

Eric Leijonram, Director-General: Data Protection Today – Reflections and Priorities from the Swedish Authority for Privacy Protection

Keynote speech at Nordic Privacy Arena, Stockholm,
28 September 2026

Working with data protection in 2026 means being at the heart of a historic transformation of our society. It means standing precisely where technological development meets people and society.

Personal data is collected, processed, and even bought and sold, in astronomical volumes – every second, every day. And now, as artificial intelligence and other technologies are rolled out across one sector after another, this is accelerating. The volume of data that can be collected about us is increasing, as is what that data can be used for.

Technological development is moving at a breakneck pace, yet we are only at the beginning of this shift. This is, of course, about AI, but also, for example, 6G, quantum cryptography, wearables, neurotechnology, nanorobots, and much more.

This technological shift has consequences for issues of welfare and entrepreneurship, for innovation and working life. Both criminals and law enforcement agencies gain new tools. It affects Sweden's preparedness and competitiveness. It touches every part of society, spanning from everyday life to major geopolitical contexts. Questions about what others are allowed to do with our personal data become central.

Data protection regulates what should take priority when different interests collide, but also how we can find solutions to use new technology to solve problems safely, with respect for our fundamental right to privacy.

Postadress:

Box 8114
104 20 Stockholm

Webbplats:

www.imy.se

E-post:

imy@imy.se

Telefon:

08-657 61 00

The Global Landscape

The technological shift makes the future, to put it mildly, difficult to predict. That this development is taking place in the current geopolitical situation makes it no less uncertain.

I am thinking of Russia's war against Ukraine and the security incidents occurring across Europe. I am thinking of China's increasingly assertive position as a global power and the tensions associated with it. And I am thinking of the unpredictability of the U.S. administration and its new relationship with its EU allies, including us in Sweden.

Surrounding President Trump are the major tech companies. They largely drive economic growth in the U.S., which makes them global power players, while they, in turn, depend on a capricious president. We have all seen how quickly tech companies rename large bodies of water on their maps when Trump requests it. It may be easy to laugh at the focus on lake names, but it says a lot about the president's power and his view of the limits, or lack thereof, of his role. And this has major implications as regards data protection.

The EU Commission's adequacy decision from 2023 enables the transfer of personal data to the U.S. But since Trump took office, he has dismissed democratic members of the Federal Trade Commission, a central authority for data protection. This summer, the U.S. Supreme Court ruled in Trump versus Slaughter that the president has the right to do this without cause. The ruling raises questions about the independence of supervisory authorities in the U.S. and could undermine the adequacy decision.

Let me be clear, the adequacy decision still stands, but organizations transferring personal data to the U.S. should monitor developments and prepare. Can they retrieve their data if necessary? What are the consequences of a change, for operations and for individuals' rights?

The altered relationship with the U.S. is hardly temporary but rather the new normal. The Greenland crisis exposed our dependence. We need more Swedish and European alternatives to American tech services to ensure resilience and sovereignty. This does not mean that European solutions are always better from a data protection perspective, but every organization must map its data flows, risks, and dependencies.

When hearing the debate's focus on digital sovereignty, it is easy to get the impression that this is the direction we are heading. But the reality is that dependence is increasing as organization after organization rolls out AI and stores more and more data in American cloud services. Now, many praise sovereignty and control. This is good. But it's necessary that words are followed by action.

To put it bluntly, this means that dependence on American tech services must be reduced, especially when it comes to sensitive data and functions that affect our resilience. This applies to both private and public sector operations. It is no small matter.

What is needed here is clearer governance and bold decisions, something I have discussed before. I'm aware that this may seem foreign to Sweden's decentralized

administrative model, which is fundamentally sound and worth defending. But it is clearly problematic that agencies and municipalities, often with limited resources, are left to take responsibility for their own IT infrastructure and AI adoption. We would hardly accept such fragmentation when it comes to the country's highways or transport networks. Change is necessary.

The lack of governance and decisive action has contributed to an over-reliance on American tech services, leaving us without the sovereignty and control that are essential.

Omnibus

When I spoke here a year ago, momentum was building regarding simplifications to the GDPR. Since then, much has happened. In November, the EU Commission presented its Digital Omnibus with proposals for extensive changes.

The proposal is now being negotiated in the Council and the Parliament. The Irish Presidency in the Council has made this a priority, and it can therefore be assumed that work in the Council will progress quickly, possibly finalized before the end of the year. However, I do not believe this will be the last initiative in this area.

From IMY's perspective, we have wanted greater clarity and to avoid legal uncertainty. Many advances appear to be made, though we wanted to go further in adopting a more risk-based, pragmatic approach to the regulation. Here, progress may not be as significant as we had hoped.

IMY – Priorities

So, what is happening at IMY? We have three priorities for guidance and supervision in 2026: children and young people, AI in the public sector, and law enforcement.

