PERSONAL DATA PROTECTION POLICY

GRIMALDI GROUP

Internal Use

REGISTER OF MODIFICATIONS

Rev.	Date	Description	State	Preparation

Verification	Approval

CONTENTS

1. OBJECTIVE 4

1.1 SCOPE OF APPLICATION 4
1.2 REFERENCE REGULATIONS 5

2. PERSONAL DATA PROTECTION POLICY 6

3. RIGHTS OF THE PARTY CONCERNED 14

3.1 EXERCISE OF THE RIGHTS OF THE PARTY CONCERNED AND FEEDBACK TIMES 14
3.2 RIGHT OF ACCESS TO DATA BY THE PARTY CONCERNED 15
3.3 RIGHT OF REPLY 16
3.4 RIGHT OF CANCELLATION 16
3.5 RIGHT OF LIMITATION OF PROCESSING 17
3.6 RIGHT TO DATA PORTABILITY 17
3.7 RIGHT OF OPPOSITION 17

1. OBJECTIVE

The objective of this Policy is to represent the rules and principles to which the Companies belonging to the Grimaldi Group have adapted in compliance with as established:

- by EU Regulation no. 679/2016 *General Regulation on Data Protection* (hereinafter also "Regulation");
- by Legislative Decree no. 196/2003 *"Code regarding the protection of personal data"* (hereinafter referred to as the "Privacy Code"), by the annexes to the Code as amended by Law 25 October 2017, no. 163 *Delegation to the Government for the implementation of European directives and the implementation of other European Union deeds - 2016-2017 European Delegation Law*;
- by the Measures, Guidelines and Opinions issued by the Authority for the protection of personal data (hereinafter "*Privacy Guarantor*"), by the Working Party (WP) pursuant to art. 29[1] and by the European Data Protection Supervisor (EDPS).

The purpose of this Policy is to describe the commitment of the Companies belonging to the Grimaldi Group to:

- protect and safeguard personal and confidential data;
- regulate the processing of personal and confidential data;
- establish the principles of good management for personal and confidential data;
- ensure that all processing takes place in compliance with the fundamental rights, freedoms and dignity of individuals;
- ensure the confidentiality of information relating to customers and to all those that have dealings with individual Group companies.

1.1 Scope of Application

The Policy applies to all processing of personal, confidential, risky, sensitive and judicial data carried out for any reason by the Grimaldi Group Companies (as better identified below) operating in Italy, each of which in their role as independent Controller of the processing of personal data carried out at the company or in their role as co-controllers for the areas covered by a specific agreement, signed on 21/05/2018.

In addition, this Policy applies to all personal data of individuals (including, by way of example and not exhaustively, those relating to data of employees, customers, suppliers and third parties operating as individual) as well as any information of a personal nature or with personal data characteristics received from other Group entities (including those located in other Member States).

[1] The Group, established by art. 29 of Directive 95/46, is an advisory and independent body composed of a representative of the personal data protection authorities designated by each Member State, the EDPS (European Data Protection Supervisor), and by a representative of the Commission. The Working Party pursuant to article 29 will be replaced as of 25 May 2018 by the *European Data Protection Board*. The board, which will replace WP29, is a vital element of the reform and will have to be fully operational from day one.

The legal entities of the Grimaldi Group (hereinafter referred to collectively as "*Group Companies*") to which the contents of this Policy on the protection of personal and confidential data of customers (hereinafter referred to as "the Policy") are applied are:

Grimaldi Group S.p.A.

Grimaldi Euromed S.p.A.

Grimaldi Deep S.p.A.

1.2 Reference Regulations

[1] EU Regulation no. 679/2016 *on the protection of individuals with regard to the processing of personal data, as well as on the free circulation of such data and repealing Directive 95/46/EC* (General Data Protection Regulation);
[2] Legislative Decree no. 196/03 *Code regarding the protection of personal data;*
[3] Document WP 243 - *Guidelines on Data Protection Officers (DPO) of 13 December 2016*;
[4] Document WP 248 rev. 01 - *Guidelines on impact assessment on data protection and determination of the possibility that processing "may present a high risk"*
[5] Document WP 250 rev. 01 - *Guidelines on Personal data breach notification*

2. PERSONAL DATA PROTECTION POLICY

The Companies belonging to the Grimaldi Group undertake to protect the personal and confidential data processed in any capacity by adapting their actions to the following general principles:

A. Collecting and processing information

Group companies shall take the measures and precautions to verify that information containing personal data is relevant, accurate, complete and current as is necessary for the purposes for which it is to be used.

