Subjects: Data Access
Occupation: Information Systems Manager
Data type: Private

Can I use the data from my clients / users at the end of the surveys?

An organization provided its customers / users with a commercial site to purchase items online. To do this, an email address and their password is required. After a few years of operation, the site lists hundreds of customers / users.
The Information Systems Manager of the organization decides to use this data at the end of the surveys. Interested in data security, he wants to use this information to investigate the precautions that the customers / users took or didn't take: Did they use the same password for their email account and access to shop?
The Information System Manager retrieves the passwords from the online shopping site and attempts to enter the email accounts of its customers / users by using the passwords they chose for the commercial site. He takes certain measures to respect the privacy of the customers / users (does not look at the messages, does not store passwords, etc.).
Made aware of the investigation, his superior asked him to stop, as he does not have the customers / users consent. He knows that this method is not acceptable: Passwords are confidential and should not be accessible in any way.
The data collected to allow online purchases may not be used for any other purpose. In addition, illegal access to a computer system is a criminal offence.

Recommendations

The data collected is for one purpose (to allow online purchases) and cannot be used for other purposes (to investigate the level of security applied by customers or users). This principle applies to all forms of research or inquiry, whether scientific or commercial. In this case it is necessary to have the definite consent of the data subject, as there are no overriding private or public laws allowing its use for other purposes. Passwords should not be stored in clear text in the database but for example through "hash" values so as to be secure and inaccessible.

Basic principles

LIPAD 37 al.1 and 2 ; CP 143, 179novies ; DPA 4, 7, 12, 13, 17

Legality, data security, transparency of the collection, purpose

Resources