DPDgroup IT Solutions sp. z o.o.
Whistleblowing Procedure

DPDgroup IT Solutions sp. z o.o.
ul. Krakowiaków 16, 02-255 Warszawa, Polska
www.dpdgroupitsolutions.pl

Author	Approver
Administration Division	Iwetta Krawczyk – Finance and Admin Director

Version No.	Effective Date	Purpose of the change
V1	10/04/2025	Creation of the Procedure

GEOPOST

CONTENTS

Introduction

At DPDgroup IT Solutions (hereinafter the "**DGITS PL**") all our team members and certain stakeholders may report behaviour that is contrary to the values and principles of Geopost or to the laws and regulations in force (hereinafter the "**Alerts**").

This Whistleblowing Procedure (hereinafter referred to as the "Procedure") has been created based on the provisions of the Act of June 14, 2024, on the Protection of Whistleblowers and defines:

(i) the rules regarding the emission, reception and handling of Alerts made, included via the Whistleblowing System; and
(ii) the rights granted to the whistleblower and certain persons connected to them.

All terms used in this Procedure are defined in **Appendix 1**.

1. Who can file an Alert?

An alert may be filed via the Alert System by: (i) all persons performing their duties within DGITS PL and (ii) certain stakeholders of DGITS PL as defined below.

(i) Within DGITS PL

The persons who may file an Alert include:

- Corporate officers;
- Persons under a contract of employment;
- Interns, trainees and temporary workers.

(ii) DGITS PL Stakeholders

DGITS PL stakeholders may also file an Alert, provided that it relates to facts related to the relationship they have or have had with DGITS PL

For DGITS PL, this may include:

- former employees;
- shareholders;
- directors;
- candidates for employment/cooperation with DGITS PL
- co-contractors (including suppliers, service providers, etc.) their employees and members of their management, executive and/or supervision bodies; and
- subcontractors of its co-contractors, their employees and members of their management, executive and/or supervision bodies.

All interested parties will be able to review the content of this Procedure by visiting the website https://dpdgroupitsolutions.pl/pl/ and navigating to the "Whistleblowers" section

2. What topics can Alerts cover?

Any person belonging to one of the categories mentioned in 1. above may report violations concerning:

1. corruption;
2. public procurement;
3. financial services, products, and markets;
4. anti-money laundering and counter-terrorism financing;
5. product safety and compliance with requirements;
6. transport safety;
7. environmental protection;
8. radiological protection and nuclear safety;
9. food and feed safety;

10. animal health and welfare;
11. public health;
12. consumer protection;
13. privacy and personal data protection;
14. security of networks and information systems;
15. financial interests of the State Treasury of the Republic of Poland, local government units, and the European Union;
16. the internal market of the European Union, including public competition rules and state aid as well as corporate taxation;
17. constitutional freedoms and human and citizen rights - in the context of interactions between individuals and public authorities, unrelated to the areas listed in points 1-16.

3. How to file an Alert?

Alert under this Procedure can be filed through the Whistleblowing System.

3.1 Filing an Alert via the Whistleblowing System

The Whistleblowing System offers the whistleblower two possibilities:

(i) entering the information relating to their Alert on the online whistleblowing platform, part of the Whistleblowing System accessible at the following address: https://www.safecall.co.uk/clients/dgitspol/ (hereinafter the "**Whistleblowing Platform**"); or
(ii) sharing their Alert information by phone, by calling the following toll-free number: 800 7233 2255.

(i) Via the Whistleblowing Platform

When a person wishes to file an Alert via the Whistleblowing Platform, they proceed as follows:

- Step 1: access the landing page of the Whistleblowing Platform dedicated to DGITS PL, by entering the address in their browser https://www.safecall.co.uk/clients/dgitspol/.
- Step 2: select the language of the Whistleblowing Platform interface (Polish or English); and
- Step 3: enter the information of their Alert by following the instructions displayed on the screen.

The landing page of the Whistleblowing Platform also offers the possibility for the whistleblower to consult/update a previously filed Alert.

(ii) By telephone

When a person wishes to file an Alert by telephone, they proceed as follows:

- Step 1: call number 800 7233 2255.
  This number is free of charge and available 24/7;
- Step 2: choice of the language (Polish or English) in which they wish to file their Alert;
- Step 3: confidentially discuss with the speaker on the details of the Alert, and answering the questions asked by the latter.