The processing of personal data carried out complies with the principle of data minimization pursuant to art. art. 5, paragraph 1, lett. c), of the Regulation according to which the collection and subsequent processing of personal data takes place in such a way as to minimize the use of personal data identifying the parties concerned.

If some processing operations, or processes or process phases, do not require the clear display of personal data and identification of the parties concerned, the same processing operations must be carried out using data that is either anonymous or, at least, codified.

B. Policies

Group Companies make every effort to ensure that all processing operations are carried out in compliance with the requirements of art. 13 of the Regulation.

The policy must always be provided to parties concerned at the time of data collection, even when it is not necessary to request their consent to processing.

The policy complies with the following principles:

- it is not permitted to process personal data without having previously provided the policy;
- it is not permitted to process personal data for purposes other than those indicated in the policy already provided to customers; further purposes can be integrated in the policy subject to sharing with the Data Processors.
- it is not permitted to communicate data to categories of third parties other than those indicated in the policy. Any other categories of parties deemed necessary for the purposes of data processing can be included in the policy after sharing with the Data Processors.

Group Companies undertake to ensure periodic updating and/or review of the various policies both on paper (i.e. employee policy, maritime policy, passengers passenger policy, etc.) and electronically (i.e. website policies).

C. Choice and consent

Group Companies undertake to respect the obligation to collect consent as set out in articles 6 and 7 of the Regulation.

Consent is validly provided when:

- it is preceded by a correct and complete policy;
- it is freely expressed;
- it is univocally referred to specific processing;
- it is documented in writing in relation to the type of data collected (ex. use of sensitive data).

Pursuant to article 6 paragraph 1, letter b) - f), of the Regulation, consent is not required when:

- processing is necessary for the execution of a contract of which the party concerned is a party or for the execution of pre-contractual measures adopted at the request of the same;
- processing is necessary to fulfil a legal obligation to which the data controller is subject;
- processing is necessary for the safeguard of the vital interests of the party concerned or of another individual;
- processing is necessary for the performance of a task of public interest or related to the exercise of public powers of which the data controller is vested;
- processing is necessary for the pursuit of the legitimate interest of the data controller or of third parties, provided that the interests or rights and fundamental freedoms of the party concerned do not prevail, which require the protection of personal data, in particular if the party concerned is a minor.

D. Access to personal data and other rights of the party concerned

Group Companies guarantee to each individual whose personal data is processed the free exercise of the rights provided for by articles 15-22 of the Regulation.

In particular, the party concerned has the right to:

- obtain confirmation of whether or not personal data processing is in progress and, if so, obtain access thereto;
- oppose specific processing of personal data for legitimate reasons in order to make it cease definitively;
- withdraw consent at any time, without prejudice to the lawfulness of processing based on consent before revocation;
- obtain from the data controller the correction of inaccurate personal data, without unjustified delay and the integration of incomplete personal data, also by means of a specific supplementary declaration;
- request that data be processed solely for the purpose of storage, with the exclusion of any other processing operation;
- obtain the cancellation of personal data when the conditions apply.

E. Transfer of personal data

Group Companies undertake to adopt the necessary measures to ensure that the transfers of personal data comply with the applicable legislation even if by third parties acting as sub-contractors.

In accordance with the principle of free circulation of personal data, the Regulation regulates the transfer of data between the Member States of the European Union or the European Economic Area (Norway, Iceland, Liechtenstein).

For the transfer of data to a country not belonging to the EU/EEA, instead, one or more of the following conditions must apply:

- The system of the country of destination or transit of data ensures a level of protection of persons deemed "adequate" by the European Commission
- contractual instruments have been adopted that offer adequate guarantees (*Standard contractual clauses*, *Binding corporate rules*, etc.);
- the party concerned has explicitly expressed consent to the proposed transfer (in writing, in case of sensitive data), after being informed of the possible risks of such transfers for the party concerned, due to the lack of an adequacy decision and adequate guarantees;
- the transfer is necessary for the execution of a contract concluded between the party concerned and the data controller or the execution of pre-contractual measures adopted at the request of the party concerned;
- the transfer is necessary for the conclusion or execution of a contract stipulated between the data controller and another individual or legal entity in favour of the party concerned;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary to ascertain, exercise or defend a right in court;
- the transfer is necessary to protect the vital interests of the party concerned or of other persons, if the party concerned is physically or legally incapable of providing consent.

