



On 4 October 2021, the assumptions ("Assumptions") to the draft act on the protection of persons who report breaches of law (the so-called whistleblowers) were published in the list of legislative and programme works of the Council of Ministers.

As announced, national regulations on the whistleblower protection will be adopted within the time limit required by the EU directive, i.e. by 17 December 2021. Although the draft act has not been published yet, businesses should already be gearing up for the challenges they will face when putting in place procedures for reporting breaches and protecting whistleblowers.

The Assumptions:

- (1) businesses will be required to **create internal channels and devise procedures for reporting breaches**. These channels must:
 - (i) ensure the confidentiality of the identity of the reporting person and the breaching person,
 - (ii) specify an impartial unit or person(s) competent for receiving reports, confirming such receipt, and following up on the reports within the specified time limits;
- (2) the internal whistleblowing and follow-up procedures will become an **internal legal act that must be agreed with company trade union organisations or –where no trade union organisations operate at a company – consulted with employees' representatives**;
- (3) **breaches can be reported** i.a. by employees, persons engaged on another basis (e.g. service recipient, persons working in the B2B model), management board and supervisory board members, shareholders, volunteers, interns, **and persons employed by contractors, subcontractors and suppliers**. Persons who report breaches after their employment has been terminated or before it has started (e.g. with respect to information disclosed during a job interview) will also enjoy legal protection;
- (4) **whistleblowers will be protected against retaliation** – it will be prohibited to treat the reporting persons adversely in any way, and in case of a potential dispute (e.g. regarding the employment termination), the employer will have to prove that the termination was not linked with a breach report (reversed burden of proof).

Pursuant to the Directive, at the initial stage the regulations discussed above are to apply to entities employing at least 250 employees. **However, the Assumptions suggest that the Polish act may immediately apply to all entities employing at least 50 employees.** Additionally, the Polish legislator intends to introduce a broader catalogue of breaches than that provided for in the Directive that will also include breaches of national provisions.

The introduction of the whistleblower protection will be a responsibility of the **managing staff in the broad sense of the term**. It is their obligation to ensure due care when aligning the company's operations with any new legal requirements.

Building a whistleblowing system is also a challenge in terms of personal data protection. Therefore, in light of the current GDPR provisions, companies are required to take into account data protection not only when developing procedures, but also when choosing the communication channel or specifying the actual scope of obtained information; all this already at the stage of devising a whistleblowing system (privacy by design).

What can we do for you?

To make your company ready for new requirements, we would be happy to help you in:

1. auditing the existing whistleblowing and investigation procedures;
2. developing and implementing internal procedures for reporting breaches, keeping a record of breaches, and keeping documentation in accordance with the Directive / statutory regulations;
3. outsourcing the duties of a compliance officer, operating internal reporting channels, conducting or assisting in conducting an investigation;
4. assisting in ensuring accountability of GDPR obligations (i.e. demonstrating that the whistleblowing system takes into account personal data protection), in particular by putting adequate procedures and policies in place, keeping a register of processing activities for the reporting process, determining the roles of entities participating in reporting breaches, concluding data processing agreements or data co-controlling agreements, minimising data, and training;
5. providing legal advice on preparing internal informative materials;
6. holding internal training sessions;
7. providing support in crisis situations, including in disputes with employees (both at the internal level, and in court).

If you have any questions, feel free to contact our experts.

Experts:**Joanna Ostojka-Kołodziej, PhD**

Adwokat (Attorney-at-law)

Counsel

Head of Employment Practice

joanna.ostojka@jdp-law.pl**Anna Matusiak-Wekiera**

Radca prawny (Attorney-at-law)

Head of Data Protection / Compliance practice

anna.matusiak-wekiera@jdp-law.pl**Magdalena Bartnik**

Adwokat (Attorney-at-law)

Associate

magdalena.bartnik@jdp-law.pl

All information contained in this newsletter is available free of charge. This newsletter is not an advertisement and serves information purposes only. None of the information contained in this material should be construed as legal advice or a commercial offer, including within the meaning of Article 66 § 1 of the Civil Code. JDP DRAPAŁA & PARTNERS Sp.j. is not liable for any claims, losses, demands or damage arising out of or relating to the use of information, content or materials contained in this newsletter.

The controller of your personal data for the purposes of: (i) informing on practicing a profession and the related activity, (ii) exchanging correspondence, (iii) archiving, is JDP DRAPAŁA & PARTNERS Sp. j. with its registered office in Warsaw. You will find more information on data processing [here](#).