Report from the "New Technologies Forum" Conference

September 20-21, 2023

University of Economics and Human Sciences, Warsaw

Dear Ladies & Gentlemen,

It is with great pleasure that I present to you the report from the "New Technologies Forum" Conference, which took place at the University of Economics and Human Sciences in Warsaw, on September 20-21, 2023. The event was organised by the Personal Data Protection Office in cooperation with the New Technologies Law Association and the University of Economics and Human Sciences in Warsaw.

The aim of the "New Technologies Forum" Conference was to explore the role and impact of advancing digitisation on the protection of personal data. The event, which brought together more than 40 experts from various fields, aimed to create a platform for discussion and exchange of knowledge on current challenges and future directions of development in the field of new technologies and privacy protection.

During the two-day "New Technologies Forum", the invited specialists presented issues related to the protection of personal data in the era of new technologies, including trends and challenges related to artificial intelligence, cloud computing, blockchain technology, and tracking technology. The conference also explored the ethical challenges posed by artificial intelligence, including the issue of responsibility in the use of new technologies. Experts explained what information security is in the digital age. Legislative changes related to the entry into force of acts that are part of the EU's Digital Services Package and Data Strategy were also discussed. The conference was summed up by an expert debate devoted to the most important trends in new technologies in the context of personal data protection.

Below you will find a summary of the sessions held during the two-day "New Technologies Forum" and the most important conclusions resulting from the discussions. This report constitutes a summary of the conference, as well as an overview of selected issues related to the challenges for data protection concerning the development of new technologies.

Jan Nowak
President
of the Personal Data Protection Office

Agenda of the New Technologies Forum

DAY I

Moderators: Anna Dudkowska,
Director of the International Cooperation and Education Department, Personal Data Protection Office,
Natalia Misiuk,
Acting Director of the High-Tech Department, Personal Data Protection Office

10:00 – 10:30 OPENING CEREMONY OF NEW TECHNOLOGIES FORUM

Jakub Groszkowski, *Deputy President of the Personal Data Protection Office*
Beata Ostrowska, *Chairwoman of the Sectoral Council for Competence in IT,*
Vice-President of the Sectoral Council for Competence in Telecommunications and Cyber Security
Xawery Konarski, attorney-at-law, *President of the New Technologies Law Association,*
Vice-President of the Polish Chamber of Information Technology and Telecommunications,
Traple Konarski Podrecki i Wspólnicy Sp. J.
Włodzimierz Chróścik, attorney-at-law, *President of the National Council of Attorneys-at-Law*

10:30 – 10:50 INTRODUCTORY SPEECH

Maciej Gawroński, attorney-at-law, *GP Partners, Member of the Scientific Council of the Personal Data Protection Law Institute*
The challenges of privacy and data protection against the background of the increasing development of new technologies and digitalisation.

SESSION I
10:50 – 13:05
PERSONAL DATA PROTECTION
IN THE ERA OF NEW TECHNOLOGIES

Agnieszka Rapcewicz, *Member of the Artificial Intelligence Working Group*
Browser settings and consent requirements set forth in the provisions on personal data protection — is Art. 173(2) of the Telecommunications Law lex specialis in relation to Art. 174 of the Telecommunications Law?
Łukasz Jarecki, *Personal Data Protection Team, Grant Thornton*
Exercise of the right to be forgotten and blockchain.
Daria Rychlik, attorney, *The Attorney Law Firm*
ChatGPT in a legal situation, commercial use, risks.

Witold Chomiczewski, **attorney-at-law**, *Plenipotentiary of the Chamber of Electronic Economy for Legislation*

Dark patterns, cookies i targeted advertising on the internet and the GDPR.

Andrzej Dulka, President of the Board at the Polish Chamber of Information Technology and Telecommunications

The future of new technologies and the protection of personal data.

Wiesław Paluszyński, *President of the Polish Information Processing Society, Chairman of the Sectoral Council for Competence in Telecommunications and Cyber Security and Member of the Sectoral Council for Competence in IT*

Cybersecurity and personal data protection.

Barbara Smalarz, *Chief Specialist for Information Security*, *KGHM Polska Miedź S.A.*

Standards and good practices for cloud computing.

Izabela Kowalczuk – Pakuła, **attorney-at-law**, *Bird & Bird*

Children's personal data in the digital age.

BREAK
13:05 – 13:30

SESSION II

13:30 – 14:30

ARTIFICIAL IINTELLIGENCE AND PERSONAL DATA PPROTECTION – LEGAL AND ETHICAL CHALLENGES, REGULATORY FRAMEWORK AND DE LEGE FERENDA CONCLUSIONS

Ewa Kurowska - Tober, **attorney-at-law**, *New Technologies Law Association*

Data protection principles and artificial intelligence - exercise of obligations and rights under the GDPR when using AI.

Agnieszka Gajewska-Zabój, attorney-at-law, *Secretary of the National Council of Attorneys-at-Law*

Legal challenges posed by the use of AI-based tools for effective protection of personal data.

Dominik Lubasz, PhD, *New Technologies Law Association*

A risk-based approach in the development and implementation of AI systems.

Maria Jędrzejczak, PhD, Adam Mickiewicz University in Poznań, *Member of the Scientific Council of the Personal Data Protection Law Institute*

Risk categories of artificial intelligence application. Practical remarks on the example of China's Social Trust System.

