Best practices for websites

Websites are now an essential part of business life. Companies, retailers, sole traders, self-employed professionals and even private individuals set up their own websites to promote themselves, provide information, present their services and products or offer distance selling.

The website also plays an important role in attracting customers and maintaining a relationship with them.

Whether the website is a simple « *showcase site* » or a « *e-commerce site* », in the vast majority of cases it involves the collection of personal data through a contact section, an online form, the creation of a customer account or the use of browser cookies.

Showcase site	E-commerce site
A « ***showcase site*** », is used to present a company, an administration, an association (...), its activity, its services and/or its products. It can also offer other functions such as: • a contact form; • a subscription to a newsletter.	A « ***e-commerce site*** » or **« *online store*** » is mainly used to offer services and/or products for sale. Another alternative is a « ***marketplace site*** », the main function of which is the intermediation of distance selling through the sale and presentation of merchants' products. In this way, Internet users can make purchases from various retailers on the same website, with a single customer account.

The purpose of this factsheet is therefore to help data controllers adopt good practices to ensure the **confidentiality** and **security** of data collected via websites.

Controlling the personal data collected

Not all websites collect the same amount of data or the same categories of data. This depends on the purposes for which the sites are created.

Once these purposes have been identified, it will be up to the data controller to determine what data are really necessary for each of these purposes and to apply appropriate retention periods to each of the categories of data collected.

➢ **On the purposes of websites**

Personal data may be collected for **several purposes**, provided that these purposes are:

- **specific**;
- **explicit**;
- **légitimate**.

Examples :

- presentation of the company and its services
- a contact section for visitors
- newsletter subscription
- creation of a customer account
- online payment

If a site includes discussion areas, the subjects discussed there must be controlled to avoid any liability arising from comments made by users (paedophilia, incitement to violence, racial hatred, etc.). This will require the appointment of a moderator.

➢ **On the data collected**

in accordance with the provisions of article 4 of Law no. 1.565 of December 3, 2024 on the protection of personal data, the personal data collected must be « *adequate, relevant and limited to what is necessary with regard to the purposes for which they are processed* ».

The data controller must therefore take care to collect only the information it needs for each of its website's purposes. If the site is already in place, the data collected should be reviewed and any that is not or is no longer necessary deleted.

This may mean, for example, adjusting the forms used to collect personal data from visitors.

➢ **On the retention period of collected data**

In accordance with article 4 of Law no. 1.565 of December 3, 2024, personal data may only be kept in a form that allows identification of the data subjects **for as long as is necessary to achieve the purposes for which they are processed.**

Example: a company's employee information on a website must be deleted as soon as the employee is no longer in post.

It is therefore important to observe the following rules:

- delete the data and contact details of an Internet user who does not respond to the data controller's requests within **a maximum period of 3 years;**

- retain data relating to the browsing habits of an Internet user for **a maximum of 13 months**, starting from the date on which the cookie is deposited;

- delete data not required for internal purposes, once these purposes have been achieved;

- systematically delete the data of people who have asked not to be contacted by the data controller, or archive them for payment purposes or for the purposes of prescription if transactions have taken place.

Special case of bank data retention
Bank details may be stored in an interim archive for thirteen months following the debit date, to serve as evidence in the event of a transaction being contested. This period may be extended to fifteen months to take account of the possibility of using deferred debit payment cards. Data may be kept for longer, subject to the customer's **express consent**, with prior notification of the purpose (facilitating payment for regular customers, for example). Such consent may be obtained by means of a checkbox, **rather than being pre-checked by default**, and may not result from the acceptance of general terms and conditions. Data relating to the visual cryptogram must not be stored. When the card expiry date is reached, the card data must be deleted.

What about copies of identity documents?
Copies of identity documents may be kept for a maximum of 6 months when they are used to verify the identity of a bank cardholder, and must be destroyed as soon as the identity of the data subject has been verified in the case of requests for reimbursement or remote payment.

A duty to provide information on the collection of personal data

The data subjects must be informed, in the general conditions and/or in a dedicated section of the personal data confidentiality policy on the site, of their rights in application of article 10 of Law no. 1.565 of December 3, 2024.

- **On the data subjects**

The data subject of a processing of personal data is the **natural person to whom the data** being processed relate.

In the case of websites, the following persons may be concerned:

« *All site visitors* »: particularly in the case of cookies and e-commerce sites;
« *employees* »: when their personal data are displayed on the site or are subject to traceability (for example: surname, first name, function, contact, photo, login, connection logs);
« *customers* »*:* in particular when creating accounts.

