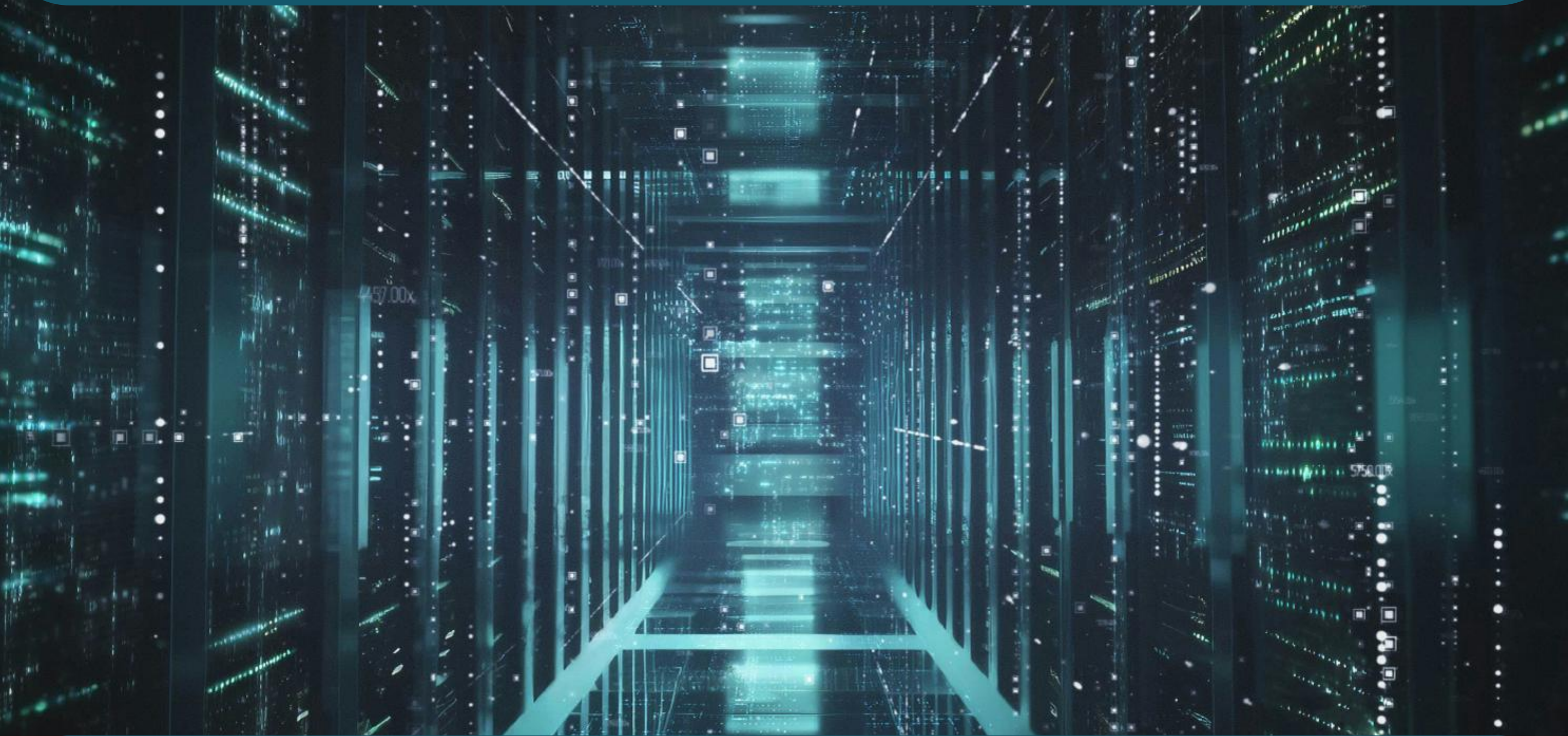




Wearable Devices and Cybersecurity Vulnerabilities

Smart glasses remain a European enforcement priority

The European Data Protection Board (the “**EDPB**”) – the body that brings together the national data protection authorities of the European Union to ensure the consistent application of the Regulation EU 2016/679 (the “**GDPR**”) – adopted, at its plenary meeting that concluded on 14 October 2026, **Statement 1/2026 on the data protection challenges raised by smart glasses**, that is wearable devices that look like ordinary glasses but incorporate cameras, microphones, internet connectivity and, increasingly, artificial intelligence functionalities such as real-time translation or facial and voice recognition; the Italian Data Protection Authority (“**IDPA**”) published its own press release the same day summarizing the findings for the Italian market.