3.2 Identification of the Alert whistleblower when the Alert is filed

Although the whistleblower may file their Alert anonymously, **it is recommended that they identify themselves**.

Identifying themselves with DGITS PL when the Alert is filed will:

- facilitate the exchange of additional information;

- facilitate the review of the Alert; and
- ensure protection against possible Retaliation.

When the whistleblower chooses to disclose their identity, they must send any information proving:

- that they perform their duties within DGITS PL
  or
- that they are a stakeholder in DGITS PL as defined in 1. above.

4. How is an Alert handled?

Once an Alert is filed, it is treated in several stages, under the responsibility of the Ethics Officer of **DGITS PL**
The whistleblower is involved throughout the process.

4.1 Step 1 – Initial entering and updating of information relating to the Alert

Provided that the whistleblower has given their consent, the information relating to the Alert is entered into the Whistleblowing Platform.

This information is entered into the platform according to what has been either:

- entered directly by the whistleblower on the Whistleblowing Platform;
- communicated by the whistleblower when calling the number indicated in 3.1 above and transcribed by the contact with whom the Alert was filed;

In all cases, the whistleblower is invited to describe the facts they report:

- as accurately, clearly and in as much detail as possible;
- providing factual information; and
- supporting the Alert with any evidence proving the facts reported (e.g. letters, e-mails, SMS, etc.).

Information relating to the Alert will be accessible by:

(i) Safecall, when the Alert is created, to check the completion of the information and ask for additional information to the whistleblower if needed;
(ii) the Ethics Officer of DGITS PL and any persons authorised to process Alerts (hereinafter the "**Authorised Persons**") within DGITS PL, once they have been notified by Safecall of the creation of a new Alert; as well as
(iii) the whistleblower.

4.2 Step 2 – Reception of the Alert and acknowledgement of receipt by **DGITS PL**

Once the information relating to the Alert has been recorded on the Whistleblowing Platform and checked by Safecall, the Ethics Officer of DGITS PL or other Authorised Persons within DGITS PL receive a notification informing them of the creation of a new Alert.

The whistleblower is then informed by the Ethics Officer of DGITS PL or any Authorised Person within DGITS PL that the Alert has been received, by sending an acknowledgement of receipt.

This must take place within 7 days of receipt of the Alert, unless the whistleblower has not provided a contact address to which the confirmation should be sent.

This acknowledgement of receipt reminds the whistleblower of the protections provided for in this Procedure (for more information on these protections, refer to 5. below).

When the Ethics Officer of DGITS PL or any Authorised Person within DGITS PL considers that the Alert relates to events that have occurred or are likely to occur in other entity belonging to Geopost, they may invite the whistleblower:

- to send their Alert to this entity as well; and/or
- to withdraw the Alert that they have filed to DGITS PL, if the Ethics Officer of DGITS PL (or any Authorised Person within DGITS PL) considers that the Alert will be handled more effectively by this other entity alone.

4.3 Step 3 – Analysis of the admissibility of an Alert

Once they are being aware of the Alert, the Ethics Officer of DGITS PL (or any Authorised Person within DGITS PL) shall first analyse the information relating to it in order to determine whether it meets the conditions of admissibility (hereinafter an "**Admissible Alert**").

To be Admissible, an Alert must:

(i) be sufficiently precise, clear and detailed and include elements necessary allowing its proper analysis (e.g. letters, e-mails, SMS, etc.);
(ii) be based on evidence that can be verified and confirmed (and not on vague suspicion or rumours);
(iii) be filed by a person belonging to one of the categories mentioned in 1. above; and
(iv) relate to one of the subjects mentioned in 2. above.

The Ethics Officer (or any Authorised Person within DGITS PL) conducts an investigation and reviews the report promptly, within no more than 3 months from the date of its receipt.
The Ethics Officer (or any Authorised Person within DGITS PL) provides feedback to the whistleblower, which includes, in particular, information on whether a legal violation was found or not, and any measures that have been or will be taken in response to the identified violation. Feedback should be provided promptly after the completion of the investigative procedure.

