Have you been a victim of or witnessed mobbing?

Do you see someone violating regulations or breaking the law at work?

Don't be indifferent, become a whistleblower!

Now you can completely anonymously report of a breach through techmark.trusty.report.

INSTRUCTIONS FOR MAKING REPORTS

In accordance with the "Procedure for receiving reports of violations and taking follow-up actions at Techmark sp. z o.o." You can file reports as follows:

1) **through the application platform.**

In order to file a report through the application platform, you need to:

a). go, in a web browser, to https://techmark.trusty.report/,

b). then click on the blue "Make a report" button on the main panel,

c). confirm that you have read the information clause,

c) select "Country of alleged breach" on the drop-down list,

d) fill out the report form honestly. Please keep in mind that the more detailed information the reporting party provides, the better the chances of an accurate and prompt explanation of its report.

Try to provide information that answers the following questions:

- *What happened and what was the exact course of events?*

- *When and where did it happen?*

- *Why did the incident occur?*

- *Who participated in the incident and what was their role (perpetrator, witness, victim)?*

- *In what way did it happen?*

- *Your comments and suggestions.*

e) An attachment (e.g., a photo) may be added to the application,

f) After approving the completed form, you can choose how to apply:

- anonymous - in the last step the system generates login data for the account created on the application platform. Please save/print/photograph your login information, as it will not be possible

to restore it. In the account, you will be able to track how the application is being processed and have a secure (anonymous) dialogue with the follow-ups. It is possible to reveal your identity at any time,

- disclose your identity - by providing your first name, last name, phone number (required data), email address, relationship to the organization, and willingness to receive notifications regarding the violation to the email address provided. In the last step, the system generates login data for the account created on the notification platform. Please save/print/photograph your login information, as it will not be able to be restored. The account will be able to track how the application is processed.

In order to check your report, complete it, or get feedback, you need to:

a). go to https://techmark.trusty.report/,

b). on the main panel of the system click on the pink button "Your inbox" ,

c). confirm that you have read the information clause,

d). enter the username and password you received when reporting the breach and log in to your account,

e). after accessing his/her report, the notifier can at any time:

- read messages from the follow-up person,

- write a message to the follow-up person,

- add a new or further attachment.

Please maintain contact with those conducting the follow-up. This is because we may need additional information from reporting parties necessary to clarify the report and take appropriate follow-up steps,

2) via email to sygnalisci@techmark.com.pl

Please provide as much detailed information as possible and stay in touch. We would like to remind you that when reporting by email, we cannot ensure anonymity, therefore, we only protect the confidentiality of the data of the reporting party.

3) a report may be made **directly to the Human Resources Department** in the presence of two employees. A report is made of the notification, signed by the reporting party and the persons accepting the report. As with email, we only protect the confidentiality of the data of the reporting party.

INFORMATION CLAUSE FOR WHISTLEBLOWERS

The original language of this Information is Polish. Supplier may make available translations of the Terms. In case of conflicts between the Polish version and any translation, the Polish version shall prevail.

Acting pursuant to Article 13 of the General Data Protection Regulation) (GDPR), I hereby inform you that:

1. The controller of your personal data is Techmark sp. z o.o. registered in the National Court Register under the number 0000005619, NIP 726-000-22-12, REGON 470513221, based at 10/12 Piotrkowska Street, 95-070 Aleksandrów Łódzki;
2. the Data Controller can be contacted by mail, by mail, phone at (+ 48) 42 712 17 95 or by email at sygnalisci@techmark.com.pl ;
3. The data controller shall process the personal data provided by you in the report necessary for the investigation and follow-up and protection of the whistleblower, persons assisting in the report or associated with the whistleblower.

   You can get more information in person at the Human Resources Department or at kadry@techmark.com.pl.

4. Your personal data will be processed:

a) in relation to the acceptance of a report or follow-up,
b) in relation to the fulfillment of the obligation to keep a register of reports,
c) in order to fulfill the administrator's legal obligations.

5. Your personal data will be processed on the basis of:

a) Article 6(1)(c) RODO in connection with Article 8(4) of the Law on the Protection of Whistleblowers,
b) Article 6(1)(a) of the RODO if you voluntarily provide your personal data in the case of a previous anonymous report,
c) Article 6(1)(a) RODO in conjunction with Article 8(1) of the Law on the Protection of Whistleblowers to the extent that your identity as a whistleblower is disclosed with your consent,
d) Article 6(1)(f) of the RODO - the controller's legitimate interest in receiving, verifying and clarifying reports of violations and conducting follow-up activities,
e) Article 9(2)(a) of the RODO in conjunction with Article 8(4) of the Law on the Protection of Whistleblowers, if you voluntarily provide special category personal data,
f) Article 9(2)(f) RODO, in conjunction with Article 8(4) of the Law on the Protection of Whistleblowers, if the processing of your special category personal data is necessary for the establishment, investigation or defense of claims,
g) Article 9(2)(g) RODO in conjunction with Article 8(4) of the Law on the Protection of Whistleblowers, if the processing of your special category personal data is necessary for reasons of important public interest.

6. The Controller ensures the confidentiality of your data, in connection with the report received. Accordingly, your data may be shared by the Controller with:

a) entities and bodies to which the Controller is obliged or authorized to make personal data available under generally applicable laws,
b) persons or entities with whom the Controller has entrusted the processing of data, and who provide services for the receipt of reports, investigation and follow-up.

7. Your personal data collected in the register of internal reports will be processed for a period of 3 years after the end of the calendar year in which the follow-up actions were completed, or after the completion of the proceedings initiated by these actions.

If an external report is forwarded to a public authority with jurisdiction for follow-up, the Controller shall keep personal data for a period of 3 years after the end of the calendar year in which the report was forwarded or the follow-up was completed, or after the proceedings initiated by these actions are completed.

Personal data that are not relevant to the processing of the report shall not be collected, and if accidentally collected shall be deleted immediately. The deletion of such personal data shall take place within 14 days after it is determined that it is not relevant to the case.

8. You have the right to demand from the Controller access to your personal data, their rectification, erasure or restriction of processing, as well as the right to object to their processing, but you have the right only if further processing is not necessary for the Controller to comply with a legal obligation and there are no other overriding legal grounds for processing. You have the right to lodge a complaint with the President of the DPA.

9. Provision of data is voluntary, but in the case of not using the anonymous channel to submit a report, it is necessary for the fair implementation of the Controller's legal obligations.