A Guide to Writing Privacy Policies for Websites and Applications

https://masaar.net

A Guide to Writing Privacy Policies for Websites and Applications

Introduction

"Masaar" noticed a number of issues related to the privacy policies used by websites and applications in Egypt, which affect users' privacy and their digital security. Some privacy policies are vague, which make them not understandable by users. Also, some websites and applications collect, store and analyze users' data and share them with third parties without their prior consent.

Some websites and applications lack data security and protection measures, and other websites do not provide users with the right to know which data was collected or the mechanisms available to erase this data. Also, some websites change the privacy policy without notifying users of these modifications, and many websites and applications do not provide sufficient information about the rules for saving information and data after users finish using the services provided by the website or application. Moreover, many websites and applications do not inform users of any security breaches that could affect their privacy and the safety of their data.

Therefore, "Masaar" provides this guide to technologists, owners of websites and applications, and companies working in the field of communications and information technology, to provide advice that helps these groups formulate the privacy policies of the digital platforms they manage. "Masaar" believes that writing and developing privacy policies for websites or applications is an ongoing process. Also, the terms of privacy policies adopted by these websites and applications must be reviewed periodically in order to keep pace with the developments of various services or software, to respond to changes in the type of data collected from websites or applications, or to adapt to changes in the infrastructure.

This guide aims to provide a number of tips that help make the privacy policies adopted by websites and applications more clear, understandable and easy to apply. The guide also provides advice on how to maintain a balance between the users' right to protect their privacy and control their data on the one hand, and the requirements of the service provider (website or application) in collecting information and data necessary to develop the services they provide, on the other hand.

First: General rules and practices

The service provider should make sure that the privacy policy is easy to understand, presented to the user in a suitable manner, and clear in its terms and clauses. The following are general rules that govern the privacy policy:

- The privacy policy texts should be clear, not broad, and easy to understand by the service recipient/user.

- Privacy policy should contain clear definitions of all the technical and legal terms used, or any other terms that may be difficult for users to understand, and that all terms are precisely defined, and not subject to different interpretations.

- There should be a way for communication between the user and the service provider to answer questions about privacy protection.

- Provides for the user's prior consent if there is a change in the privacy policy.

- The policy should explicitly state that users are entitled to protection -because of the collection and analysis of their data- from sexual exploitation, physical and psychological abuse and from degrading treatment.

- Users must be enabled to refuse or accept the use of cookies on the website or application, and not to activate any of the cookies used except after the user's consent, provided that the default is not to activate cookies.

- The use of data collection software and tools should be rationalized and the usage patterns monitored.

- The privacy policy should not include a reference to any type of charity, legal liability, or promotional offers, as these contents affect the users' impression while reading the policy, for example referring to charitable work carried out by the website or the application.

- We also recommend that the software used in managing and operating the websites or applications be subjected to an independent technical review regarding security and protection; the results of this review should be announced to users.

Second: Data collection

The basic rule: The process of collecting users or service recipients' data across websites and applications must be based on their prior consent. This includes the consent of users and service recipients on the quality of the data collected. The service provider collects data and information either by requesting them directly from the service user/recipient, or through software used by the service provider. In all cases the privacy policy must explain the data collection method in an unambiguous way:

1. Data provided voluntarily

These are data that users or service recipients provide while they are using the website or application, for example: email, user name, phone number, date of birth, gender, credit card number or other payment information. The privacy policy must also provide an exclusive definition of the type of data collected by the website or application, and the service provider should not trade in the data collected from users.

2. Data collected by cookies

These are two types, the first: Season cookies, which remain until users or service recipients leave the website or application. The second are persistent cookies, which remain on the devices of users or service recipients, even after leaving the website or closing the application, and are deleted by the users or service recipients manually.
Cookies contain information related to users or visitors, including but not limited to: geographic location, IP Address, type of device used, the way the user connects to the Internet, type of browser and operating system. The websites and applications also use third parties services that use cookies to collect data about users or service recipients, and the latter type of data is subject to the third-party's privacy policy.

The terms of the privacy policy must contain a complete list of data collected by the website or application's cookies, whether it is used by the website or application itself and for itself or by services provided by third parties. The privacy policy must also state how long such data is retained, the procedures and the type of processing to which it is subjected and how it is secured, stored and processed.

Third: The purposes of data collection and analysis

The basic rule in relation to the purposes of data collection and analysis is that the process of collection and analysis must be based on the prior consent of users or service recipients, including thier agreement on the type of analysis to which the data is subject. The users or the service recipients have the right to be fully aware of the purposes of collecting and analyzing data, and in this context, the terms of the privacy policy must state that:

• In all cases, the service provider may not use the data collected by the website or the application for any purpose other than those stipulated in the privacy policy, which were previously approved by the users or recipients of the service.

• The terms of the privacy policy should state –clearly, accurately, and exclusively– the purposes of collecting data that is provided voluntarily by the users or recipients themselves.