4.4 Step 4 – Verification of the facts relating to the Alert during the Investigation

When the Alert is qualified as Admissible, the Ethics Officer of DGITS PL shall lead the Investigation to verify the facts relating to the Alert and whether it is confirmed by substantiated evidence (hereinafter a "**Substantiated Alert**").

The Investigation is conducted:

- by the Ethics Officer of DGITS PL themselves; or
- by the Ethics Officer of DGITS PL and one or more Authorised Person(s) within DGITS PL;
  In this case, it is the Ethics Officer of DGITS PL who appoints the latter, in concertation with the President of Management Board or two Board Members of DGITS PL.

In order to ensure the Investigation is handled in an independent and impartial manner, the Ethics Officer of DGITS PL and/or the Authorised Person(s) within DGITS PL appointed to conduct the Investigation (hereinafter the "**Investigators**") are specially trained for this purpose.

In the event that an Investigator contacts a third party for their cooperation in the conduct of the Investigation (in particular to communicate documents, participate in an interview or otherwise), the latter has a duty to preserve the confidentiality of their exchanges, under penalty of sanctions, in particular disciplinary sanctions.

4.5 Step 5 –Alert follow-up with the whistleblower

On the Whistleblowing Platform, the Ethics Officer of DGITS PL (or any Authorised Person within DGITS PL) and the whistleblower may access a secure messaging service, guaranteeing the anonymity of the whistleblower, if applicable.

They may thus communicate about the processing of the Alert filed directly via this service, or by any other means guaranteeing the confidentiality of their discussions.

For example, the whistleblower may be contacted:

(i) During the Admissibility Analysis, in order to invite them to transmit information and documents which may complement and/or substantiate their initial Alert;
(ii) During the Investigation, in order to obtain details or any document likely to support the allegations made under the Alert.

4.6 Step 6 – Closure of the Alert

The Ethics Officer of DGITS PL is responsible for appropriately closing:

(i) Alerts which are not-Admissible;
(ii) Alerts which are Admissible, but not Substantiated; and
(iii) Alerts which are Admissible and Substantiated, after the implementation of any pertinent disciplinary measures and/or legal actions where applicable.

The rules concerning the closure of an Alert are specified below.

4.6.1 Informing the whistleblower

The whistleblower shall be informed by the Ethics Officer of DGITS PL (or any Authorised Person within DGITS PL) of the closure of their Alert.

The information provided to the whistleblower on this occasion differs depending on whether the Alert is (i) not Admissible or (ii) Admissible.

(i) If the Alert is qualified as non-Admissible because it does not meet the criteria mentioned in 4.3 above, the Ethics Officer of DGITS PL (or any Authorised Person within DGITS PL) shall inform the whistleblower:

- the reasons why they considered the Alert to be non-admissible; and
- any directorates, departments or persons to whom the whistleblower may disclose the facts initially reported in the context of this Procedure, in order for remedial actions to be taken, where applicable.

(ii) If the Alert is qualified as Admissible, the Ethics Officer of DGITS PL (or any Authorised Person within DGITS PL) shall inform the whistleblower of:

- the actions taken in response to the Alert;
- measures taken to assess the accuracy of the facts reported in the Alert; and
- measures taken, if necessary, to remedy them.

The feedback is provided to the whistleblower within a period not exceeding 3 months from the date of confirmation of receipt of the Alert or, if no confirmation was provided, within 3 months from the expiration of 7 days from the date the Alert was made, unless the whistleblower has not provided a contact address to which the feedback should be sent.

4.6.2 Anonymisation and archiving of the Alert

The Ethics Officer of DGITS PL is responsible for rendering all Personal Data transmitted in connection with the Alert anonymous (hereinafter the "**Anonymisation**"), or for deleting them, if necessary.

Personal data related to the receipt of the report, information contained in the Internal Report Register, data processed in connection with follow-up actions, and other documents related to the report are stored 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 proceedings initiated by those actions.

4.6.3 Internal Reports Register

DGITS PL maintains an internal Reports Register and serves as the controller of personal data contained within this register. DGITS PL authorizes the Ethics Officer and employees collaborating with them in the process of receiving and handling reports to make entries in the register and to update the information in the register as necessary to reflect the factual state.

