Microsoft's East US data center in Virginia, the West Europe data center in The Netherlands, and in the Australia East data center in New South Wales.

Can I retain control of the password that ClickDimensions uses to connect to my CRM?
Yes. When you register your CRM with ClickDimensions, the connection information is securely transmitted in encrypted format. At any time after installing ClickDimensions, you can change the password our system uses from within CRM by clicking on Settings > ClickDimensions Settings > Service Credentials. (Note that you must update it here prior to actually changing the password for the user.) See here for more details.

What IP addresses does the ClickDimensions' service use?
Some companies wish to restrict access to their CRM to only specific IP addresses. See this article for the IP addresses currently being used by the ClickDimensions application.

For more information or questions regarding ClickDimensions' stance on privacy issues, please contact us at privacy@clickdimensions.com.