F. Data integrity

Pursuant to art. 5 of the Regulation, Grimaldi Group Companies carry out the processing of personal data by adapting their work to the following general criteria:

- all processing must take place in a lawful, transparent and correct manner;
- the data processed must be collected and recorded for specific, explicit and legitimate purposes, and used in other processing operations in terms not incompatible with said purposes;
- the data processed must be accurate and, if necessary, updated;
- the data processed must be adequate, relevant and limited to as necessary with respect to the purposes for which it is processed;
- the data processed must be stored in a form that allows identification of parties concerned for a period of time not exceeding the achievement of the purposes for which it is processed;

- the data must be processed in such a way as to guarantee adequate security of personal data, including protection, through appropriate technical and organizational measures, from unauthorized or unlawful processing and accidental loss, destruction or damage ("*integrity and confidentiality*").

G. ***Data security***

Grimaldi Group Companies undertake to adopt, to the extent possible, the necessary and adequate security measures to ensure that personal data and information is protected from loss, misuse, unauthorized access, disclosure, alteration or destruction as well as the reasonable checks to ensure that said measures are constantly updated.

Pursuant to the provisions of articles 24 and 32 of the Regulation, all Grimaldi Group Companies have implemented a security program that requires the adoption of measures in line with the following principles:

- ensure that personal data is processed by default required for each specific processing purpose (*Security and Privacy by Default*);
- effectively implement the principles of data protection and integrate the necessary guarantees in processing from the design in order to protect the rights of parties concerned (*Security and Privacy by Design*);
- ensure, in case of violation of personal data, communication to the parties concerned and the Privacy Guarantor in the manner and timing of the Regulation;
- carry out, for processing that presents high risks for the rights and freedom of parties concerned, the impact assessment in the ways and times provided for by the Regulation;
- ensure adequate specialist training on IT security issues;
- adopt techniques of anonymization or encryption of personal data when necessary.

Providing the foregoing, and in addition to the above, Group Companies undertake to process personal data only if the following safeguards are implemented:

- ***IT authentication systems***

Group Companies adopt authentication credentials that consist of a code for identifying the user (UserID) associated with a reserved key word known only by the same (password).

Each user is individually assigned and associated with one or more credentials for authentication.

- ***Secrecy and custody of authentication credentials***

Group Companies invite users to keep their authentication credentials with maximum confidentiality and not to share them with other users. All users are responsible for the correct and lawful use of the authentication credentials assigned.

- ***Passwords***

Group companies use passwords composed of at least 8 characters, and in any case, not less than the one required, from time to time, by law and with characteristics that make any attempt to identify them difficult.

The password is changed every 90 days, i.e. with a lower periodic frequency (i.e. 30 days), depending on the type of data processed (i.e. particular data: sensitive, judicial, etc.), in order to reduce the risk that unauthorized or malicious users are able to identify it.

Users must change their password on first access and can change it subsequently. The 5 passwords used previously cannot be reused.

Passwords must not contain the user's account name or references easily referable to the same user and must contain characters from at least three of the following four categories:

- Capital letters of the Latin alphabet (from A to Z);
- Lower case letters of the Latin alphabet (from a to z);
- Numbers based on 10 (from 0 to 9);
- Non-alphanumeric characters, such as exclamation point (!), Dollar ($), pound sign (#), or percentage (%).

- ***Disabling authentication credentials***

Group Companies ensure that authentication credentials are deactivated if they are not used for a period of at least 3 months. Credentials are also deactivated if the owner no longer needs to use them due to a change in their job duties or interruption of the employment relationship.

- ***Suspension of work sessions***

Group Companies oblige users to block their computers when they leave their work place even for limited periods of time. However, blocking is automatic after a set period of inactivity.

- ***Firewalling and antivirus software***

The information system of Group Companies is protected against unauthorized access from public communications networks.

All computers are equipped with up-to-date anti-virus software to limit the risk of intrusion of virus and malicious programs.

