



M-Sec EU and Japanese IoT citizens and stakeholder's consultation

M-Sec has launched its e-consultation survey to the European and Japanese IoT community. Help us by taking the survey and providing us with your feedback

The [M-Sec Project](#) was born in July 2018, as an EU and Japanese R&D project made by [twelve partners](#) (six European and six Japanese). The main motivational factor arose from the fact that many data sources in the IoT and smart city domain may contain sensitive information that raises issues on privacy and data protection. The main objective sought by M-Sec was, thus, to develop a framework that provides security and integrity of data traffic, end to end, from the device to the Cloud and to the application in a secure and transparent way.

The M-Sec survey

In the scope of this research, the project is conducting an **online survey to all EU and Japanese IoT citizens and stakeholders**, considered as potential users of the M-Sec solution, to collect feedback on their experience when using IoT devices and applications and on their knowledge of EU and Japan's data protection regulations.

The main goal of this survey is to help the project better understand the IoT ecosystem in which M-Sec is expected to operate, what are people's main IoT habits and their awareness regarding data protection regulation in their region.

Filling in this survey will not take more than 1 minute.

Preliminary results

From an initial sample of 250 answers, most respondents (56%) identified health devices – such as fitness bracelets – as the IoT device that they most commonly use, followed by smart watches, home devices and appliances and voice assistants. 36% of respondents seem to use those devices every day, all day, which shows how they are becoming part of citizens daily lives and routines. However, most of them (53%) are not fully aware of security and privacy data protection policies of the IoT devices and applications they use, meaning that they do not always carefully read those policies when start using a device of application or when those policies are updated by the provider. Therefore, when confronted with a hypothetical scenario in which a given IoT device or application suffers a cyber-attack, respondents prefer to stop using that device or application immediately and go through the data protection policies to become more aware of their rights. Main privacy and security concerns seem to be more related with the wrongful use of data by others (>60%) than the actual malfunction of the IoT device or application itself. Regarding EU and Japan's GDPR and APPI data protection regulations, EU respondents show a satisfactory level of awareness (>80% are fully aware or have heard about it), while most Japanese respondents are not acquainted with their data protection rights.

Want to take part in this survey and help our project?

[Fill in the survey here](#)

Get involved!

Visit www.msecproject.eu • Join our community on [Twitter](#) & [LinkedIn](#) • Send us a message to hello@msecproject.eu • Check out our [Resources](#) and [News](#) sections



The M-Sec project is jointly funded by the European Union's Horizon 2020 research and innovation programme (contract No 814917) and by the Commissioned Research of National Institute of Information and Communications Technology (NICT), JAPAN (contract No 19501).