DGITS PL collects, among others, the following data in the internal Reports Register:

- Alert number;
- subject of the violation;
- personal data of the whistleblower and the person to whom the Alert pertains, necessary for - identifying these individuals;
- whistleblower's contact address (If provided);
- date of the Alert submission;
- information on follow-up actions taken;
- date of case closure.

5. How are the whistleblower and the other persons concerned protected?

The whistleblower has a certain number of rights protecting them when filing an Alert under this Procedure.

This protection also extends to certain categories of persons who may be involved in the process (persons referred to in the Alert, closely connected with the whistleblower, assisting the whistleblower, etc.), as the case may be.

5.1 Confidentiality and integrity of information relating to the Alert

Any information relating to an Alert communicated by the whistleblower must be:

- strictly confidential; and
- protected with regards to its integrity.

These protections aim to protect:

- the identity of the whistleblower;
- information relating to the Alert.

5.1.1 Measures to ensure the confidentiality and integrity of information relating to the Alert

To guarantee this confidentiality and integrity, the Ethics Officer of DGITS PL is themselves specially trained in this regard and subject to a strengthened confidentiality obligation.

In addition, they shall ensure that the Authorised Persons within DGITS PL involved in handling an Alert:

- are limited in number, to the strict minimum;
- are formally authorised to read and treat the Alert;
- have, due to their position within DGITS PL or otherwise due to their status, the competence, authority and sufficient means to carry out their tasks;
- are able to demonstrate they are impartial and do not present in a conflict of interest; and
- have received proper training.

If information relating to the Alert is required to be communicated to third parties, the Ethics Officer of DGITS PL must ensure that such communication:

- is subject to the prior agreement of the Whistleblower if it involves the disclosure of their identity;
- is necessary to handle the Alert;
- does not imply the disclosure of information to identify the targeted person before the Alert is confirmed (unless it is required by the judicial authority).

The identity of the person(s) targeted in the Alert shall also be protected in this respect.

5.1.2 Sanctions

Whoever makes a report or public disclosure, knowing that no violation of the law has occurred, shall be subject to a fine, a penalty of restriction of liberty, or imprisonment for up to two years.

DGITS PL also reserves the right to impose sanctions against any person initiating such disclosure.

5.2 Protection against retaliation

The following persons may benefit from protection against Retaliation:

(i) any whistleblower, filing an Alert:

- relating to one of the topics mentioned in 2. above;
- relating to facts of which they have become personally aware or, at the very least, of which they have become aware in the context of their professional activity;
- with reasonable grounds to believe that the information reported was true when filing (hereinafter "**Good Faith**");
- without direct financial consideration; and
- without breaching any legally protected secrets (such as secrets related to medical, classified information, attorney-client privilege, judicial deliberations and investigation or judicial inquiry).

(ii) any person:

- who is connected with the whistleblower and could suffer from direct or indirect actions, undertaken on the basis of an Alert ("**Retaliation**") in the context of past, current or future work activities (the "**Work-Related Context**").
  These may be colleagues or relatives of the whistleblower;
- persons assisting the whistleblower as part of the Alert process in a Work-Related Context, and whose assistance must remain confidential; and/or
- persons contacted or questioned by an employee of Geopost or an external service provider formally authorised to receive, become aware of and treat an Alert, and/or provide information or documents to any Authorised Person within DGITS PL;

(iii) any legal entity that the whistleblower:

- owns; or
- for which they work; or
- with which they are otherwise connected in a Work-Related Context.

5.2.1 Purpose of protection

The persons mentioned above may not be subject to any Retaliation measures taken due to:

- the Alert they have filed;
- the Alert that they have facilitated or aided; or
- their connection with the whistleblower.

Any type of Retaliation in response to an Alert is prohibited, including threats or attempts at Retaliation.

