ELEARNINGNEWS ARTICLE

Year 6 - number 202 Wednesday 11 may 2022

# E-learning and privacy, how to navigate the web

***How to protect oneself from hacker attacks and the dissemination of data provided on the web? Here are the strategies that platform operators and users can follow to avoid privacy threats***

Smart working, distance learning and online courses. **E-learning**, and new technologies in general, have become an important part of everyday life, affecting various aspects of daily routine. From school to work to leisure time, more and more people are turning to online platforms to access training and refresher courses, videoconferences, remote meetings, but also games and music. The increase in the use of these platforms and the evolution of new technologies also brings with it another aspect: the other side of the coin is represented by cyber threats, which are becoming increasingly sophisticated and deceptive for users, who are exposed to different potential risks each time. For this reason, attention to **privacy** and the protection of data provided on the web has become a fundamental aspect to be taken care of, both by those who surf the Net and by the person responsible for data processing.

In Italy, the main reference figure in this area is the **Garante per la protezione dei dati personali**, the authority responsible for protecting rights and ensuring respect for dignity in the processing of personal data. The reference legislation is the General Data Protection Regulation, approved by the European Parliament and Council in 2016 and in force since 23 May 2018.

## Privacy: the rules

The General Data Protection Regulation (GDPR) refers to the "wholly or partly automated processing of personal data" and lays down the rules for navigating the Internet in the field of privacy protection. The document specifies the cases in which it is appropriate to proceed with the processing of personal data. In particular, for this to be lawful, at least one of the following **conditions** must be met:

- The data subject has given consent to the processing;
- The processing is necessary for a contract, such as those for the provision of services or subscriptions;
- The processing is necessary for a legal obligation, such as when the employee's data must be provided to Inps;
- Processing is necessary to safeguard the vital interests of the person, for example for health reasons;
- Processing is necessary to carry out a task carried out in the public interest or for the exercise of public authority, such as in schools or public administration;
- The processing is justified by legitimate interest, as in the case of bank audits.

The request for **consent** to process personal data must be made in a 'clearly distinguishable manner' and in a 'comprehensible and easily accessible form, using simple and clear language'. Transparency and clarity are therefore the fundamental characteristics on which the data controller must focus in order to ensure that the data subject is able to give his consent to the processing of his data in an informed manner.

Once consent has been given, however, the user can always withdraw it. Article 7 of the Data Processing Regulation, in fact, recalls that 'the data subject shall have the right to withdraw his consent at any time'. But even if consent is withdrawn, the lawfulness of the processing is not affected.

## Cookies: what they are and what they are used for

Usually, when you surf the Net, when you open a web page or a platform, a window warns you of the presence of Cookies. But what are Cookies and what are they used for? And why are they important for privacy? **Cookies** are files that websites visited by users send to the device from which they are browsing, which stores them and transmits them to the same sites the next time they visit. Cookies make it easier and quicker for users to access websites because they store information when they first access them, and they can simplify the experience by keeping track, for example, of items previously placed in an online shopping cart. In addition to these functions, cookies are also very useful for website operators, who use them to collect and process personal

data, such as IP address and e-mail address.

Last June, the Italian Data Protection Authority approved new guidelines on cookies and tracking tools, according to which data controllers are required to provide users with transparent and accessible information. In order to do so, the information must be in plain language and multi-layered, e.g. using pop-ups. The Garante points out that cookies can be both technical and non-technical. In the first case, the information notice can be placed on the home page, while in the second case, a clearly visible pop-up banner must be used, containing:

- A command to close the banner;
- An indication of the use of Cookies;
- A link to the privacy policy, containing the full privacy statement;
- A command to accept all cookies;
- A command or link to choose which cookies to accept.

# E-learning and privacy

The use of **LMS platforms**, intended for e-learning, also implies the processing of the users' personal data. The use of a platform allows the owner to collect various data about people accessing the course, such as date of birth, e-mail address, telephone number, first and last name and the profile with which the user is registered on social networks. For this reason, greater attention must be paid to data processing, both by the operators of these platforms and by the user.

Read also **eLearning and GDPR**.

The operator must ensure that it acts in a way that complies with the Data Protection Regulation, by providing a clear, easy-to-understand and accessible **privacy policy**, and by making the conditions of use of the LMS in question clear. To protect the privacy of users, the LMS provider must not collect more data than is necessary for the purpose, nor use it for purposes other than those stated. Article 13 of the European Regulation sets out the information that the data controller is required to provide to the data subject when requesting the data. In general (and therefore also for the processing of data in an e-learning platform), the information must contain:

- Contact details of the data controller;
- Contact details of the data protection officer;
- The purposes of data processing and the legal basis for processing;
- Possible recipients of the data;
- Any intention of the data controller to transfer the data to third parties.

Once the data have been obtained, the data controller must also indicate the data retention period, the existence of the data subject's right to request access to the data, the possibility of withdrawing consent and the right to lodge a complaint with the supervisory authority.
In order to ensure that they are acting in accordance with the Regulation, the platform operator and the data controller can make use of the numerous **e-learning courses** on privacy, i.e. training courses carried out remotely, with the help of an LMS platform, in which the basics of the rules for managing personal data are explained.

On the one hand, therefore, the operator must ensure that the purposes and methods of processing are respected, but on the other hand, users should also adopt the necessary strategies to protect themselves.

# How to protect yourself?

To ensure that users' **privacy is protected**, the platform or site operator and the owner must adhere to data processing guidelines. But what can individual users do to **keep their data safe**? The following strategies can be used to make sure that your data is kept safe:

1. Use security software: to prevent a hacker from breaking into your devices, it is a good idea to install **antivirus software**, which can protect your PC, smartphone and tablet. To ensure effective protection, however, it is not enough to install antivirus software: you need to keep it updated and schedule regular scans to check for security threats on your

device.
2. Use a **virtual private network** (VPN) to hide your IP address and encrypt your internet traffic.
3. Make your **social** profiles private, to prevent unknown people from accessing your data and viewing your posts or locations.
4. Use an intruder-proof **password** that does not allow others to easily access your emails, profiles or data.

With regard to the last point, the Data Protection Authority gives some tips to guide users in setting a secure and **privacy-proof password**. To achieve this, your password should have the following characteristics:

- Be at least eight characters long;
- Contain at least four different types of characters: upper and lower case letters, numbers and special characters (such as punctuation marks);
- Not contain personal references that are easy to guess, such as first and last names;

It would also be useful to set a password with fancy words, as there is software that can decipher commonly used words in various languages. Choosing a password to keep your data safe, however, is not enough. It would be a good idea to periodically update passwords and use multi-factor authentication mechanisms (such as OTP codes or text messages). It is better to vary the passwords protecting different accounts, not to use passwords that have already been used in the past and to avoid writing it on cards or sharing it via email or text messages.