Because their discreet appearance means that people nearby may be recorded or filmed without realizing it, the EDPB notes that the risks are even greater in sensitive environments such as hospitals, schools, changing rooms or workplaces, with children especially exposed. The statement clarifies how responsibility is shared: **a person who uses smart glasses for purely personal or household purposes is not subject to the GDPR at all**, under what is commonly referred to as the household exemption, although the use of the device may still be governed by criminal, civil or employment law; by contrast, **a person who shares images on a public social media profile, or who uses the device for official or professional activities, is considered a data controller and is therefore subject to the corresponding obligations**, as are manufacturers and providers of related applications or services whenever they determine the purposes and means of the processing, who cannot transfer their own obligations, including transparency obligations, onto end users. **Transparency** is identified as one of the central challenges, bystanders should be able to recognize when they are being filmed, and the EDPB recommends that manufacturers and providers adopt visible, reliable and hard-to-disable indicators, such as lights, sounds or distinctive designs, that make smart glasses clearly distinguishable from ordinary glasses.

Any processing falling within the scope of the GDPR must in any event rest on a valid legal basis, which the statement notes can be difficult to establish given that consent is hard to obtain from people recorded unknowingly and reliance on legitimate interest requires careful balancing. To reduce these risks, the EDPB encourages controllers to adopt **technical measures** such as limiting continuous recording and retention periods, blurring faces, pseudonymizing data, restricting use in sensitive locations, and slowing down sharing on social media, with particular protection for minors. For businesses, this is a clear signal that wearable AI devices should be factored into existing privacy governance frameworks covering device deployment, data retention and accountability among manufacturers, providers and business users; employers in particular should assess the implications for workplace monitoring and the rights of workers and visitors, since further supervisory guidance is to be expected.

The EDPB's statement focuses on data protection, but smart glasses raise an additional issue that is likely to become more significant as this category of devices becomes more widespread: the classification of data generated as a byproduct of normal device use – as occurs with other connected devices – which may be, for example, **technical operating data and fall within the scope of the Data Act** (Regulation EU 2023/2854 on fair access to and use of data), which requires connected products to be designed so that the data they generate can be shared and gives users a right to access it and, in some cases, to have it shared with third parties, provided that they comply with data protection laws if personal data are involved. For manufacturers and providers, this means that data governance for smart glasses cannot be designed around privacy compliance alone: it should also account for the device's status as a connected object, and for the possibility that both personal and non-personal data flows may need to be made shareable under the Data Act.

