

INFORMATION CLAUSE

ŁUKASIEWICZ RESEARCH NETWORK - INSTITUTE OF POLYMER MATERIALS

ABOUT THE PROCESSING OF PERSONAL DATA

PERSONS REPORTING VIOLATIONS OF THE LAW

In order to comply with the legal obligation imposed on the Controller of personal data by the provisions of Article 13(1) and (2) of the Regulation. 1 and 2 and Article 14(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 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

Your personal data will be processed on the basis of:

- 1) Article 6(1)(c) GDPR in conjunction with the Act of 14 June 2024 *on the protection of whistleblowers* - in order to receive and consider a report of a violation of the law, to follow up, contact the whistleblower, document the report and to fulfil the obligations arising from the said Act;
- 2) Article 6(1)(f) of the GDPR – in order to establish, pursue or defend against claims related to the notification or the ongoing investigation (legitimate interest of the Administrator);
- 3) Article 9(2)(g) GDPR in connection with the provisions of the *Whistleblower Protection Act*, when the processing is necessary for an important public interest as defined by law (where special categories of personal data have been included in the notification);
- 4) Article 6(1)(a) of the GDPR in the event that you have given your explicit consent to the disclosure of your identity. Such consent is voluntary and may be withdrawn at any time. The withdrawal of consent does not affect the lawfulness of the processing carried out before its withdrawal.

Your personal data may be processed on the basis of Article 6(1)(e) of the GDPR to the extent necessary for the performance of the statutory tasks of the Administrator performed in the public interest - the performance of tasks related to detecting, preventing and combating violations of the law and the protection of the public interest in the Administrator's activities.

4. Type of personal data and categories of data subjects

With regard to: whistleblowers reporting a violation of the law; persons to whom the report relates (i.e. persons to whom a violation of the law is attributed); persons indicated in the report as witnesses, persons with information or persons associated with the case; persons assisting the whistleblower in making a report; persons associated with the whistleblower who may experience retaliation; employees, co-workers, contractors and other persons whose data are necessary to consider the report and follow up on it, the following categories of personal data are processed: identification data (name, surname, job position, place of work); contact data (correspondence address, e-mail address, telephone number); data concerning employment, cooperation or relations with the Controller; data contained in the content of the report, explanations, attachments and documentation related to the report; data concerning the circumstances of the reported violation of the law; other data necessary to accept the report, follow up and perform obligations under the Act *on the Protection of Whistleblowers*.

If it is necessary to clarify the matter, the Controller may also process special categories of personal data referred to in Article 9(1) of the GDPR, if they have been included in the notification or collected in the course of follow-up actions, in particular data concerning health, trade union membership or other data of a special category relevant to the case under consideration.

5. Data recipients or categories of data recipients

Your personal data may be disclosed only to persons authorised by the Controller, obliged to maintain confidentiality and processing data to the extent necessary to fulfil the obligations related to receiving reports and conducting follow-up activities. The Controller ensures the confidentiality of your personal data, including information allowing for the establishment of your identity, in accordance with the provisions of the *Whistleblower Protection Act*.

The recipients of your personal data may be entities providing IT services to the Administrator related to the operation of the reporting system (if the report was made electronically), to which the data may

be entrusted for processing on the basis of personal data processing entrustment agreements. Your personal data may also be made available to public authorities, courts, law enforcement agencies and other entities authorized to receive them on the basis of generally applicable provisions of law. Data enabling the identification of a whistleblower are not subject to disclosure to unauthorized persons, unless with the express consent of the whistleblower or when the obligation to disclose them results from the provisions of law.

6. Data retention period

Your personal data will be processed for the period necessary to receive and consider the report, to carry out follow-up actions and to fulfil the obligations arising from the *Whistleblower Protection Act*. Personal data and documentation related to the report will be stored for a period of 3 years after the end of the calendar year in which the follow-up activities were completed or the proceedings initiated by these activities were completed. After the expiry of the retention period, the Administrator deletes personal data and destroys documentation related to the report, unless their further storage results from separate provisions of law. The provisions of the Act of 14 July 1983 do not apply to documentation related to whistleblower reports. *on the National Archival Resources and Archives*.