SESSION III

14:30 – 15:45

ETHICS AND RESPONSIBILITY IN THE USE OF TECHNOLOGY

Barbara Podwysocka, *Director of the Security Division, Polski Holding Hotelowy Sp. z o.o.*

Moral responsibility – i.e. the ethical use of artificial intelligence.

Alicja Kaszuba, *Member of the Artificial Intelligence Working Group*

Legal and ethical aspects of emotion analysis and processing.

Przemysław Olszewski, *Checkbox Sp. z o.o.*

Ethics of new technologies as an element of Compliance. Based on the European Union project "SIENNA".

Kamil Wojciechowski, *Forsafe Sp. z o.o.*

Development of new technologies and the impact on data protection and on the role of data protection officers.

Natalia Bender, *Warsztatownia.eu*

Cyber-vetting in the job recruitment process.

15:45 – 16:00

BREAK

SESSION IV

16:00 – 17:30

INFORMATION SECURITY IN THE DIGITAL AGE

Jakub Groszkowski, *Deputy President of the Personal Data Protection Office*

Conclusions from the inspection of mobile applications.

Tomasz Ochmiński, *Head of Inspection Team, Inspections and Breaches Department, Personal Data Protection Office*

Prompt engineering in the light of GDPR.

Renata Podlewska, *Data Protection Officer, Karol Marcinkowski Medical University in Poznan*

Audit as a tool for ensuring information security in the digital age.

Paweł Ornoch, *Director of Security Office at PKO BP Finat and* **Maciej Jurczyk**, *Security Expert at PKO BP Finat*

Hardening the security system in the organisation.

Piotr Kamiński, *nFlo Sp. z o.o.*

Information security in online transactions: How to protect your financial and personal data when shopping online?

Łukasz Bonczek, *Sales Project Analysis Director, EXATEL S.A.*

What should we do to make our economy more cyber-secure?

END OF THE I DAY OF THE FORUM

DAY II

SESSION V

10:00 – 11:30

THE MOST IMPORTANT LEGISLATIVE CHANGES IN 2023/2024

Magdalena Witkowska-Krzymowska, PhD, *Director of the Legal Department at the Ministry of Digitalisation*

mObywatel application.

Xawery Konarski, *attorney-at-law, President of the New Technologies Law Association, Vice-President of the Polish Chamber of Information Technology and Telecommunications, Senior Partner at Traple Konarski Podrecki i Wspólnicy Sp. J.*

Artificial Intelligence Act.

Joanna Litwin, *Data Protection Officer at the Municipal Centre for Family Assistance in Szczecin, Higher School of Professional Education in Wrocław*

European Health Data Space (EHDS) in the context of personal data protection.

Piotr Drobek, *Counsellor at the Personal Data Protection Office*

Transfers of personal data from the EU to the United States.

Małgorzata Skórska, *WKB Lawyers*

Modern digital marketing and personal data protection - behavioural advertising, targeting, tracking technologies and the future of cookies - a legal and practical perspective.

Agata Szeliga, attorney-at-law, *New Technologies Law Association*

The impact of the Data Act on the GDPR and the processing of personal data.

BREAK

11:30 – 12:00

SESSION VI

12:00 – 13:00

THE ERA OF INNOVATION AS A CHALLENGE FOR DATA PROTECTION AUTHORITIES

Maria Skwarcan, *International Cooperation and Education Department, Personal Data Protection Office*

The European Data Protection Board in the face of the challenges posed by the development of new technologies.

Rocco Panetta, *IAPP Country Leader - Italy, Managing Partner at PANETTA*

Artificial intelligence and compliance with the GDPR - lessons from recent proceedings before the Italian Data Protection Authority.

Kari Laumann, *Head of Research, Analysis and Policy Section,*
Norwegian Data Protection Authority
The Norwegian regulatory sandbox experience for artificial intelligence and privacy.
Yuliia Derkachenko, *Representative on information rights of the Ukrainian Parliament Commissioner for Human Rights*
Artificial intelligence as a catalyst for change: the role of DPAs in the modern world.

DEBATE

13:00-14:00

KEY TRENDS OF NEW TECHNOLOGIES IN THE CONTEXT OF PERSONAL DATA PROTECTION

Moderator: **Adam Sanocki**, *Spokesperson of the Personal Data Protection Office*
Participants in the debate:
Jakub Groszkowski, *Deputy President of the Personal Data Protection Office*
Monika Krasińska, *Director of the Case Law and Legislation Department, Personal Data Protection Office*
Maciej Gawroński, **attorney-at-law**, *GP Partners, Member of the Scientific Council of the Personal Data Protection Law Institute*
Xawery Konarski, **attorney-at-law**, *President of the New Technologies Law Association, Vice-President of the Polish Chamber of Information Technology and Telecommunications, Traple Konarski Podrecki i Wspólnicy Sp. J.*
Ewa Kurowska – Tober, **attorney-at-law**, *New Technologies Law Association*
Agnieszka Gajewska – Zabój, **attorney-at-law**, *Secretary of the National Council of Attorneys-at-Law*
Marcin Wysocki, *Deputy Director of the Cybersecurity Department, Ministry of Digital Affairs*

CLOSING OF THE CONFERENCE

Opening ceremony and introductory speech

Opening ceremony:

Jakub Groszkowski

Deputy President of the Personal Data Protection Office

Beata Ostrowska

Chairperson of the Sectoral Council for Competence in IT and Vice-Chair of the Sectoral Council for Competence in Telecommunications and Cybersecurity

Xawery Konarski

Attorney-at-law, President of the New Technologies Law Association, Vice-President of the Polish Chamber of Information Technology and Telecommunications, Senior Partner at Traple Konarski Podrecki i Wspólnicy Sp. J.