- **On the information to be provided**

Under article 10 of Law no. 1.565 of December 3, 2024, the data controller must take **appropriate measures** to provide the data subject with information on the use of his or her data and to facilitate the exercise of his or her rights.
This information includes:

- **the identity and contact details of the data controller**, and where applicable, its **representative** established in Monaco or, failing that, within a Member State of the European Union;
- the **purpose**s and **legal basis** for the processing;
- the **categories of personal data** concerned;
- the **period for which the data will be stored** or, where that is not possible, the criteria used to determine that period;
- where processing is based on **consen**t, the right to withdraw consent **at any time;**
- the **recipients** or **categories** of recipients;
- the means of exercising their **rights of access, opposition, rectification, deletion, limitation** or **portability**;
- the right to **object to the use** of their data **on behalf of third parties** or to **the communication** to third parties of personal data concerning them **for prospecting purposes**, in particular for commercial purposes.

For websites, this information must be provided via the **General Terms and Conditions** and/or a **page dedicated to the personal data privacy policy**, easily accessible on the website.

However, there are a number of situations in which this information is not sufficient. For example, the Internet user's consent must be expressly requested in the case of commercial prospecting by e-mail and, in certain cases, when cookies are used.

ⓘ **Information**
Cookies are small files that are placed on a user's computer by the website at the time of consultation. These files then record information about the user, including personal data. The information collected in this way can then be analyzed to facilitate site navigation, offer targeted advertising and analyze browsing habits. However, cookies have no access to the contents of the user's computer. There are several types of cookies: - technical/functional cookies (including audience measurement cookies) ; - third-party application cookies - cookies from advertising partners; - optional cookies.

Where consent is required, it must be possible to withdraw it quickly and easily.

- **Case of data transfers to a country without an adequate level of protection**

Such a transfer of data collected by the websites, in particular to the United States of America, may occur, for example, when the said websites use service providers for the following services:

- statistics, cookies, Google Analytics ;
- newsletter ;
- hosting;
- ReCaptcha ;
- Online payment.

NB : The list of countries with an adequate level of protection is available on the APDP website.

The Internet user must be informed of the transfer, and in most cases consent to it, and measures must be taken to ensure the confidentiality and security of the data transferred.

Examples :

Google Analytics
When a website uses **Google Analytics**, the following data are sent to Google Inc. in the USA: IP address, Internet domain name of the user, pages visited and their number, number of views per page, time spent on each page, number of clicks, name and version of the user's web browser, user's operating system, time stamp of access to the site and pages visited on the site. The APDP has the following requirements! - a « *Cookie* » banner must be displayed to allow Internet users to accept or refuse the deposit of cookies on their terminal; - this information banner must appear when the site opens, before any cookies are deposited, and without the user having to take any action whatsoever; - this banner must inform Internet users of the transfer of their data to the United States, a country that does not offer an adequate level of protection; - if the user refuses to accept the cookies, he/she must be informed that his/her request has been taken into account. He/must must also be able to continue browsing; - in the section dedicated to the cookie policy, Internet users must be able to change their settings and withdraw their consent at any time. However, there are European (European Union) alternatives to Google Analytics. Their use does not require a **cookie banner** on the website, as there is no transfer of data to a country without an adequate level of protection. Furthermore, if the last two bytes of the IP address are anonymized, there is no need to obtain the user's consent for the collection of statistical data.

Mailchimp
Mailchimp is a marketing automation platform and email marketing service. It enables customers to create e-mail communication campaigns. Users can personalize their campaigns according to the segmentation criteria of their contact base. The platform also offers the possibility of sending automatic e-mails based on events or characteristics associated with a contact. The aforementioned platform is located in the United States, and therefore involves the transfer of data to a country that does not offer an adequate level of protection whenever a website uses it. As a result, the APDP requests that anyone wishing to subscribe to a newsletter managed by this platform be warned by a message that their data will be hosted by the US-based service provider Mailchimp. It also requests that this person be able to unsubscribe from the newsletter at any time, thereby withdrawing his or her consent.

Google ReCaptcha
The « *ReCaptcha* » feature distinguishes humans from robots. It consists of a « *I'm not a robot* » checkbox, often supplemented by an image recognition test. The APDP prohibits the use of this Google ReCaptcha, which results in the transfer of personal data to the United States without the prior consent of users. To distinguish a human from a robot, however, solutions similar to this ReCaptcha are available on the market from countries with an adequate level of protection. ReCaptcha functionality can also be developed in-house by the technical departments of data controllers.