- ***Updating computer programs***

Group Companies periodically provide for the installation of updates (patches) to solve the problems identified in compliance with the indications and policies in use.

- ***Backup and recovery of data***

Group Companies implement actions able to guarantee the availability of information in line with the provisions of the law, as well as periodic checks of the effective readability and integrity of the information saved.

- ***Electronic tools for protection against unauthorized access***

The IT network used by Group companies is protected by specific tools such as firewalls, intrusion prevention and detection systems, which can reduce the risk of unauthorized access.

- ***Removable support***

Group Companies adopt specific protocols for safe custody, deletion and destruction of both removable media used for saving or transferring personal data and computers, both fixed and portable, disused or no longer used.

- ***Control and custody of deeds and documents***

Group Companies provide indications, in coordination with the Data Managers of the individual Departments, so that paper deeds and documents are checked and retained by users during all processing operations.

In any case, all personnel of Group Companies are always responsible for the use and custody of deeds and documents. At the end of processing operations, paper deeds and documents must be filed in locked cabinets/drawers. Where possible, similar measures must be taken in the event that the user temporarily moves away from the workstation.

- ***Control and custody of deeds and documents containing particular data (i.e. sensitive or judicial)***

Group Companies provide indications, in coordination with the Data Managers of the individual Departments, so that paper deeds and documents containing sensitive and judicial data are used exclusively by personnel expressly appointed to process them. Said personnel is responsible for the use and custody of the deeds and documents containing these categories of specific data; in particular, they must ensure that other unauthorized personnel does not have access to information that falls outside the related scope of processing. At the end of processing operations, paper deeds and documents must be filed in locked cabinets.

- ***Control of access to archives containing particular data (i.e. sensitive or judicial)***

Only those authorized to do so may access the archives for the performance of their job duties. At the end of the working day and after the office closing time, the archives may be accessed with identification, also by means of electronic tools (ex. badges).

- ***Control of access to the offices of Group companies***

Only employees/collaborators or authorized external personnel are allowed to access the offices of Group Companies.

Access to the offices by employees is only possible through electronic identification means (ex. badges), or through identification by security personnel, or by the reception staff.

- ***Control of access to Data Centers***

Only users authorized by the EDP Department, or by the Management of Group Companies, can access the Data Centers where there electronic processing tools.

- ***Video surveillance systems***

Video surveillance systems, aimed at strengthening the physical security of the offices of Group companies, are implemented in accordance with the provisions of the Guarantor and in coordination with the General Secretariat Department regarding aspects of worker protection (see article 4 Law 300 of 1970).

H. Data retention

Group companies adopt measures to store personal information only for the time necessary for the purposes for which it was collected and in any case not exceeding as required by law.

Retention times will be regulated by suitable operating procedures and communicated to parties concerned by specific policies and according to the indications contained in the Provisions of the Guarantor or indicated by the legislation in force.

I. Control and compliance

Group companies establish procedures to monitor compliance with the principles set out in the Regulation.

It is the responsibility of all personnel of Group Companies to know, understand and respect this Policy and its contents.

Non-compliance could result in significant risks for Group companies, and may subordinate each individual to disciplinary actions, up to and including dismissal or termination of the professional relationship.

In this sense, Group companies periodically carry out checks to verify their own information system through personnel involved, based on the level of control implemented.

Group companies also ensure the collection of any reports of non-conformities emerged both during analysis and/or development of new products, and during ordinary management, addressing them to the Data Managers of the various Departments and monitoring the effective resolution.

J. Contact data

Questions or doubts regarding the interpretation or methods of application of this Policy may be addressed by writing to the Data Protection Officer, ***Mr. Nicola Principe***, at the following email address: ***DPO@grimaldi.napoli.it***.

3. RIGHTS OF THE PARTY CONCERNED

The Regulation recognizes to the party to which the data processed refers (for example, customer, shareholder, employee, etc.) certain rights aimed at ensuring an adequate and direct control on compliance by Group Companies with the limits and conditions of personal data processing.

Group Companies undertake to guarantee the effective execution of the processes necessary for the exercise of the rights of parties concerned (ex. customers, suppliers, personnel, etc.).