• The privacy policy should include -clearly, precisely and exclusively- clauses explaining the purposes for which data is collected by means of cookies, the purposes of processing to which it is subject, the type of data it uses and information about cookies from third parties, including the privacy policy to which the third party is subject.

• There are many types of data that can be collected, and it may include, for example, but not limited to: Some information provided by the user voluntarily, such as user name and e-mail, or information collected by website cookies and third-party cookies, which is used for the purpose of providing users with the services of the website or application and to facilitate its management, such as providing the best browsing experience to the user, managing subscriptions, conducting financial transactions, and addressing technical problems. These purposes must be specified in the privacy policy.

• Sometimes, websites and applications use data that is provided voluntarily by users to send updates, alerts and promotions. The privacy policy must provide a clear and accurate listing of these activities, especially if it relies on third parties to perform them.

Fourth: Sharing data with third parties

The basic rule: Data sharing with third parties must be based on the prior consent of the users/service recipients, and this must include their consent to the type of data that is shared and the privacy protection measures that the third party is subject to.

The websites and applications share the data they collect from the users/service recipients with third parties; either to obtain specific services related to -for example- the analysis of this data or the implementation of a court order. Service providers must provide a clear and accurate description of sharing data with third parties, and this should be stated in the privacy policy:

• That the terms of the privacy policy are clear, accurate and transparent in the wordings and provisions for sharing data with third parties, and that these parties are exclusively identified.

• That the data is shared with third parties in an anonymous way; the data should not contain information that can reveal the identity of the users/service recipients.

• That the privacy policy stipulates any activities related to data analysis and sharing with third parties, and also listing all the purposes. Privacy protection standards (by third parties) must be a requirement in addition to the prior consent of users.

In any event, data sharing procedures with third parties must be governed by rules that attach great importance to the privacy of users and recipients of the service, including but not limited to:

• Prior consent: The service provider is obligated not to share any user/service recipient data and information without their prior consent.

• Respect for privacy by third parties: The service providers are obligated not to share any of the information and data they collect with any third party if there is reason to suspect that the third party is misusing them or violating the privacy of users.

• Meeting legal obligations: The service provider is obliged not to disclose any data and information about the users/service recipients to any law enforcement agency except in the case of a prior judicial order.

• Prior consent :

The service provider is obligated not to share any user/service recipient data and information without their prior consent.

• Respect for privacy by third parties:

The service providers are obligated not to share any of the information and data they collect with any third party if there is reason to suspect that the third party is misusing them or violating the privacy of users.

• Meeting legal obligations:

The service provider is obliged not to disclose any data and information about the users/service recipients to any law enforcement agency except in the case of a prior judicial order.

•Technical reasons:

Data and information may be shared anonymously with third parties in order to facilitate the operation of the website or application and improve their performance, address technical problems and make the necessary improvements to the servers, and in this context the information must be anonymous.

•Digital security measures:

Data and information may be shared with third parties with the aim of taking the necessary security measures to ensure that user/ service recipient data is kept secure or to ensure that payment systems are secure for processing financial payments by payment service providers.

•Transfer of ownership:

In the event that ownership of the website or application is transferred to a third party, and if the new owner will follow a new privacy policy; the service provider is obligated not to share and/or disclose any information or data related to users and service recipients that was stored during their use of the website, except after obtaining their prior consent.

Fifth: Securing data and information

In all cases, service providers must give particular attention to securing the data and information that they store and process, and the privacy policy must state the following:

• Make certain that data and information collected or stored by the website or application is securely processed and stored. Access to such data and information must be limited to the minimum number of individuals employed by the website or third parties, while ensuring that they are subject to confidentiality obligations.

• The provision that the website or application is subject to all available measures to ensure the safe collection, storage and processing of data and information in accordance with the privacy policy agreed to by users/recipients of the service. Although the transmission of information over the Internet is not entirely secure, service providers must provide assurances that they will do their utmost to protect users' data, and use strict procedures to try to prevent unauthorized access to this data.

• That the privacy policy provides for the right of users to use encryption protocols, whenever possible, whether in the transfer or storage of data and information.

• That the privacy policy makes recommendations to users/service recipients to rely on privacy protection software such as Virtual Private Networks (VPN) and/or Tor Browser.

Sixth: The user's control over their data

Users and service recipients have the right to have control over their data, including their right to erase it and not to have it processed. In this regard, the privacy policy must explicitly state the right of users to erase their data and information stored on the servers of the website or application. Here are some of the rules that should be covered in a privacy policy:

- **The right to cancel the subscription:**

stipulating the right of users/ service recipients to request the cancellation of their subscriptions at any time; the website or application is obligated to cancel the subscription.

• **Erasing data:** Users/service recipients have the right to request erasing their data and personal information at any time. The website or application is obligated to implement this and inform the users/service recipients of the time required for the erasure and clarify its procedures.

