

INFORMATION CLAUSE

ŁUKASIEWICZ RESEARCH NETWORK - INSTITUTE OF POLYMER MATERIALS

ABOUT THE PROCESSING OF PERSONAL DATA

AS PART OF VIDEO SURVEILLANCE

In compliance with the legal obligation imposed on the Personal Data Controller by the provisions of Article 13(1) of the 1 and 2 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC – (General Data Protection Regulation), (OJ L 119, p. EU L 119 of 4 May 2016, p. 1 and OJ L 127 of 23 May 2018, p. 2) – hereinafter referred to as **GDPR**, we hereby inform you that:

1. The administrator of personal data is:

Łukasiewicz Research Network - Institute of Polymer Materials (abbreviated name **Łukasiewicz-IMPiB**) with its registered office at 55 Marii Skłodowska-Curie Street, (87-100 Toruń), which can be contacted:

- 1) via e-mail address: sekretariat@impib.lukasiewicz.gov.pl ;
- 2) by letter to the address of the registered office: 87-100 Toruń, 55 Marii Skłodowska-Curie Street or via the e-delivery box: AE:PL-69485-13407-CBVJH-24 ;
- 3) by phone: +48 (56) 650-00-44; fax no.: +48 (56) 650-03-33, weekdays from 7:00 a.m. to 3:00 p.m.

2. Contact details of the Data Protection Officer

The Administrator has appointed a Data Protection Officer, who can be contacted electronically by e-mail: iod@impib.lukasiewicz.gov.pl or by letter to the Administrator's address, in all matters related to the processing of personal data and the exercise of rights related thereto.

3. Purposes of processing and legal basis of processing

We process your personal data on the basis of:

- 1) Article 6(1)(c) and (e) of the GDPR – in order to fulfil the legal obligation incumbent on the Controller and to perform tasks carried out in the public interest, as the Controller, as a state legal entity (Łukasiewicz Research Network Institute), operates on the basis of the Act of 21 March 2019. *o Łukasiewicz Research Network*, and m.in. the Act of 16 December 2016 *on the principles of state property management* (Articles 5 and 5a), and if you are an Employee of the Administrator – also the Act of 26 June 1974 – *the Labour Code* (Article 22 (2) § 1) and processes your data in order to protect property, ensure public order and safety of persons staying on the premises of the Administrator;
- 2) pursuant to Article 6(1)(f) of the GDPR – in order to pursue the Administrator's legitimate interest consisting in establishing, pursuing or defending against claims related to the performance of the agreement;
- 3) Article 6(1)(a) of the GDPR – your consent. Consent is required when the right to process personal data does not result directly from the provisions of law, and you provide the Administrator with more data on your own initiative than is necessary to deal with your case (the so-called clearly confirmatory action).

4. Type of data processed and categories of data subjects

With regard to persons entering (or staying) in the area covered by the monitoring (in particular employees, co-workers, customers, contractors, interested parties, visitors, passers-by), the scope of personal data includes primarily the image. Only the image (without sound) is subject to recording and recording data on the carrier.

5. Data recipients or categories of data recipients

The recipients of your personal data may be entities providing us with services necessary to achieve the purposes of processing (e.g. IT/ICT service providers, postal/courier companies, law firms, security agencies, auditors, advisors, and health and safety and fire protection specialists). We entrust or share this data only on the basis of appropriate data processing agreements or in compliance with relevant legal requirements. We make sure that the cooperating entities guarantee the highest security standards and protect your privacy. Our authorized employees also have access to the data – only to the extent necessary to perform their daily duties.

In addition, we may make your personal data available to external entities, including the media and authorized state authorities (e.g. courts, police, prosecutor's office, NIK, ZUS or tax office), only if it results directly from generally applicable law.

6. Data retention period

Your personal data will be processed:

- 1) for a period not exceeding **7 days** from the date of recording, after which they will be automatically overwritten (the exact storage period depends on the number of events and the capacity of the DVR's disk);
- 2) for a period of **up to 3 months** – provided that a written request is submitted within the deadline referred to in point 1 by a person having a legal interest or on the initiative of the administrator – until the final conclusion of the proceedings or the expiry of the limitation period for claims related to the securing of the recording as evidence. After this time, the data are made available only to authorised authorities on the basis of the provisions of law or are subject to destruction. Exceptions are situations where separate regulations (including the Act of 14 July 1983. *on the National Archival Resources and Archives*) or the internal regulations of the administrator (Uniform Material List of Files) provide otherwise.

7. Your rights

Under the GDPR, you have the following rights:

- you can check what data we process about you and receive a copy of it (Article 15 of the GDPR);
- in certain situations, you can request the deletion of your data ("*right to be forgotten*" – Article 17 GDPR);
- you can suspend the processing of your data for the duration of the processing of your request (Article 18 of the GDPR);
- you can object to the processing of your data for the purposes of legitimate interests (Article 21 of the GDPR);
- you have the right to information (Article 13 of the GDPR) about the use of video surveillance by means of legible warning signs and a shared information clause posted at the entrance to the facility, you should be aware of the presence of cameras, the purpose of their installation, the recipients of the data and the storage time of the recordings, even before you enter the range of their lens;
- if you believe that we process data unlawfully, you can file a complaint with the supervisory authority – the President of the Office for Personal Data Protection – at the address: 00-193 Warsaw, 2 Stawki Street, tel. 22 531 03 00, e-mail: <https://uodo.gov.pl/pl/p/kontakt> (Article 77 of the GDPR);
- You can withdraw your consent at any time, but this does not affect the lawfulness of the processing that took place before its withdrawal (Article 7 of the GDPR).

8. Profiling and automated decision-making

We do not use automated decision-making in individual cases with regard to your personal data, including profiling in accordance with Articles 20 and 22 of the GDPR.

9. Source of data origin

Your personal data is obtained directly from you.

10. Information on voluntariness or obligation to provide data

Entering the monitored area is associated with the automatic recording of your image. Providing this data is not a statutory or contractual requirement, but results from the fact that you are within the range of cameras. It is voluntary in the sense that the decision to enter the Administrator's premises is up to you. If you enter, your data will be recorded.

11. Information about the intention to transfer personal data to a recipient in a third country or international organisation and about the determination or absence of an adequate level of protection by the European Commission or in the case of a transfer referred to in Article 46, Article 47 or Article 49(1), second subparagraph, GDPR

We do not currently transfer or plan to transfer personal data to third countries (outside the EEA) or international organizations. Exceptions are the use of Microsoft 365 and Active Directory software, which involves storing data in the cloud within the Microsoft 365 tenant structure and may result in data being transferred outside the EEA. However, Microsoft guarantees the highest standards of security and privacy protection, as confirmed by independent audits and ISO/IEC 27001 and ISO 27018 certifications, guaranteeing compliance with international standards and assurance that your data in the cloud and within the tenant will not be used for marketing purposes.

The following documents govern Microsoft's data processing and data protection policy:

- "Microsoft Privacy Statement" – available at the link: <https://www.microsoft.com/pl-pl/privacy/privacystatement> and;
- "Microsoft Services Agreement" - link: <https://www.microsoft.com/pl-pl/servicesagreement>