Retaliation includes but is not limited to the following:

- suspension, lay-off, dismissal or equivalent measures;
- demotion or withholding of promotion;
- transfer of duties, change of workplace location, reduction in wages, change in working hours;
- withholding of training;

- negative performance assessment or employment reference;
- imposition or administration of disciplinary measures imposed or administered, reprimand or other penalty, including financial sanction;
- coercion, intimidation, harassment or ostracism;
- discrimination, disadvantageous or unfair treatment;
- failure to convert a temporary employment contract into a permanent one, where the worker could legitimately expect to be offered a permanent employment;
- failure to renew or early termination of a temporary employment contract;
- harm, including to the person's reputation, particularly in social media, or financial loss, including loss of business and loss of income;
- blacklisting based on sector or industry level formal or informal agreement, which may entail that the person will not find employment in the future in the sector or industry;
- early termination or cancellation of a contract for goods or services; and/or
- cancellation of a licence or permit.

Protection against Retaliation also protects the above-mentioned individuals from legal action and possible prosecution based on information relating to their Alert.

5.2.2 Sanctions for Retaliation

DGITS PL has a zero-tolerance policy for Retaliation.
Any person directly or indirectly engaging in Retaliation against protected persons shall be subject to disciplinary and/or legal action.

5.2.3 Cases of exclusion from protection

A whistleblower is not entitled to legal protection if the report or public disclosure was made knowingly in bad faith, for instance, with full awareness that the reported information is false.

Furthermore, the wrongful use of the Whistleblowing System may lead to disciplinary sanctions as well as legal actions (for example: declaration made with the aim of harming a person, deliberately false declaration, etc.).

5.3 Right to Alert

When they become aware of a wrongful act, any person concerned by this Procedure is free to file an Alert or not.
Failure to file an Alert shall not lead to any sanction.

Whoever prevents or significantly hinders a whistleblower from making a report shall be subject to a fine, a penalty of restriction of liberty, or imprisonment for up to one year.

6. Protection of personal data

6.1 Processing of Personal Data

The processing of personal data of the Whistleblower, individuals involved in the report, individuals assisting in the submission of the report, and individuals connected to the Whistleblower is carried out based on the provisions of the GDPR.
The data controller for the personal data of the individuals making the report, those involved in the report, those assisting in the submission of the report, and those connected to the Whistleblower is DGITS PL.

Access to the personal data of the Whistleblower and other individuals whose personal data is processed during the investigation may only be granted to persons authorized to process personal data in this regard. The template for the authorization to process personal data is attached as Appendix 2 to the Procedure.

The responsibility for fulfilling the information obligation towards the Whistleblower, the individual involved in the report, the individual assisting in the report, and individuals connected to the report lies

with the Ethics Officer or any Authorised Person within DGITS PL. To fulfil this obligation, an information clause based on Articles 13 and 14 of the GDPR will be applied.

The information obligation towards the individual involved in the report may be postponed if it could create a risk of preventing or seriously hindering the investigation process. In such cases, the Ethics Officer or any Authorised Person within DGITS PL will document the reasons for the delay in fulfilling the information obligation. The information clause will be provided as soon as the identified risk has ceased.

Personal data that is unrelated to the allegations will be deleted immediately after the report is received. An individual whose negative actions are the subject of suspicion may not be held liable for disciplinary actions until the investigation is concluded, and any actions taken against such an individual in connection with the report are prohibited.

6.2 Rights attached to Personal Data

The whistleblower, the persons targeted by an Alert and, more generally, any person identified in connection with an Alert or its handling shall be informed, where possible, of the collection of Personal Data concerning them.

These persons shall have a right of access, rectification, opposition, where possible, and erasure of their Personal Data.

Persons whose Personal Data is thus processed may exercise their rights by contacting dgits@dpdgroup.com.

6.3 Storage of collected data

The deadlines and procedures for Personal Data archiving are specified in 4.6.2 above.

7. External reporting and public disclosure

A report may, in any case, also be made to the Commissioner for Human Rights or a public authority, and, where appropriate, to institutions, bodies, or entities of the European Union, bypassing the procedure outlined in the Procedure.

The public authority establishes a procedure for receiving external reports and taking follow-up actions, which particularly defines the procedure for handling information about legal violations reported anonymously.

The Commissioner for Human Rights and the public authority ensure that the procedure for receiving external reports and the associated processing of personal data:

- prevent unauthorized persons from gaining access to information covered by the report;
- guarantee the confidentiality of the Whistleblower's identity and the identity of the person concerned by the report.