• **Obtaining a copy of the information and data:** Users/service recipients have the right to request a copy of all their data and information at any time and without giving any reasons.
Backup copies: Service providers must work to find technical solutions to erase data and information from backup copies, so that they are erased upon request by users/service recipients.

Seventh: Notifying of a change or an update to the privacy policy

As stated at the beginning of the guide, the privacy policy must be periodically updated and developed in line with the development of the software or services provided by the website or application. In this context, the privacy policy must state the following:

• **Prior-notification requirement:** Service providers are obliged to notify all users and service recipients via e-mail and through the home page of the website of any changes or modifications to the privacy policy before the modifications are put into effect.

• **Approval:** The service provider is obligated to obtain the approval of the users/ service recipients before applying any amendments or changes to the privacy policy, provided that the announcement of the amendments or changes includes setting a deadline for acceptance or rejection of the new policy by the users/ service recipients, and the effective date of the amendments or the changes.

• **Rejection:** In the event that the users/service recipients refuse the amendments or changes to the privacy policy, the service provider may take the following measures:
Canceling the user's subscription and returning any amounts paid; in proportion to the time the user benefited from the website or application, or continuing to work with the privacy policy without modifying or changing it until the user's subscription ends.

In the event that the user enjoys a free subscription to the website's services, the website has the right to stop the service provided to the user from the effective date of the changes and without using any data collected according to the old privacy policy.

• **Availability of previous policies**: The service provider is obligated to make available the previous policies and the changes that are made to them on an ongoing basis.

Eighth: Loss of the right to use or retain data and information

Service providers must respect the right of users/service recipients to revoke the right of the website or application to use, process and/or retain the data and information collected in the following cases:

• The user's request to unsubscribe.

• The user's request to erase their data and information.

• Suspension of the service for which the data and information were collected.

• The purpose for which the data were collected has ended.

• The user does not consent to the modifications or changes that occur to the privacy policy, and in this case the website or the application does not use any of the data and information collected before the modification/change.

Ninth: Reporting data leaks and security problems

The service providers are obligated to inform the users/recipients of the service about any leakage of data and information that is collected and stored, or any of the security problems that may affect their privacy. This is done as soon as the service providers become aware of the leakage. The service provider is also obligated to inform the users/service recipients of the possible damage to their privacy due to the discovered data leaks and security issues.

Tent: Recommendations on the use of web analytic software

In general, it is recommended to limit the use of Google Analytics, Google Tag Manager, Mixpanel or any of the software and services that can affect the privacy of users and service recipients, while the open source Motomo software that provides privacy protection options is reliable.

Also, the privacy policy should refer to the (pixel tag), which is a specific type of technology that is placed on a website or within an e-mail in order to track the activity of the web browser, or track the activity when the e-mail is opened or its contents are viewed. This is often done with the help of cookies. The privacy policy should indicate that the website or application uses pixel tags on Facebook and Twitter in order to track the transition from browsing social media to browsing the website.

Find more information on Facebook and Twitter here.

Recommendations on Google Analytics or Mixpanel

The following is recommended if using Google Analytics, Mixpanel, or similar software:

• Not to integrate (CRM) data with (Google Analytics) for any of the purposes related to marketing and advertising.

• Not to use the (User-ID) feature in (Google Analytics).

• Disable data sharing settings that are collected by (Google Analytics) with other (Google) services, whether with Google products and services, Benchmarking, Technical support and/or Account specialists.

• Close the data processing amendment in Google Analytics.

• Close the data collection for advertising feature in Google Analytics.

• Enabling users to delete their data collected by Google Analytics through the use of the User Deletion API feature provided by Google.

• Relying on IP Anonymization or IP masking technology in Analytics to collect and analyze the data collected by Google Analytics.

• Ensuring that the Geolocation information sent to Google Analytics is not GPS specific or highly detailed.

• Replace personally identifiable information (for example: e-mail or username) in URL schemes - including addresses sent from the website to users via e-mail- with the unique site-specific identifier.

• Using POST instead of GET to send forms via HTTP to avoid sending form information as part of addresses (URLs).

• Respect the "Do Not Track" feature in all services that you use to analyze and track usage patterns, especially in Google Analytics and Google Tag Manager, and provide the "Opt-out" option for users.

• Activating the (opt-out) feature so that users can prevent the tracking of their activities while using the website.

• Modifying "Opt-In Event" in the Mixpanel software so that none of the personal data of the website or application users is collected, for example, but not limited to: Device ID, User ID and City.

• Enabling website or application users to delete their data collected by Mixpanel by using the "Submit Requests via API" feature provided by Mixpanel.

• Taking all possible measures provided by Mixpanel regarding anonymization of the data collected by the website by applying "Tracking Truly Anonymous Data" measures.

Get help writing a privacy policy

We are happy to provide voluntary assistance in

writing privacy policies for websites and applications

If you are a service provider and want our help, send us an email to

masaarnet [at] gmail.com

https://masaar.net