ACN issues urgent warning on “PHP2Shell” exposure

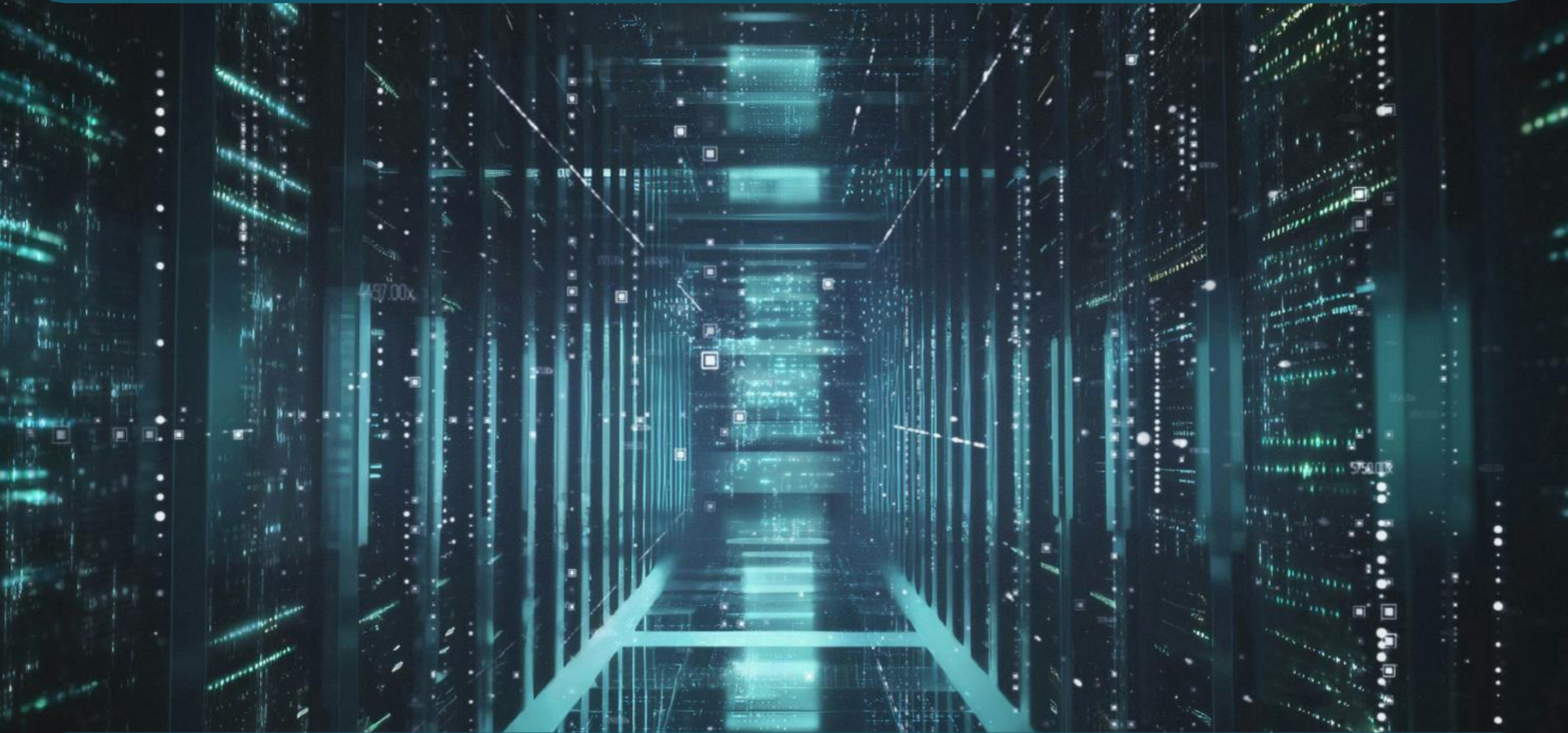
The Italian National Cybersecurity Agency (“**ACN**”) warned, on 21 October 2026, of two critical vulnerabilities affecting *php-src*, a core component of PHP, one of the most widely used programming languages for building websites and web applications. The vulnerabilities, which have since become known as “**PHP2Shell**”, are tracked under the identifiers CVE-2026-109618 and CVE-2026-109619 (CVE – Common Vulnerabilities and Exposures, is the public reference system used worldwide to identify known cybersecurity flaws). Both received the highest severity score on the standard scale used to measure the seriousness of security vulnerabilities. On 23 October 2026, ACN flagged a further, related vulnerability, CVE-2026-115560, which may likewise allow remote code execution under certain application and configuration conditions and for which, at the time, the vendor had not yet released a patch, having indicated only a temporary mitigation.

On 25 October 2026, **ACN reported that**, based on monitoring carried out by CSIRT Italia, **approximately 81.9% of the PHP services identified nationwide with a known version may be vulnerable to the PHP2Shell attack chain**, corresponding to roughly 285,000 potentially vulnerable services out of around 741,000 detected in the country, noting that exploitation attempts had already been observed and that proof-of-concept exploit code was publicly available, and calling on administrators to act with the utmost urgency, prioritizing systems directly exposed to the internet. ACN recommended (i) immediately updating PHP installations in line with the vendor’s advisories; as an immediate mitigation for CVE-2026-115560, (ii) disabling the related session file-upload progress-tracking functionality pending a patch; where available (iii) configuring web application firewalls in blocking mode; and, where none of these measures can be applied in time, (iv) considering taking the exposed services offline.

It also recommended retrospective checks of logs and security events for signs of prior exploitation, such as unusual web requests, memory-related errors, unexpected process interruptions, or subsequent suspicious activity. The warning is operational rather than regulatory, but businesses should not treat it as a purely technical matter: a publicly known, critical vulnerability of this kind sets a visible benchmark for what adequate cybersecurity measures look like and ignoring it can later weigh against an organization when its compliance with the EU's NIS framework or with data-protection rules is assessed, particularly if an incident occurs in the meantime.

Data Law Alert

○ Data Law



For further information, please contact:

Andrea Fedi
afedi@legance.it

Lucio Scudiero
lscudiero@legance.it

Martina Balzani
mbalzani@legance.it