Włodzimierz Chróścik

Attorney-at-law, President of the National Council of Attorneys-at-Law

Introductory speech:

Maciej Gawroński

Attorney-at-law, Partner at GP Partners,

Member of the Scientific Council of the Personal Data Protection Law Institute

During the conference opening ceremony, experts unanimously emphasised that cyber threats related to the use of new technologies are becoming more and more advanced, therefore it is necessary to take multidirectional actions to counter this phenomenon.

The role of data protection officers (DPOs) and their competences in the area of cybersecurity were indicated. In this respect, the importance of sectoral councils was emphasised, the task of which is to closely monitor the labour market and, on the basis of observations, identify, build the competence needs of DPOs, as well as educate and adjust them to the system.

The experts also presented the activities of the New Technologies Law Association. This organisation, associating lawyers specialising in new technologies, conducts educational and publishing activities and cooperates with regulators. The activities of the New Technologies Law Association take place in working groups, the most important of which is the "GDPR and e-privacy" group. Members of this group were well represented at the Forum as speakers.

The President of the National Council of Attorneys-at-Law stressed that cybersecurity issues should be viewed from the perspective of ethics and responsibility of its creators. The National Council of Attorneys-at-Law expressed great interest in the conclusions de lege ferenda formulated during the conference. It was also declared that as part of the work of the Centre for Research, Studies and Legislation, the National Council of Attorneys-at-Law will support the legislative initiatives signalled in the speeches.

The introductory speech discussed the challenges for privacy and data protection in the context of the development of new technologies and digitisation, with an emphasis on the potential threats posed by artificial intelligence (AI), such as the objectification of people and digital censorship. The topic of the use of AI in the surveillance of citizens was also discussed, as well as concerns related to a single digital currency, quantum computers and the centralisation of AI management.

It was underlined that technological progress is inevitable, but it is important that dominant technology companies take into account human rights, including the right to privacy and the protection of personal data, and adapt their solutions to the provisions of the GDPR.

Session I: Personal data protection in the era of new technologies

Speakers:

Agnieszka Rapcewicz

Attorney-at-law, Internet. Time to Act! Foundation, Kozminski University

Łukasz Jarecki

Data Protection Team, Grant Thornton

Daria Rychlik

Attorney-at-law, The Attorney Law Firm

Witold Chomiczewski

Attorney-at-law, Plenipotentiary of the Chamber of Digital Economy for Legislation

Andrzej Dulka

President of the Management Board of the Polish Chamber of Information Technology and Telecommunications

Wiesław Paluszyński
President of the Polish Information Processing Society, Chairman of the Sectoral Council for Competence in Telecommunications and Cybersecurity and Member of the Sectoral Council Competence in IT

Barbara Smalarz
Chief Specialist in the Security and Internal Control Department, KGHM Polska Miedź S.A.

Izabela Kowalczuk-Pakuła
Attorney-at-law, New Technologies Law Association

During the first session, special attention was paid to the conditions for obtaining a valid consent for the collection of cookies on the basis of the applicable regulations. It was recalled that in order for consent to be valid, it must be informed, freely given, unambiguous and specific. Importantly, the default consent excludes informed and specific consent, and only the browser's factory settings automatically rejecting the request to create cookies are a condition for the proper functioning of this mechanism.

The implementation of the right to be forgotten in the context of blockchain technology was also discussed. What has been emphasised is that the implementation of a request to remove specific data from the blockchain involves the deletion of these data inside all blockchains that are on the device. As a consequence, the effective exercise of the right to be forgotten requires the cooperation and coordination of the activities of all controllers, which is a huge challenge and shows that the GDPR has not foreseen the effects of data processing within technologies such as blockchain.

The session also focused on the practical aspects of using other advanced systems based on artificial intelligence (AI), especially the ChatGPT model, in the context of current and proposed regulations. Conference participants explored both the potential and the challenges of using these technologies in different sectors. A wide spectrum of ChatGPT applications was discussed, from customer service automation to content generation and decision-making support.

Of particular note is the question of how ChatGPT and similar AI tools can contribute to greater efficiency and innovation, while not overlooking issues related to responsibility for the generated content and the protection of personal data. Particular attention should be paid to

the legal and ethical aspects of the use of AI, including responsibility for decisions made with the use of AI, copyrights to the generated content, and potential risks of abuse. The participants discussed how to ensure compliance of these technologies with the GDPR, especially in terms of transparency of data processing and users' rights to access, rectification and erasure of data.

In this context, attention should be paid to the actions taken so far by the Personal Data Protection Office in connection with the complaint against OpenAI, the creator of the ChatGPT model, which is being considered by the authority. The complainant among others raised the issue of the lack of transparency of OpenAI's data processing policy, accusing the company of failing to provide information on the manner and purpose of the processing of his/her personal data. The Personal Data Protection Office is conducting proceedings in this case.

In addition, due to the increasing number of complaints lodged by data subjects with European supervisory authorities against OpenAI's activities, in April 2023 the supervisory authorities jointly decided to set up a ChatGPT Taskforce. The Taskforce was established to support cooperation and exchange of information between authorities on their investigations in the field of data processing by Open AI, as part of the operation of Chat GPT.