The following paragraphs outline the guidelines and the type of requests that each party concerned has the right to exercise with particular reference to:

- Right of access to data by the party concerned
- Right of reply
- Right of cancellation
- Right of limitation of processing
- Right to data portability
- Right of opposition

3.1 Exercise of the rights of the party concerned and feedback times

The party concerned has the right to exercise related rights according to the procedures and within the limits set by the Regulation. Group Companies undertake to provide the party concerned with information relating to the action taken regarding a request without unjustified delay and, in any case, at the latest **within 30 days** from receipt of the request. This term may be extended by two months if necessary, taking into account the complexity and the number of requests. Furthermore, Group Companies will undertake to inform the party concerned of such extension, and of the reasons for the delay, within one month of receiving the request. If the request of the party concerned is presented by electronic means, the information will be provided, where possible, by electronic means, unless otherwise indicated by the party concerned.

These rights may be exercised by sending an e-mail to **privacy@grimaldi.napoli.it** or through written communication, specifying the subject of the request, to the attention of the ***Data Protection Officer*** (hereinafter "**DPO**"), **Mr. Nicola Principe**, domiciled for the office at the company's headquarters located in Via Marchese Campodisola, 13, 80133 Naples NA.

Upon receipt of the request, the General Secretariat, or the DPO if the request is addressed to the same, cannot refuse to fulfil the request of the party concerned, unless Group Companies demonstrate that they are unable to identify the party concerned. If the party concerned is identifiable, the General Secretariat or the DPO must send by e-mail or, if received in paper form, deliver it directly to the reference Data Managers within two days of receiving it.

In particular, based on the content of the request and the type of party concerned making the request, they are addressed to:

- Passenger Department for passenger requests;
- Corporate Short Sea Shipping Commercial Department for Cargo requests;

- Purchasing Department for requests from Third Parties/Suppliers;
- Human Resources Department for requests from HQ employees and Applicants;
- Crew Department for requests from Seafarers and Applicants.

The individual Data Managers will notify receipt of the request through communication via e-mail or by written communication to the General Secretariat or the DPO within one day of receipt of the request. The Data Manager with the support of the DPO will have to assess whether the requests will be manifestly unfounded and/or require an economic effort not proportional to the request, in particular due to their repetitive nature. In this case, Group Companies will be able to evaluate the possibility of:

- charging the administrative costs incurred to provide the information or communication or take the action requested to the party concerned;
- refusing to process the request by informing and justifying the decision to the party concerned.

Within 7 days, the Data Manager will notify Group Companies of the assessment of the validity/groundlessness of the request. If the request is deemed unfounded and therefore the request of the party concerned is not fulfilled, Group Companies inform the party concerned without delay, and at the latest within one month from receipt of the request, of the reasons for non-fulfilment, of the possibility of proposing a complaint to a control authority and filing a judicial appeal. If the request is considered founded, for execution, the individual Data Managers, with the support of authorized processors, will take over the same with respect to their area of competence and the operating procedure adopted by each department. These procedures provide for the full responsibility of each individual Data Manager during all the phases of handling requests, both if the data is filed in paper format and if the activities necessary for the exercise of the rights of individual parties concerned envisage technical actions on the Company's IT systems. In this last case, the individual Data Managers will eventually be supported by the Software Projects Design and Management Department for requests from parties concerned in the Cargo area and by the EDP department for all other types. If the Data Manager needs regulatory and/or legal support, it is possible to consult the DPO.
Group Companies undertake to make available to each individual Data Manager a register of requests with the dual purpose of tracing the management of certain requests, respecting the principle of accountability, and of harmonizing the process among all departments in order to avoid potential errors/duplications of requests received by the Controller.

Within 7 days from the result of the assessment of the request, the activities necessary for execution of the request must be completed. In particular, the Data Manager will send communication to Group Companies with annexed documentation or evidence of the actions performed to execute the request. The latter, supported by the DPO or the General Secretariat, will communicate the results to the party concerned within 7 days.

3.2 Right of access to data by the party concerned

The party concerned has the right to obtain from Group Companies confirmation that processing of related personal data is in progress and, in this case, to obtain access to personal data and the following information:

- processing purposes;
- categories of personal data in question;
- recipients or categories of recipients to whom the personal data has been or will be communicated, in particular if recipients of third countries or international organizations;

- whenever possible, the retention period of the personal data provided or, if not possible, the criteria used to determine this period;
- existence of the right of the party concerned to ask Group Companies to rectify or delete personal data or limit the processing of related personal data or to oppose processing;
- right to file a complaint with a control authority;
- if the data is not collected from the party concerned, all information available on the origin.

