EY VIRTUAL COMPLIANCE OFFICER ("VCO")
TERMS OF USE

§ 1. DEFINITIONS

1. **Irregularity** – any breach of law and/ or internal rules.
2. **Policy** – these rules.
3. **Company** – Fabryka Łożysk Tocznych – Kraśnik S.A. with its registered office in Kraśnik
4. **VCO** – an IT system providing an anonymous channel for reporting Irregularities.
5. **Whistleblower** – a person reporting an Irregularity and/ or a reasonably suspected Irregularity at the Company. The Whistleblower may choose to remain anonymous.
6. **Report** – a notification of an Irregularity and/ or a suspended Irregularity reported via the VCO.
7. **Supplier** - Ernst & Young spółka z ograniczoną odpowiedzialnością Consulting sp. k. in Warsaw.

§ 2. GENERAL

1. The VCO is a tool the Company relies on for its internal purposes linked with reporting Irregularities.
2. The rules governing the VCO are set out in this Policy and the provisions of applicable law.
3. The VCO is designed to facilitate reporting suspected Irregularities in a confidential and easy way and is generally available (to people inside and outside the organisation). Whistleblowers may report Irregularities via the VCO free of charge.
4. A Whistleblower reporting an Irregularity via the VCO is required to comply with this Policy.
5. Communication between a Whistleblower's terminal and the VCO is via encrypted transmission (SSL). The VCO supplier does not disclose IP addresses to the Company. Stored on the Whistleblower's device is solely the cookie with the session identification number (the so-called zero cookie) which is used for enabling a connection with the online reporting system. This cookie file is enabled until the session continues and is then cleared.

§ 3. RULES GOVERNING THE USE OF THE VCO

1. The VCO must not be used in a way that is against the law and acceptable standards of behaviour, i.e. any use of the VCO must respect personal interests and intellectual property rights of third parties.
2. A Whistleblower undertakes not to use the VCO to carry out any act against the law, including particularly for the purpose of blackmailing, libelling, threatening, defaming a person etc.
3. No VCO resources and functions may be used for the purpose of a Whistleblower conducting any operations that would breach the interests of the Company or the VCO supplier and/ or that of using any part of the VCO software and/ or the VCO software source code to develop any other, particularly similar, software.
4. The VCO default settings enable a Whistleblower to report an Irregularity anonymously. The Whistleblower may opt for disclosing his/ her personal data when reporting an Irregularity.
5. The Whistleblower is accountable for his/ her Report, which should refer to the facts the Whistleblower witnessed and/ or those the Whistleblower was informed about and which in the Whistleblower's judgement qualify as an Irregularity. No untrue and/ or defamatory information may be provided in any Report. When providing his/ her Report, the Whistleblower should not disclose any of the Company's confidential information or any special personal data (sensitive data) concerning the Whistleblower or any third parties unless such disclosure is required for the purpose of describing the Irregularity.
6. Once the Report on an Irregularity is submitted, the Whistleblower cannot remove or withdraw his/ her Report, nor may he/ she request the Company and/ or the VCO supplier to do so.
7. The VCO offers the option to request and receive the Company's feedback on a Report, on an anonymous basis.
8. If there is no other contact with the Whistleblower (the Whistleblower did not provide his/ her contact data), the token delivered after the Report was submitted should be retained and kept in a safe place to be

used for checking the status of the Report. Should the token be mislaid, it cannot be set up anew and no Report status checks are available; in this case the Report may be submitted once more and should be accompanied by a statement that a Report concerning a given Irregularity has already been submitted, and the date of the first Report should be provided.

9. The Company guarantees full anonymity and undertakes not to take any action with a view to establishing the Whistleblower's identity, nor will it not seek such information from the VCO supplier. The Company ensures confidentiality of the data and information provided through the VCO unless the Company has a right or duty to report a given Irregularity to competent public authorities under the applicable law.

§ 4. PERSONAL DATA PROTECTION

1. This information on personal data protection is designed to set out the Company's VCO practices in the area of protecting the personal data of all individuals whose personal data are processed and retained in the VCO.

2. The data of the Company, which acts as a data controller, are provided in § 1 of the Policy. The Whistleblower's personal data will be processed and retained by the Company.

3. The personal data kept in the VCO may be disclosed by the Company solely to the VCO solution supplier and his/ her contractors providing VCO maintenance as well as those involved in the process of examining the Irregularities.

4. The VCO is hosted on the supplier's technology platform in the MS Azure data centre managed in the territory of the Netherlands.

5. The personal data processed in the VCO are used in the following way:

- **a.** the Whistleblower's data, if provided by the Whistleblower, serve to identify him/ her at the point when an Irregularity is reported,
- **b.** the data supplied in the Report are used for the purpose of the Whistleblower reporting the Irregularity and the Company examining the Irregularity and proceeding with the Report.

6. The purposes for which the Company uses personal data in the VCO are as follows:

- **a.** the processing of personal data is necessary for the purpose of the data controller and/ or a third party safeguarding their legitimate interests, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.
  A special interest is the Company's intention to discover Irregularities in its organisation,
- **b.** The processing of personal data is necessary in the light of the legal duty imposed on the data controller directly by Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law, which is to enable data controllers to report breaches submitted by whistleblowers.

7. The VCO system processes the following types of personal data: first name, surname, email address, type of relationship with the Company, e.g. an employee, subcontractor, consumer, patient and other categories of data that may be provided in the Report for the purpose of a detailed description of an Irregularity. Such data are supplied by Whistleblowers and may relate to the Company's employees, subcontractors, clients and suppliers or other persons whose data were to be supplied for the purpose of describing the Irregularity.

8. Sensitive personal data are data that disclose racial or ethnic origin, political beliefs, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health or sexual life or orientation. The Company does not deliberately collect any sensitive personal data. The VCO is not designed to process any such data.

9. The personal data stored in the VCO are available to the following persons:

- **a.** the Whistleblower - with access limited to his/ her own Report only,
- **b.** selected employees of the Company or the suppliers involved in the process of examining and proceeding with a given Irregularity,
- **c.** the Supplier's employees - for technical purposes linked with the maintenance of the VCO.

10. The Company may make the personal data collected available to Ernst & Young spółka z ograniczoną odpowiedzialnością Consulting sp. k., which is the VCO supplier. Such data may also be disclosed to EY Group members where reasonably necessary. The Company engages suppliers for the purpose of its internal auxiliary processes, for example service providers to ensure, launch and support the VCO. The suppliers are required to ensure compliance with appropriate data protection standards and the security and confidentiality of personal data.

11. Personal data are kept for the purpose of the Company satisfying its professional and regulatory requirements, for exercising or defending its rights and for archiving and keeping track records. The Company is required to retain information over significant periods of time, i.e. until claims under the applicable law, including the Civil Code, become statute-barred and/ or until illegal acts under the applicable law, including the Criminal Code, become statute-barred. Once the retention period expires, the personal data will be erased.

12. The Company protects confidentiality and security of any data made available to it in the course of its business. Access to such data is restricted and the rules and procedures governing data are designed to protect data against loss, unauthorised use or disclosure.

13. Where an open Report is submitted (i.e. one in which the Whistleblower has provided his/ her personal data), the Whistleblower has a right to request the Company to provide him/ her with the personal data stored in the VCO which concern the Whistleblower.

14. If you want to discuss any issues linked with the processing of personal data in the VCO, please contact iodo@flt.krasnik.pl

§ 5. MISCELLANEOUS

1. This Policy takes effect on the date when it is uploaded to the VCO.

2. The Policy is available in English.

3. Any changes the Company has made to the Policy will take effect on the date when they are uploaded to the VCO.