During the session, the experts also touched on the topic of deceptive design patterns (so-called *dark patterns* or *deceptive patterns*). They pointed out the need to clearly inform users about the purpose of processing, the rights of data subjects, as well as the risks associated with deceptive design patterns. It has been emphasised that the purpose in itself cannot be regarded as a prerequisite for legalising the processing of data. The fact that the controller has a specific purpose for obtaining data does not mean that it can already process the data. The controller can process personal data only if the conditions for legalising the processing contained in the GDPR (Articles 6 and 9 of the GDPR) are met.

Of particular note in the context of deceptive patterns are the practical guidelines adopted to identify and prevent the use of deceptive design patterns, including actions taken by supervisory authorities. In February 2023, the European Data Protection Board (EDPB), which comprises supervisory authorities, including the Personal Data Protection Office, adopted Guidelines on *deceptive design patterns* in social media platform interfaces[1]. The Guidelines provide practical recommendations for designers and users of social media platforms on how to recognise and avoid deceptive design patterns in social media interfaces

[1] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en

that violate GDPR requirements. The EDPB provided specific examples of types of deceptive design patterns, recommending best practices for different use cases and providing specific recommendations for user interfaces designers to facilitate the effective implementation of the GDPR.

The experts also touched on the important topic of protecting children's personal data in the digital space in the context of the GDPR. They discussed the issue of online advertisements addressed to children and the challenges of recipients' age verification, and highlighted the need for education and awareness campaigns on children's online safety.

Session II: Artificial intelligence and personal data protection – legal and ethical challenges, regulatory framework and *de lege ferenda* conclusions

Speakers:

Ewa Kurowska-Tober
Attorney-at-law, New Technologies Law Association

Agnieszka Gajewska-Zabój
Attorney-at-law, Secretary of the National Council of Attorneys-at-Law

Dominik Lubasz, PhD
Attorney-at-law, New Technologies Law Association

Maria Jędrzejczak, PhD
Adam Mickiewicz University in Poznań, Member of the Scientific Council of the Personal Data Protection Law Institute

Session II focused on analysing the role of artificial intelligence in personal data processing. It was pointed out that AI-based systems rely on huge amounts of personal data, which is essential to perform their tasks. However, due to their ability to process data on an unimaginable scale, they are becoming difficult to understand and to control.

The conference participants discussed the challenges of ensuring the security of personal data in the context of rapidly developing AI technologies. It was pointed out that compliance with GDPR obligations is crucial, as the proposed provisions on AI are largely based on the same principles.

In order to ensure the security of personal data, due to the development of AI technology, it is necessary first of all to ensure the implementation of the obligations listed in the GDPR, as the proposed Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) has been largely constructed on this model and takes over many of the solutions adopted in its provisions. The risk principle, the penalty model, the obligations model, the authorities that will manage the area of artificial intelligence, etc., are all modelled on the solutions adopted in the GDPR. Based on this model, the responsibilities of AI developers can be put into 5 main areas: (1) compliance with the basic principles of personal data processing, (2) automated data processing, (3) realisation of the rights of data subjects (4) information obligation and (5) data protection impact assessment. The basic principles of personal data processing are: legitimacy, fairness and transparency, purpose limitation, adequacy and data minimisation, substantive accuracy, time limitation, integrity and confidentiality, and accountability.

As a result, it can be assumed that the GDPR will naturally fill a gap in the future provisions of the Artificial Intelligence Act, thereby ensuring that its impact on the rights and freedoms of individuals is taken into account throughout the life cycle of the AI system.

During the session, the lack of transparency in the processing of personal data in artificial intelligence technology was highlighted. The same problem arises with regard to the principle of purpose limitation, minimisation or adequacy. As experts pointed out, at the moment when artificial intelligence creates artificial neural networks, it searches a huge number of sources in search for information. This raises the question of how AI is to self-restrict its access to information and personal data that it is unlikely to need at all for a given task. This poses a challenge for artificial intelligence developers, particularly in light of the privacy by design principle, which stipulates that AI should be designed at the core to ensure the protection of personal data. With regard to the principle of minimisation set out in the GDPR, the Artificial Intelligence Act Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) introduces an additional principle – comprehensiveness (Article 10(3) of the draft Artificial Intelligence Act). The completeness principle states that training data sets (i.e., those from which AI derives its skills) must be adequate, error-free and complete.

Automated decision-making, including profiling - and the related information obligation- is another important aspect, raised by session participants, related to the construction of artificial intelligence systems. Artificial intelligence models make extensive use of profiling

solutions, so an important task for AI developers is to ensure that the rights of the data subject are effectively exercised.

The protection of personal data is crucial for the ethical use of artificial intelligence. What needs to be emphasised is that education, increased awareness, and cooperation with data protection specialists are essential when developing AI models. Importantly, a data protection impact assessment should be conducted for any use of artificial intelligence, and risk analysis is one of the key tools in the process of using AI. The development of new technologies is so dynamic that already some formulations of regulations raise questions about their validity, which poses another challenge for AI developers and users.