If personal data is transferred to a third country or to an international organization, the party concerned has the right to be informed of the existence of adequate guarantees.

Group Companies provide a copy of the personal data processed. In the event of further copies requested by the party concerned, Group Companies may charge a reasonable expense contribution based on administrative costs. If the party concerned submits the request by electronic means, and unless otherwise indicated by the party concerned, information is provided in a commonly used electronic format.

3.3 Right of reply

The party concerned has the right to obtain from Group Companies the correction of inaccurate related personal data without undue delay. Taking into account the purposes of processing, the party concerned has the right to obtain the integration of incomplete personal data, also by providing an additional declaration.

3.4 Right of cancellation

The party concerned has the right to obtain from Group Companies the deletion of related personal data without undue delay and Group Companies are obliged to cancel personal data without undue delay, if one of the following reasons exists:

- the personal data is no longer necessary with respect to the purposes for which it was collected or otherwise processed;
- the party concerned revokes consent on which the processing is based and if there is no other legal basis for processing;
- the party concerned opposes processing and there is no prevalent legitimate reason to proceed with processing;
- the personal data has been processed unlawfully;
- the personal data must be deleted in order to fulfil a legal obligation provided for by the law of the Union or of the Member State to which Group Companies are subject;
- the personal data has been collected with regard to the provision of information society services

The above information does not apply to the extent in which processing is necessary:

- for the exercise of the right to freedom of expression and information;
- for the fulfilment of a legal obligation that requires processing provided for by the law of the Union or the Member State to which Group Companies are subject or for the performance of a task performed in the public interest or in the exercise of public powers of which Group Companies are vested;
- for purposes of archiving in the public interest, scientific or historical research or statistical purposes to the extent that there is a risk of making impossible or seriously affecting the achievement of the objectives of such processing;

- for the assessment, exercise or defence of a right in court.

3.5 Right of limitation of processing

The party concerned has the right to obtain from Group Companies the limitation of processing when one of the following hypotheses occurs:

- the party concerned disputes the accuracy of personal data for the period necessary for Group Companies to verify the accuracy of such personal data;
- the processing is illegal and the party concerned opposes the deletion of personal data and instead requests that use be limited;
- although Group Companies no longer need it for processing, the personal data is necessary for the party concerned to ascertain, exercise or defend a right in court;
- the party concerned opposes processing pending verification of the eventual prevalence of the legitimate reasons of Group Companies with respect to those of the party concerned.

If the processing is limited, such personal data is processed, except for storage, only with the consent of the party concerned or for the ascertainment, exercise or defence of a right in court or to protect the rights of another individual or legal entity or for reasons of significant public interest of the Union or of a Member State.

The party concerned that obtained limitation of processing is informed by Group Companies before said limitation is revoked.

3.6 Right to data portability

The party concerned has the right to receive related personal data provided to Group Companies in a structured, commonly used and readable format by automatic device and has the right to transmit such data to another Data Controller without impediments by the Data Controller to which it was provided if:

a) processing is based on consent on a contract;
b) processing is carried out by automated means.

In exercising the rights with regard to data portability, the party concerned has the right to obtain direct sending of personal data from one controller to another, if technically feasible.

This right does not apply to processing necessary for the performance of a task of public interest or related to the exercise of public powers of which Group companies are vested.

3.7 Right of opposition

The party concerned has the right to oppose at any time, for reasons related to the particular situation, to the processing of related personal data, including profiling on the basis of these provisions. Group Companies refrain from further processing personal data unless it is demonstrated that there are binding legitimate reasons for proceeding with processing that prevail over the interests, rights and freedoms of the party concerned or for the ascertainment, exercise or defence of a right in court. If personal data is processed for direct marketing purposes, the party concerned has the right to oppose at any time to the processing of related personal data for such purposes, including profiling insofar as it is related to such

direct marketing. If the party concerned opposes processing for direct marketing purposes, the personal data is no longer processed for these purposes.

If personal data is processed for scientific or historical research purposes or for statistical purposes, for reasons related to the particular situation, the party concerned has the right to oppose processing of related personal data, unless processing is necessary for the performance of a task of public interest.