2 October 2024

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

The European Cyber Security Month (ECSM) 2024

Speech by;

Wojciech Wiewiórowski
European Data Protection Supervisor

Safeguarding Digital Europe: Strengthening Cybersecurity and Combating Social Engineering in the European Institutions

I. Welcome remarks - Introduction

Dear colleagues, dear all, allow me first to thank you for inviting me to this kick-off event of the 2024 European Cybersecurity month.

If you followed last year's event, you probably already know that I am the European Data Protection Supervisor. The EDPS is the independent data protection authority of the EU institutions, bodies and agencies.

As of 1st August 2024, I have an additional important role: That of the Supervisor for the EU Institutions that fall within the scope of the EU Artificial Intelligence Act, which is globally the first legal framework on AI.

In addition to these official roles, the EDPS is also a permanent member of the Inter-Institutional Cybersecurity Board, the Cybersecurity Supervisory Authority for EU institutions. Some of you might be aware of a new regulation that entered into force on 7 January 2024, aiming to enhance the overall cyber security level across EU institutions, which also has an important interplay with personal data.

I take up these new important roles with very high sense of responsibility. Nevertheless, in all of these roles, through different angles, there is a common denominator, which remains my ultimate duty: protection of people. This comes down to protection of personal data and privacy, and upholding the respect to fundamental rights.

In times of continuous acceleration and sophistication in cyber-attacks, this campaign becomes more and more an opportunity for all of us to work together and to provide updated cybersecurity awareness to individuals, who by the way are the first line of defence for cyber threats, such as those using social engineering techniques.

Cyber security is no longer a best effort task nor just a useful tool; it is a major cornerstone for our digital lives. Unfortunately, social engineering continues to be overlooked, causing major cyber attacks and data breaches. My wish for this year's campaign is that it is successful in raising much needed awareness around the topic, both for the organisations and for the individuals.

II. Interplay between Cybersecurity & privacy and the data protection

As you might know already, in opinions and formal comments issued by the EDPS on cybersecurity legislative initiatives, I have always stressed the importance of cybersecurity for the protection of personal data.

Cybersecurity in particular becomes more and more important for data protection, due to the continuous rise of cyber threats. Indeed, in the last two years, my data protection notification function observes, a rise in personal data breaches caused by cyberattacks, and they are now one of the most common sources of data breaches.

Looking from the perspective of cybersecurity, insufficient compliance with data protection legislation may lead to personal data falling on the hands of malicious actors whose aim is to use them for cyber-attacks, using techniques such as impersonation, identity theft and social engineering.

I wish to point your attention to the fact that sometimes, a cyberattack can be a chain of different breaches, and data obtained from one breach can be used for new attacks. This is why, in line with data protection legislation, it is of paramount importance to inform as soon as possible individuals whose data have been breached and equally important to provide them guidance on how to protect themselves from cyber-attacks, and in particular social engineering.

Ladies and gentlemen, if we want to combat cyber-attacks, and social engineering, it is now more important than ever before, all of us, data protection authorities, cybersecurity authorities, data protection officers, and cybersecurity experts, to work together and share knowledge on the matter.

To foster this collaboration, we organise this month along with ENISA, a pilot exercise for EUIs, PATRICIA, with scenarios of cyberattacks leading to personal data breaches. This comes after another initiative we took this year, as part of our 20th anniversary, a survey to assess the maturity of the data breach management processes in EUIs.

III. The interplay with AI

At the same time, we all witness an unprecedented speed of developments in the artificial intelligence and in particular in the so-called generative AI. Everybody, companies and individuals, wants to use AI systems to gain competitive advantages and efficiency. While this "AI rush" unfolds so rapidly, I am deeply concerned that personal data protection as well as cybersecurity aspects may be overlooked.

To give you an example, we see more and more sophisticated phishing attacks employing a very dangerous combo: AI and social engineering. A malicious AI system can be trained to trick human psychology with text and deep fakes, accelerating as never before cyber-attacks. It can even do so by keeping conversations with human to slowly lower their defences.

On the positive side, AI can help us defend from cyber-attacks. Security systems using AI, can detect, predict and defend from cyber-attacks, as never before. And they can be a useful tool for both simple and professional users.

But we must not forget that AI systems themselves are trained with personal data and they may present security weaknesses. It is of paramount importance for all AI actors, developers,

deployers, and organisations profiting from AI, to comply with the AI act, as well as data protection and cybersecurity legislation, to avoid AI systems offering new attack opportunities.

But most of all, I am concerned about overlooking the user awareness. First, we should not over-trust AI systems: Be mindful not to give prompts with personal data or sensitive data for your organisations, as this might result, eventually, in data breaches due to the lack of proper cybersecurity of systems.

Second, you should not over-rely on them- always review the responses and be on top, as they might influence your decisions and reduce your critical thinking.

IV. Conclusion

To conclude my speech, it is obvious that we are entering uncharted waters, where cybersecurity becomes a critical cornerstone of our digital lives.

What's more, artificial intelligence changes dramatically the digital landscape, and it might be a very flammable ingredient for both data protection and cybersecurity, in particular social engineering.

I wish to repeat, that it is now more than ever before essential to work together, engaging also the users, to address all these new risks in this new digital landscape.

Before leaving, please remember to visit our stand just outside, showcasing the AI deep fake generator.

Thank you very much for your attendance and please accept my best wishes for a successful cybersecurity month.