Session II also highlighted the content of the Joint opinion of the EDPB and the EDPS on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)[2]. It should be noted that the EDPB and the European Data Protection Supervisor (EDPS) in their opinion called for a ban on the use of AI for biometric identification and certain other uses that may lead to discrimination and risk of interfering with the rights and freedoms of individuals. Importantly, many of the comments have been taken into account by the European Parliament and there is a chance that the legislative process will move in the direction set by the EDPB and the EDPS towards greater protection of data subjects.

Session III: Ethics and responsibility in the use of technology

Speakers:

Barbara Podwysocka

Director of the Security Division, Polski Holding Hotelowy Sp. z o.o.

Przemysław Olszewski

Checkbox Sp. z o.o.

Kamil Wojciechowski

Forsafe Sp. z o.o.

Natalia Bender

Warsztatownia.eu

[2] https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en

The subject of the third session was ethics and responsibility in the use of technology. The speeches focused on the ethical use of artificial intelligence. The basic conclusion of all the speeches was the recognition that artificial intelligence should be used to promote the well-being of humanity.

During the session, the topic of ethics of new technologies as an element of compliance was presented. According to experts, artificial intelligence should serve society and be a useful organisational tool. AI developers should evaluate a solution not only from the side of designing the technology, but also from the side of its subsequent use. By assumption, designers of systems using AI must create them with respect for the fundamental rights of individuals, including the right to privacy and data protection. Systems must not be designed in an unethical manner.

What is important and was also emphasised earlier at the conference, is the transparency of the process, the collection of data by AI. At the time the tool is designed and implemented, its developer must have planned the management of the system, and have full control and a plan for its operation.

New technologies such as generative artificial intelligence, virtual reality, image and sound manipulation, profiling services in marketing, processing of children's personal data - these are real challenges users are facing. Each of these technologies is based on data processing. Therefore, in this context, it is crucial to understand how the technology works, identify the risks generated, control the flow of data and ensure the safe use of the system by users. It is also important to keep in mind the role of data protection officers, who support controllers in realisation of these objectives within the organisation.

Cyber-vetting in the job recruitment process is also an extremely important topic in the context of ethical use of new technologies. When using artificial intelligence tools to find publicly available information about job candidates, employers must remember that building opinions on candidates based on information from social media or other publicly available sources can lead to cognitive errors and pose significant challenges in recruitment processes. It can also lead to discrimination against candidates.

Session IV: Information security in the digital age

Speakers:

Jakub Groszkowski

Deputy President of the Personal Data Protection Office

Tomasz Ochmiński

Head of Inspection Team, Inspections and Breaches Department, Personal Data Protection Office

Renata Podlewska

Data Protection Officer, Karol Marcinkowski Medical University in Poznan

Paweł Ornoch

Director of Security Office at PKO BP Finat

Maciej Jurczyk

Security Expert at PKO BP Finat

Piotr Kamiński

nFlo Sp. o.o.

Łukasz Bonczek

Sales Project Analysis Director, EXATEL S.A.

An inherent element of technology development is the use of mobile applications. The acceleration of digital transformation and the proliferation of e-services in most industries, has provided an opportunity for a high cybercriminal activity and an increase in data protection breaches. That is why the Personal Data Protection Office, as part of its 2023 sectoral inspection plan, has addressed verification of how personal data is processed using online and mobile applications. The Personal Data Protection Office carried out inspections at entities from the following sectors: medical, commercial, banking, catering, tourism, transport and government administration. Mobile applications were the main work tool used, e.g. in the transport industry, or they were an additional tool - e.g. in the work of entities from the finance sector.

The inspections most often included the legal basis for processing personal data in the organisation, the scope and type of personal data processed, the implementation of appropriate technical and organisational measures for the operation of mobile applications and related IT system resources. It was also checked whether a risk analysis had been carried out and whether

the effectiveness of the technical measures applied had been regularly tested, measured and evaluated. The inspections showed that the inspected controllers generally implemented appropriate technical and organisational measures and took into account the principles of privacy by design and privacy by default at the stage of designing and implementing mobile applications, while ensuring effective protection of personal data processed in the organisation.

The Personal Data Protection Office presented several examples of good practices related to the safe use of mobile applications in the work of controlled entities, such as application security audits, including penetration tests to detect potential vulnerabilities. Examples of undesirable practices were also presented, such as requiring users to send a photo or scan a linked credit card to confirm their identity. The results of the inspections conducted will be presented in early 2024.

During the session, different models of generative artificial intelligence were also discussed. It was emphasised that AI is not always able to give an unambiguous answer, which stresses the need for users to be cautious and verify information. Experts also repeatedly emphasised the role of audit as one of the basic tools for effectively securing personal data against information security incidents, cyber-attacks and data breaches. The participants also stressed the importance of "hardening" the security system in the organisation and focused on the role of staff training and effective implementation of post-audit recommendations.

During the session, the Polish Internet security landscape in Poland in 2023 was presented, particularly in the field of small and medium-sized enterprises. The most common security measure used by small and medium-sized enterprises, as experts point out, is strong password authentication, while less popular is making back-ups and controlling access to the enterprise network.

This session also identified the main problems associated with ensuring cybersecurity in the economy. According to experts, the biggest problems related to ensuring cybersecurity in the economy result from the lack of business awareness, inappropriate allocation of funds for cybersecurity by public entities, or the lack of these funds altogether. Most often, the high real costs of building a safe organisation are indicated: equipment, training, services, audits, human resources. Some response to these constraints may be to define precisely what budget funds are to be spent on, to develop models of good practices in the organisation, to set good trends in building threats awareness, and to effectively enforce regulations and publicise cases of misconduct.

