aepd agencia española protección datos

www.aepd.es @AEPD_es

PRIVACY RISKS OF INTERNET OF THINGS AT HOME

Televisions, toys, robot vacuum cleaners, lightbulbs, alarms, loudspeakers or doorbells are just a few examples of devices which can be operated though the Internet.

When using smart devices at home, some risks for our own privacy and that of others living with us or visiting us may appear. Knowing them is key to prevent them.

A device does not know its users' voice: it can collect and storage voice data, images or information of third persons (other family members or guests) without them being aware of it.

Besides those data directly and consciously fed to the device by us, devices include sensors to catch and store other data, including images and audio.

Many companies that take part in the service provisions (device manufacturers, software developers, service providers, etc.) could access our data and process them for further purposes.

Combining collected data with information from other users allows to obtain information regarding out habits, behaviour and/or physical status.

Some devices can track our movements, and, at the very least, they can locate us at a certain point, over a certain period of time.

The sheer volume of data ant its combination with information from other devices allows to elaborate accurate profiles of our habits, preferences and device usage.

Even when we are not directly and consciously interacting with a device, it can still be collecting and processing personal data.

Any Internet-connected device with default insecure settings or unresolved vulnerabilities can become the access gate to cyber criminals in search of exploiting our personal data.

Personal data are processed by third parties who, in case of undergoing a security breach, may be exposed.

SECURE USE RECOMMENDATIONS FOR INTERNET OF THINGS AT HOME

Follow these recommendations to improve your privacy if you use smart devices.

1. The fundamental right to data protection also depends on you:

- Consider which data are required for each device and do not provide more data than necessary.
- Review the information provided by the manufacturer, and, if in doubt, consult their Data Protection Officer.
- Only give consent to the purposes that suit your preferences and needs.

2. Choose products by manufacturers and providers that provide privacy and data protection guarantees and that commit to provide security updated throughout the useful life of the project.

3. **Before** purchasing a product, inform yourself through the privacy policies about:

a. Who will process your personal data and how can you contact the Data Protection Officer.

b. Which type of data are to be processed and for which purposes,

c. If your personal data are to be transferred to third parties and for which purposes,

d. How you can exert **your rights** regarding personal data protection, including your **right to data portability**.

4. **During commissioning,** ensure to review and set up your preferences and the **privacy and security options**. You must be able to give your consent or express your **right to object** to the different purposes. Always change default **usernames and passwords**. Ensure to update the device. Disable any function you're not going to use.

5. **While using** the device:

a. Ensure that the device can be disconnected when not in use, and in such case enable the mode that disables data collection.

b. Regularly review privacy and security updates.

c. Install any available security updates.

6. **When you discontinue using** the device:

a. Do not keep an obsolete, unused or not-updated device connected to the internet.

b. You are entitled to request the erasure of your personal data, and it is convenient to remove any user accounts in those data provider which you are not going to use.

c. You can also exercise your **right to portability**.

d. Erase any data that the device could contain **before selling or recycling it**.