As you know, children are a particularly protected group under the GDPR. We and our sister authorities in other countries have provided guidance with a new app aimed at children about data protection in social media, FantomApp. It was developed by our French counterpart, CNIL, and IMY has adapted it for Swedish conditions. The app allows users to learn about their rights, test if their passwords are strong enough, and get step-by-step guidance on security settings in their social media. It is aimed at children, but to be honest, I think it could be just as useful for many adults.

The children's news program Lilla Aktuellt featured the app and had 12-year-olds test it. One child's verdict was "pretty okay." Coming from a 12-year-old about an app developed by an authority, I think that could be seen as high praise.

We have also produced guidance on streaming children's and youth sports. Across Sweden, sports clubs broadcast matches where children and young people compete. Many children think it's fun, while others find it uncomfortable that anyone can see what they did on the field. And if a child has a protected identity, streaming a game naturally becomes a serious matter. There has been uncertainty about what applies, but now there is comprehensive guidance on what determines legality.

Our second priority area is AI in the public sector. Here, we have, among other things, the report on transcription in social services which we published this spring, a report long awaited by many public sector organizations across the country. We have also, as of recently, started a new sandbox project on AI agents for decision-making chains in healthcare and social care.

In the field of supervision, we have an ongoing review of Region Gävleborg regarding AI-based transcription in primary healthcare. The review concerns their security measures and among other things, includes how the service is used and how incorrect transcriptions are handled. This is a review I know many are following.

The third priority area is law enforcement. Law enforcement agencies have gained many new tools in recent years, and as they start to be used, our role as a supervisory authority becomes important. The area is prioritized because serious crime has devastating consequences for those affected and impacts society as a whole, but also because the tools raise many privacy issues. Among other things, we have a new role as the market surveillance authority for the police's real-time facial recognition.

Law enforcement is not just about supervision; it also requires close dialogue with the Police Authority and others to provide guidance and advice. As in all operations, data protection works best when it is integrated from the start, not added as an afterthought.

IMY – Operations

Sweden has a situation with search services that does not exist elsewhere in Europe. Anyone can easily find a great deal of information about us online, for any purpose. This is a privacy issue in itself and takes on new significance in light of the serious security situation we are facing. This largely concerns the system of voluntary publication licences. When the system was introduced, the legislator saw a risk that it would create vast registers of persons – and so it has.

IMY has four ongoing supervisory cases in this area, two concerning personal data relating to criminal offences and two regarding the right to erasure of other types of personal data. Now, we have received the EU Court of Justice's ruling on the matter, and I expect a conclusion to our supervisory cases before the end of autumn.

But I also expect that we will continue discussing how the ruling affects the relationship between our constitutional laws and the GDPR. In my view, the legislator will need to act, in one way or another. The collections of data published by search services, with their significant privacy implications, are natural for us to review. But I do not want IMY to be forced into becoming an authority that scrutinizes publications in constitutionally protected media engaged in journalistic activities. The Swedish exclusivity principle in media constitutional law is an indispensable part of our system of government. It must continue to be defended.

Among the major concluded cases this year are the supervisions of Miljödata and Sportadmin. Both cases involved data processors servicing hundreds of data controllers and personal data on large parts of Sweden's population. In both cases, we found that the technical and organizational security was insufficient

given the type of personal data that was being processed. Among other things, we emphasized the importance of real-time monitoring to detect suspicious activity in their systems. These are important guiding decisions.

We are continuing our review of our legal opinion on personal data concerning criminal offenses. We have submitted a request to the European Data Protection Board, the EDPB, for clarification regarding which data regarding criminal offenses fall under Article 10. The reason is that we have seen divergence in how Article 10 is interpreted in different member states.

One of the things that has gained much attention this year is our ten tips for individuals using smart glasses. For us, it has been important to be part of the conversation about this new technology and highlight data protection aspects. When a new technology emerges, it is inadequate to step in late in the process when the technology is already established. IMY and data protection need to be part of the discussions from the very beginning, so that we, as a society, can shape development and innovation responsibly, together.

Looking a year ahead, much suggests that the *Integritetsskyddsmyndigheten* will be renamed the *Dataskyddsmmyndigheten*. The Data Protection Agency. We raised the issue of a name change six years ago, arguing that *Dataskyddsmmyndigheten* would better reflect our operations. When we raised the question again this year, a process was initiated by the government. No decision has been made yet, but there is a proposal to change the name in June 2027. Our mission is to work for the protection of people's fundamental freedoms and rights in connection with the processing of personal data – that is, data protection. That is how we contribute to safeguarding privacy in society.

Closing

IMY is on a transformative journey with our sights set on who we will be in 2030. We are working to become open, active, and make a difference. We will prioritize activities that have a real impact on data protection in society.

It is also about the importance of viewing data protection pragmatically. This applies to all of us working with these issues. We must never come to see the law as an end per se. We need to view it as the tool it is. This requires an understanding of the operations to which the rules apply and the ability to balance different interests against each other. Conflicting interests will always exist. It is difficult, but that is also what makes data protection so interesting and important.

We live in a time of transition where new technology is reshaping our society. Data protection helps us navigate these changes. It is about securing the right to privacy even in this new era while finding ways to use technology to improve our lives. That is how we create a safer digital Sweden.