7. Your rights

Under the GDPR, you have the following rights:

- 1) access to personal data (Article 15 of the GDPR);
- 2) rectification of data (Article 16 of the GDPR);
- 3) restriction of data processing (Article 18 of the GDPR);
- 4) delete data in cases provided for by law (Article 17 GDPR);
- 5) object to data processing based on Article 6(1)(e) or (f) of the GDPR (Article 21 GDPR);
- 6) withdraw consent at any time if the processing is carried out on the basis of Article 6(1)(a) of the GDPR;
- 7) lodge a complaint with the President of the Office for Personal Data Protection, in accordance with Article 77 of the GDPR – if you believe that we process data unlawfully. A complaint to the President of the Office for Personal Data Protection – should be submitted to the address: 00-193 Warsaw, 2 Stawki Street, tel. 22 531 03 00, e-mail: <https://uodo.gov.pl/pl/p/kontakt>.

These rights may be subject to restrictions under the provisions of the GDPR and the *Whistleblower Protection Act*, in particular when their exercise could violate the rights and freedoms of others or make it difficult to follow up.

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

Providing personal data is voluntary. However, failure to provide identification or contact data may make it difficult or impossible to conduct correspondence, obtain additional information necessary to consider the report and provide feedback on the follow-up actions taken. The Administrator is not obliged to consider a report of a Breach committed anonymously and generally leaves it unexamined in the manner specified in the internal regulations.

10. 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>

Definitions:

1. **Personal data/data** - means information about an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a natural person;

2. **Processing** - means an operation or set of operations performed on personal data or sets of personal data by automated or non-automated means, such as collection, recording, organization, structuring, storage, adaptation or modification, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
3. **Consent of the data subject** – means a voluntary, specific, informed and unambiguous expression of will, by which the data subject, in the form of a statement or a clear affirmative action, consents to the processing of personal data concerning him/her.
4. **Recipient** of data – means a natural or legal person, public authority, entity or other entity to which personal data is disclosed, regardless of whether it is a third party. However, public authorities that may receive personal data as part of a specific procedure in accordance with generally applicable law are not considered recipients – the processing of such data by these public authorities must comply with the data protection regulations applicable in accordance with the purposes of the processing; whereby the phrase "third party" means a natural or legal person, public authority, body or entity other than the data subject, the controller, the processor or persons who – under the authority of the Controller or the processor – may process personal data.
5. **GDPR** - 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;
6. **The Act** – is the Act of 14 June 2024. *on the protection of whistleblowers* (Journal of Laws of 2024, item 928).
7. **Whistleblower** – is a natural person who reports or discloses to the public information about a violation of the law obtained in a work-related context, including: (1) an employee; (2) a temporary worker; (3) a person providing work on a basis other than an employment relationship, including a civil law contract; (4) an entrepreneur; (5) a proxy; (6) a shareholder or partner; (7) a member of a body of a legal person or an organisational unit without legal personality; (8) a person performing work under the supervision and direction of a contractor, subcontractor or supplier; (9) an intern; (10) a volunteer; (11) an apprentice; (12) an officer within the meaning of Article 1(1) of the Act of 18 February 1994 on Pension Provision for Officers of the Police, the Internal Security Agency, the Intelligence Agency, the Military Counterintelligence Service, the Military Intelligence Service, the Central Anti-Corruption Bureau, the Border Guard, the Marshal Guard, the State Protection Service, the State Fire Service, the Customs and Tax Service and the Prison Service and their families; (13) a soldier within the meaning of Article 2(39) of the Act of 11.03.2022 on the Defence of the Homeland.
8. **A legal entity** – as defined in Article 2(10) of the Act, it is Łukasiewicz – IMPIB, which is an institute of the Network (a state-owned legal entity), operating on the basis of the Act of 21 February 2019 on *the Łukasiewicz Research Network* (Journal of Laws of 2026, item 194).
9. **Breach** – it should be understood as information, including reasonable suspicion regarding an existing or potential violation of the law, which has occurred or is likely to occur in a legal entity in which the whistleblower has participated in the recruitment process or other negotiations prior to entering into a contract, works or has worked, or in another legal entity with which the whistleblower maintains or has maintained contact in a work-related context, or information regarding an attempt to conceal such a violation of the law;
10. **Notification** – is an oral or written internal notification or an external application, submitted in accordance with the requirements set out in the Act.
11. **Follow-up action** – it should be understood as an action taken by a legal entity or a public authority to assess the veracity of the information contained in the report and to counteract the violation of the law that is the subject of the report, in particular by means of an investigation, initiation of an inspection or administrative proceedings, filing an indictment, an action taken to recover funds or closing a procedure carried out as part of the internal procedure for reporting violations of the law and taking follow-up actions or the procedure for receiving external reports and taking follow-up actions.
12. **Retaliation** – this should be understood as a direct or indirect act or omission in a work-related context that is caused by a report or public disclosure and that violates or may violate the rights of the whistleblower or causes or may cause unjustified harm to the whistleblower, including the unjustified initiation of proceedings against the whistleblower.