Session V: The most important legislative changes in 2023/2024

Speakers:

Magdalena Witkowska-Krzymowska, PhD

Director of the Legal Department at the Ministry of Digital Affairs

Xawery Konarski

Attorney-at-law, President of the New Technologies Law Association, Vice-President of the Polish Chamber of Information Technology and Telecommunications, Senior Partner at Traple Konarski Podrecki i Wspólnicy Sp. J.

Joanna Litwin

Data Protection Officer at the Municipal Centre for Family Assistance in Szczecin, Higher School of Professional Education in Wrocław

Piotr Drobek

Counsellor at the Personal Data Protection Office

Małgorzata Skórska

WKB Lawyers

Agata Szeliga

Attorney-at-law, New Technologies Law Association

Session V focused on the most important legislative changes planned for 2023 and 2024. The legal basis for the mObywatel application and its functionality was analysed, noting the legislator's unique approach in creating a separate act for this application. This was followed by a presentation of the 10 theses on the interplay between the Artificial Intelligence Act and GDPR, highlighting that the two acts should function as a legislative tandem. The draft European Health Data Space (EHDS) was presented, explaining the primary and secondary uses of electronic health data.

The session focused on the European Health Data Space (EHDS) project, which is rooted in the European Data Strategy to create a single data space. The main objectives of the EHDS include giving individuals in the EU more practical control over their electronic health data and creating a truly single market for digital health products and services through regulatory harmonisation.

The EHDS draft regulation covers primary and secondary uses of electronic health data. Primary use - will refer to the processing of personal electronic health data for the provision of health services to assess, maintain or restore the state of health of the natural person to whom that data relates, including the prescription, dispensation and provision of medicinal products and medical devices, as well as for various services, e.g. reimbursement services. In contrast, secondary use – refers to the processing of personal data in education or teaching activities in health or care sectors. Importantly, while the EHDS clearly strengthens the control and rights of health data subjects, there is a danger of weakening data protection law - considering mainly the categories of data and the purposes of secondary use.

During Session V there was also a discussion of the history of the establishment of rules for the transfer of personal data to the United States, dating back to the time of Directive 95/46/EC, focusing in particular on the assumptions of the current EU-US Data Privacy Framework, adopted on 10 July 2023 through the EC Decision to ensure an adequate level of protection of personal data. As a result of the decision, personal data can only be transferred without the need for additional authorisations or the use of legal instruments such as standard contractual clauses or binding corporate rules to those entities that are certified under this programme. The EU-US Data Privacy Framework is based on self-certification and only those entities that have signed up to it participate therein.

It was emphasised that the current programme does not differ in many elements from its predecessors. In contrast, the main problem signalled by the Schrems II judgment is the access of US services to data processed by data importers in the US, on a basis that does not meet, inter alia, the criteria of proportionality, necessity and does not provide any mechanism to guarantee judicial recourse. In order to address this problem, an executive order of the US President introduced additional safeguards and established additional institutions, including, inter alia, a special data protection appeals court.

Following the first complaints related to the functioning of the EU-US Data Privacy Framework, according to experts, it is expected that the question of whether the current EU-US Data Privacy Framework provides sufficient protection and is valid will be settled within a few years.

The discussion also presented a legal perspective and a practical approach to modern digital marketing in the context of ensuring the security and protection of personal data. As pointed out during the session, the modern market economy requires entrepreneurs

to constantly strive for the consumer's interest, compete with their competitors and develop cooperation with the environment. To do this, information is needed, especially information influencing consumer choices. The difference between behavioural advertising, which is based on the observation of a person's behaviour at a given time, and targeting, which is the action of directing or targeting a given message to a specific group of people, was presented. Both cases undoubtedly involve the processing of personal data and it is therefore necessary to effectively enforce the rights of data subjects guaranteed by the GDPR.

Participants of the session also explained the impact of the Data Act on the GDPR and the processing of personal data. The Data Act is part of the EU's strategy to create a legal framework for the collection, processing, secondary use and sharing of personal data. It also aims to facilitate access to information by opening up public data spaces so that, as a result, the full potential of the digital economy can be realised. Nevertheless, in the opinion of many experts, the Data Act contains provisions that may be harmful to legal clarity, privacy protection, protection of intellectual property and equal treatment of the actors that make up the EU market. The huge economic and social opportunity arising from the digital transformation was highlighted, provided that a constructive dialogue is ensured between regulators and the entities which will be affected by the new regulations.

Session VI: The era of innovation as a challenge for data protection authorities

Speakers:

Maria Skwarcan

International Cooperation and Education Department, Personal Data Protection Office

Anna Buchta

Head of Policy and Consultation Unit, European Data Protection Supervisor

Rocco Panetta

IAPP Country Leader - Italy, Managing Partner at PANETTA

Kari Laumann

Head of Research, Analysis and Policy Section, Norwegian Data Protection Authority

Yuliia Derkachenko

Representative on information rights of the Ukrainian Parliament Commissioner for Human Rights

Session VI began with an overview of what the European Data Protection Board is doing in the face of the challenges posed by the development of new technologies. One of the points of the EDPB's 2021-2023 strategy is the approach that data protection does not hold back innovation, but helps to ensure the development of technology, new business models and society in line with values such as human dignity, autonomy and freedom.