A Whistleblower may make a report as part of a public disclosure and is protected if:

- they have made an internal report, followed by an external report, and within the time limit for providing feedback established in the internal reporting regulations, and subsequently, within the time limit for providing feedback established in the procedure for reporting legal violations to the public authority, the employer and then the public authority fail to take appropriate follow-up actions or fail to provide feedback to the Whistleblower; or
- they make an external report immediately, and within the time limit for providing feedback established in the procedure for reporting legal violations to the public authority, the public authority fails to take appropriate follow-up actions or fails to provide feedback to the Whistleblower unless the Whistleblower has not provided a contact address for the feedback to be sent to.

A Whistleblower making a public disclosure is also protected if they have reasonable grounds to believe that:

- the violation may pose a direct or obvious threat to the public interest, particularly if there is a risk of irreversible harm, or
- making an external report would expose the Whistleblower to retaliatory actions, or
- in the case of making an external report, there is little likelihood of successfully preventing the violation due to special circumstances of the case, such as the possibility of concealing or destroying evidence, or the possibility of collusion between the public authority and the perpetrator of the violation, or the involvement of the public authority in the violation.

8. Implementation of the Procedure

The procedure has been subject to consultations with employee representatives.

The procedure enters into force 7 days after being communicated to employees and associates.

It can be revised at any time at the initiative of DGITS PL

The latest version of the Procedure is published on the website at the address www.dpdgroupitsolutions.pl and DGITS PL Intranet at https://geopostgroup.sharepoint.com/sites/DGITSPL-intranet.

Each DGITS PL employee and associate is obliged to read the Procedure and confirm that it was read.

Appendix 1: Definitions

Alert	information, including a justified suspicion, regarding an actual or potential violation of the law that has occurred or is likely to occur at DGITS PL
Alert, Admissible	any Alert that, as determined by the Ethics Officer of DGITS PL or any Authorised Person within DGITS PL, has met the conditions of admissibility defined in 4.3
Alert, Substantiated	any Admissible Alert that is considered verified and confirmed by substantiated evidence
Anonymisation	the process of rendering all Personal Data anonymous
Authorised Person	any DGITS PL team member or external service provider formally authorised to receive, be aware of and handle an Alert
DGITS PL	DPDgroup IT Solutions sp. z o.o. with its registered seat in Warsaw, address: ul. Krakowiaków 16, 02-255 Warsaw, entered into register of business entities of National Court Register maintained by the District Court for the capital city of Warsaw in Warsaw, XIV Commercial Division of the National Court Register under n° 0000713060, share capital: PLN 31 005 000,00, NIP: 5223110136
GDPR (General Data Protection Regulation)	the common name for **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). The regulation aims to ensure a uniform level of personal data protection across the European Union, foster trust in digital services, and strengthen individuals' control over their personal data
Ethics Officer	the person in charge of ethics and compliance within DGITS PL
Investigation	the objective, impartial and documented process for verifying the merits and severity of an allegation submitted as part of an Alert in order to determine if any wrongdoing has occurred, is occurring or may occur
Investigator(s)	the person(s) responsible for investigating an Alert
Personal Data	any information relating to any natural person that can be used to identify said person, directly or indirectly
Procedure	DGITS PL whistleblowing procedure
Retaliation	any direct or indirect action, undertaken on the basis of an Alert, against the whistleblower or which would cause harm to the whistleblower, to persons closely associated with them, such as colleagues or relatives who are in a Work-Related Context, or to legal entities owned by the whistleblower or with which the whistleblower is otherwise connected in a Work-Related Context
Whistleblower	a natural person who reports a violation in a work-related context, regardless of their position, form of employment, or type of cooperation
Whistleblowing System	the technical system implemented to receive an Alert, either via telephone or via the Whistleblowing Platform
Work-Related Context	past, present or future work activities through which an individual acquires information about wrongdoing

AUTHORIZATION TO PROCESS PERSONAL DATA

I authorize ..... (name and surname), to process personal data (including special categories of data) of individuals in connection with investigations within the framework of the procedure indicated in the Procedure for reporting and handling violations of law and protection of whistleblowers at DPDgroup IT Solutions sp. z o.o., in particular, data concerning whistleblowers, persons affected by the report, and witnesses in the investigation.

The authorization shall expire upon termination of participation in the work of the team accepting applications.