A data security obligation

Article 31 of Law no. 1.565 of December 3, 2024 specifies the security obligations incumbent on data controllers.

They must take **appropriate technical and organizational measures** to guarantee a **level of security appropriate to the risks** to the rights and freedoms of the data subjects.

The adoption of these measures requires an **analysis** to identify the risks, and then to determine their **level of probability** and **seriousness**.

In accordance with the law, the risks incurred include the following

- data destruction ;
- loss of data;
- alteration of data;
- unauthorized disclosure of data;
- unauthorized access to personal data.

These risks may arise **accidentally** or **unlawfully**.

This is why, when it comes to websites, the data controller must take measures to ensure not only **data confidentiality**, but also **data security.**

- **Measures to ensure data confidentiality**

- access to data is restricted to those who need to know them. Depending on their activity, these people may only have access to certain categories of data (for example, the accounting department may only have access to the identity and address of an Internet user, as well as information linked to the purchase it needs to invoice, without necessarily having access to other information potentially collected on the customer);

- **access to administration tools and interfaces must be restricted to authorized personnel only. In particular,** the use of administrator accounts **should be restricted** to IT staff, and only for those administrative actions that require an access;

- authorizations and passwords must be regularly updated to ensure that only authorized personnel can access the data required to carry out their tasks;

- a **logging mechanism for processing operations and accesses** must be set up;

- maintenance operations must be **traceable**, and stored equipment must no longer contain personal data. Particular care must be taken when changing equipment, especially hard disks, which can be a source of data leakage if they are not properly erased when disposed of.

How to protect copies of identity documents?
With regard to **identity documents**, the APDP is particularly vigilant about the way in which they are collected. The aim is to combat identity theft and usurpation, the illicit use of personal data contained in these documents and the consequences this may have for victims. As far as e-commerce sites are concerned, data may only be collected for the purposes of verifying the identity of a bank card holder or to manage requests for payment or reimbursement following participation in a game. The APDP requests that remote collection methods be protected and in particular that copies of identity documents be deposited on a secure page. It also recommends that people whose copies of identity documents are collected be asked to send these in black and white and crossed out, to make it difficult to reproduce them.

How to protect credit card data?
The data required to carry out a remote transaction by payment card are the cardholder's name, card number, expiry date and visual cryptogram. The use of online payment methods and the storage of bank card numbers must be subject to traceability measures enabling any illegitimate access to the data to be detected *a posteriori* and attributed to the person who accessed the data illegitimately. As bank card data is particularly sensitive, it is important to know which members of the e-commerce site's staff may have accessed it. The data controller must take the appropriate organizational and technical measures to protect the security, integrity and confidentiality of bank card numbers against any unauthorized access, use, misappropriation, communication or modification by using secure payment systems that comply with the state of the art and applicable regulations. In particular, these data must be encrypted using a strong algorithm. Where the data controller keeps bank card numbers for the purpose of providing evidence in the event of a transaction being disputed, these numbers must be subject to technical measures designed to prevent any illegitimate re-use or any re-identification of the data subjects. These measures may include storing bankcard numbers in hashed form using a secret key. In addition, given the sensitivity of this data, the payment card number may not be used as a commercial identifier. The data controller or its service provider must not request the transmission of a photocopy or digital copy of the front and/or back of the payment card, even if the visual cryptogram and part of the numbers are masked. When the payment card number is collected by telephone, security measures must be put in place, such as the traceability of access to card numbers. An alternative secure solution, at no extra cost, must be offered to customers who do not wish to transmit their card details by this means.

- **Measures to ensure data security**

Security measures for premises and information systems must be put in place to prevent files from being distorted, damaged or accessed by unauthorized third parties.

The TLS protocol (replacing SSL) must be implemented on all websites, using only the most recent versions and verifying its correct implementation.

The use of TLS should be mandatory for all authentication pages, form pages and pages on which non-public personal data are displayed or transmitted.

Only communication ports that are strictly necessary for the proper operation of installed applications should be retained. If access to a web server is via HTTPS only, only incoming IP network traffic to this machine should be authorized on port 443, and all other ports blocked.

The number of components used must be limited and kept up to date.

A technical watch must be set up to ensure that security is **always** up to date.