In order to promote an approach to new technologies based on fundamental rights, the EDPB has adopted a number of guidelines in recent years (e.g. the Guidelines on virtual voice assistants[3], the Guidelines on deceptive design patterns in social media platform interfaces[4], mentioned earlier at the conference, and the Guidelines on the use of facial recognition technology in the area of law enforcement[5]). Work on further documents is ongoing.

The experts also presented the opinions of the EDPB and EDPS on the draft legislation submitted by the European Commission as part of the Digital Strategy and Data Strategy. Importantly, although the recommendations of the EDPB and the EDPS, on draft EU legislation, are not binding, in practice they have an impact on the subsequent legislative process. In particular, the European Parliament, sometimes also the Council of the EU, increasingly introduce amendments inspired by the EDPS and EDPB recommendations.

In the documents indicated, the EDPB raised a number of concerns and recommendations regarding the compatibility of the legislative proposals with existing Union data protection legislation, which essentially concerned the lack of sufficient protection of the fundamental rights and freedoms of natural persons, fragmented supervision and the risk of inconsistency with the current data protection framework.

A key aspect highlighted by the EDPS in its opinions relates to the so-called interplay between the various new pieces of legislation and existing data protection legislation. This is despite the fact that, inevitably, many of the new regulations, although not directly regulating personal data protection, will apply in situations and in the context of the same business models that are already dealt with under the GDPR.

Participants of the session stressed that the right to the protection of personal data derives from the fundamental law of the European Union and has a very special status in the

[3] https://edpb.europa.eu/system/files/2021-07/edpb_guidelines_202102_on_vva_v2.0_adopted_en.pdf
[4] https://edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf
[5] https://edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf

EU, and therefore steps should be taken to ensure that this right is fully respected, also in the context of competition and consumer protection matters. Consequently, both the EDPB and the EDPS emphasise that the implementation of new EU legislation should absolutely comply with the content of the GDPR, but also with its well-established interpretation. Importantly, in some cases where it was necessary to align the proposed regulations with existing legislation, the European Parliament and the Council introduced amendments confirming that the new legislation will have to be applied without prejudice to existing legal provisions.

There are also concerns that data protection authorities are not designated in the new legal instruments as the main authorities competent to enforce their provisions. Member States have limited choice and options to decide which authorities will be competent in a given area. This is justified by the fact that these new legal instruments have different objectives than the GDPR. This does not change the fact that whoever will be in charge of implementing the new legislation will have to take into account the views of the data protection authorities. This is necessary, if only because of the so-called 'interplay' raised earlier. Although the objectives of the regulations differ, at the same time it should be noted that they are complementary, they are complementary.

Experts also pointed out the need to fully incorporate the provisions of the GDPR as applicable legislation in the context of a completely data-driven, generative artificial intelligence technology. This is why it is so important that the draft Artificial Intelligence Act is GDPR-compliant and based on GDPR.

The findings of the proceedings before the Italian DPA regarding artificial intelligence were also discussed. The conclusion of the proceedings indicated is clear: it is necessary to take the provisions of the GDPR fully into account as applicable legislation in the context of generative artificial intelligence technology. Following this, it is crucial that the draft Artificial Intelligence Act is compliant with the GDPR.

The Norwegian supervisory authority shared its experience with the regulatory sandbox project for artificial intelligence and privacy. This initiative has assisted in building the authority's internal competences in the area of artificial intelligence and helped the authority's staff to better understand the business environment related to artificial intelligence, resulting in a better assessment of how to apply the requirements of the GDPR.

During the session, the role and experience of the Ukrainian competent authority for data protection in the context of technology development was also presented. The development of an artificial intelligence legal framework in Ukraine, as the expert pointed out, is based on international standards and is moving towards a European strategy for the development of artificial intelligence. By developing a legal framework and becoming an EU candidate, Ukraine is committed to developing an artificial intelligence system that will be useful for citizens, businesses and the government. In view of Ukraine's chosen course of European integration, the development and further refinement of national legislation on regulations for the use of artificial intelligence should, be based on already formed European standards, principles and recommendations.

Ukraine's relevant activities in the sphere of artificial intelligence were also presented. An important step for Ukraine was the adoption of the European Ethical Charter on the use of artificial intelligence in judicial systems and related environments by the European Commission for the Efficiency of Justice of the Council of Europe. In 2020, Ukraine created the Concept of Development of Artificial Intelligence in Ukraine, which for the first time at the legislative level set out the definition, purpose, principles and tasks for the development of artificial intelligence technology in Ukraine. Among other things, Ukraine also joined the "Digital Europe" Programme (2021-2027), aimed at developing leading digital skills and making digital services even more accessible to citizens and state institutions of the EU and associated countries.

The final conclusion was to emphasise the need for a global (binding) international legal framework for the development and deployment of artificial intelligence, in order to be able to prevent its unlawful use.

Debate: Key trends of new technologies in the context of personal data protection

Moderator:

Adam Sanocki

Spokesperson of the Personal Data Protection Office, Director of the Communications Department in the Personal Data Protection Office

Participants in the debate:

Jakub Groszkowski

Deputy President of the Personal Data Protection Office

Monika Krasińska

Director of the Case Law and Legislation Department, Personal Data Protection Office

Maciej Gawroński

Attorney-at-law, Partner at GP Partners, Member of the Scientific Council of the Personal Data Protection Law Institute

Xawery Konarski

Attorney-at-law, New Technologies Law Association, Vice-President of the Polish Chamber of Information Technology and Telecommunications, Traple Konarski Podrecki i Wspólnicy Sp. J.

Ewa Kurowska-Tober

Attorney-at-law, New Technologies Law Association

Agnieszka Gajewska-Zabój

Attorney-at-law, Secretary of the National Council of the Attorneys-at-Law

Marcin Wysocki

Deputy Director of the Cybersecurity Department, Ministry of Digital Affairs

The expert debate constituted a summary of the conference and addressed the dynamic development of innovations and their impact on data protection, revealing important points concerning regulations and business practices. Participants in the debate stressed that the pace of technological progress is outpacing current regulations, which raises the need to create standards and good practices that can balance the development of technology with privacy protection.

The importance of supporting instruments such as regulatory sandboxes which allow to identify risks and respond to them effectively was emphasised. It was pointed out that with the development of technology, various challenges arise, such as the certification of cloud computing, especially in the context of key data categories and potential economic damage.

The consensus was that many issues can be effectively addressed by using existing regulations such as the GDPR. An example of this approach is the principle of accountability, which provides a specific point of reference. Another practical guideline relates to national certification - even unapproved industry codes provide a valuable instrument, a guideline for proper conduct.

In the context of the existing tools, guaranteed by the GDPR, the importance of the privacy impact assessment and the privacy by design principle was emphasised. Privacy impact assessment is often downplayed, while data protection experts should be involved at the early design stage of any technological endeavour.

Experts also stressed that new technologies should be a tool for development and not an end in itself. The question of evaluating this tool becomes crucial. Perhaps the appetite for data needs to be strongly reduced through legislative measures. The drive to maximise profit, translating into the minimisation of rights, becomes a serious topic for reflection. This issue should be discussed internally, and it should be done on the basis of consumer trust. It is worth noting that the voice of data protection officers is still missing in the whole process.

Participants in the debate expressed the belief that the law will always have difficulties in keeping up with the development of society. A positive opinion was expressed about GDPR, which provides a foundation on which to build activities in the area of adapting new technologies to the need to protect individual rights. Referring to earlier comments on the need for certification and approval of codes of conduct, it was recalled that the first approved code of conduct already exists and, assured that the President of the Personal Data Protection Office will support any solidly prepared initiative.

Experts also pointed out that the discussion on ethics is gaining momentum in the context of artificial intelligence. Ethics is recognised as one of the main goals of regulation, especially in the context of technologies that tend to exploit weaker individuals. In doing so, the need for two factors to coexist was highlighted: good legislation and proactive action by supervision authorities.

Concluding the debate, the participants agreed that, ultimately, the most important thing is to put people, their rights and freedoms at the centre of new technologies. An uncritical faith in digitalisation is old-fashioned, and modern successful business requires attention to the sphere of consumer privacy.

General conclusions from the "New Technologies Forum" Conference

The "New Technologies Forum" Conference was a key event focusing on the complexities and challenges of data protection in an era of increasing digitalisation. Discussions held and presentations given during the five sessions highlighted that technological development, while offering unprecedented opportunities, also entails new risks to privacy and personal data security. Conference participants, representing a wide range of perspectives from technological to legal ones, unanimously emphasised the need for a holistic approach to data protection issues.

Key areas requiring special attention included the ethical aspects of the use of artificial intelligence, the challenges of technology in the context of individual's rights, and the need to ensure transparency of the technologies and data processes used, in order to allow data subjects to exercise real control over their personal data.

Equally important was the issue of aligning new regulations, emerging in response to rapidly changing digital realities, with the current data protection framework, in order to ensure compliance with and interpretation of the GDPR and thus guarantee the protection of individuals' rights.

Also of particular importance in this context is the strengthening of cooperation between regulators, the technology industry, academic world and NGOs in order to develop sustainable data protection solutions. Knowledge and experience sharing platforms should also be developed to help adapt regulations and practices to the rapidly changing technological environment.

In order to ensure the development of technology, while ensuring that the rights of data subjects are strengthened, it is also significant to develop codes and certifications in the technology industry, as well as to promote best practices among controllers on the ethical and responsible use of personal data in new technologies.

Summary and acknowledgements

The “New Technologies Forum” Conference demonstrated the importance of constantly following and responding to changes in the technology world, especially in the context of personal data protection. Future strategies and actions should balance innovation with the ethical and legal aspects of privacy protection, which requires the joint efforts of all stakeholders.

The Personal Data Protection Office would like to thank everyone who contributed to the success of the "New Technologies Forum" Conference. We extend our sincere thanks to the Academy of Economics and Human Sciences in Warsaw and the New Technologies Law Association for co-organising the event. We address special thanks to the patrons and sponsors who supported our conference. Your support was invaluable in ensuring the high quality and reach-out of this event.

We would like to thank all the speakers for their invaluable knowledge, experience and insight into issues related to new technologies and personal data protection. Your presentations and discussions constituted a significant contribution to understanding and addressing today's challenges.

We would also like to thank all participants for attending the conference in large numbers. Your interest in personal data protection issues and the positive reception of the conference are the best motivation for the Personal Data Protection Office to organise further events of this type. As the Personal Data Protection Office, we are grateful for the opportunity to conduct such an important dialogue and raise awareness of privacy and personal data protection in the digital age in the years to come, inviting you to the next events organised by the Personal Data Protection Office.