Subject: **Data Subject Rights Policy**	Department: **Dana Europe**		Approved by: **Executive Leadership Team**
	Responsible Officer: **Chief Compliance Officer**	Date of Last Revision/Reivew **May 2018**	

1. **OBJECTIVES OF THE POLICY**

This standard operating policy ("**SOP**") shall regulate:

- the process of receiving, analysing and fulfilling requests from employees and other workers, including temporary or agency employees, contractors and interns ("**Data Subjects**") concerning their rights set forth by Regulation EU 679/2016 ("**GDPR**") and its implementing acts (together with the GDPR, "**Data Protection Laws**"); and

- modalities to fulfil such requests from Data Subjects promptly and correctly on the basis of the GDPR.

2. **SCOPE OF APPLICATION**

The modalities and procedures set forth in the present SOP shall apply to all Dana entities located in the European Union.

Data Protection Laws provide that the exercise of Data Subjects rights shall be facilitated by the entity controlling the relevant personal data (the "**Controller**"). The management of Data Subjects' requests and related processing activities shall be carried out in compliance with applicable laws, as well as the principles of necessity, proportionality, and lawfulness of the processing.

Under the scope of this SOP, "**Personal Data**" means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

By way of example, the definition of "personal data" includes the name and/or surname of an individual (e.g. an employee or an applicant not part of the company yet), an email address (e.g. name.surname@company.com), or a code allowing his/her identification (e.g. access control badge number).

3. **MODALITIES TO MANAGE DATA SUBJECTS REQUESTS**

3.1 For the purposes of this SOP, each entity of Dana should have a single point of contact ("**SPOC**") for collecting and managing Data Subjects' requests. The SPOC shall be an internal employee duly granted with powers in relation to the management of privacy issues, such as the data protection officer, where appointed, or a human resources professional. The SPOC shall be able to identify the processing activities and shall handle the contacts to external and internal data processors to the extent it is necessary to manage Data Subject requests.

The contact details of the SPOC shall be made available in privacy notices provided to Data Subjects or made available to them in the company intranet or in other suitable ways commonly used to inform Data Subjects such as blackboards, internal newsletters, etc.

3.2 For the purposes of this SOP, the categories of Data Subjects shall be limited to employees or other workers (including, without limitation, temporary or agency workers, contractors, interns, etc.).

3.3 The SPOC shall be provided with adequate means to receive Data Subject requests, such as a dedicated email address where necessary. However, since the GDPR allows Data Subjects to submit their requests freely, **the SPOC shall also process requests arriving from different channels, including oral requests**.

3.4 Upon receiving a request, the SPOC shall authenticate the requests. If there are doubts concerning the identity of the requestor, the SPOC shall identify the requestor and, if necessary, request additional information which shall be communicated by means of secure channels to avoid the likelihood of data breaches. Documents and information collected for the purpose of identifying the Data Subjects shall not be retained for a period of time longer than the purpose for which they have been collected, unless they may be necessary for the defence or enforcement of any rights in a judiciary proceeding.

3.5 Data Subjects shall receive an acknowledgment of the receipt of the request **within 7 days from the receipt**.

3.6 The SPOC shall assess the legitimacy of the requests, and the amount of information which shall be communicated. For such purposes, the SPOC shall take into account:

(a) Restrictions to Data Subjects requests, which are set forth by the GDPR (see below); and

(b) Restrictions to Data Subjects requests set forth by local law (see below).

When doubts arise concerning the lawfulness of requests, the SPOC shall escalate the request to the legal department.

3.7 The requests shall be satisfied **within 1 month after receipt, which can be extended to up to 3 months**, taking into account the complexity and number of other requests.

3.8 In case of denial or delay in the response, the SPOC shall inform the Data Subject no later than one month from the receipt of the request, providing reasons for the delay/denial and informing the Data Subject of the possibility to lodge a complaint to the competent supervisory authority.

3.9 Requested information shall be provided either in written form or by electronic means. When the request has been presented by electronic means, information shall be provided electronically where possible, unless otherwise requested by the Data Subject. Any response requires that the identity of the Data Subject has been sufficiently established.

3.10 Responses to Data Subjects requests shall be **free of charge**. However when requests are manifestly unfounded or excessive (including repetitive requests), requests might be:

(a) charged with a reasonable fee, limited to administrative costs necessary to provide information; or

(b) refused.

When such circumstances arise, the SPOC shall consult the legal department. The assessment process and the reasons for the refusal of the request or the decision to charge costs shall be documented, as the relevant Dana entity acting as the Controller bears the burden of the proof.

3.11 All requests, regardless of their outcome, shall be documented and stored in a central and secured repository accessible only by the SPOC and/or the legal department, and shall be kept for no longer than 10 years, unless otherwise required to defend or enforce a right in a judiciary proceeding. The repository shall include

(a) Date of the request;

(b) Name of the requester;

(c) Type of request;

(d) Status of the request;

(e) Date of request closure; and

(f) Comments.

Appropriate technical and organizational measures shall be implemented to prevent unauthorized access to the repository.

4. DATA SUBJECTS RIGHTS

4.1 **Access Right**: Data Subjects shall have the right to access their Personal Data and exercise such right easily and within reasonable periods of time in order to be aware of the processing of their Personal Data and assessing its lawfulness. Such right applies to all Data Subjects who, first, have the right to obtain confirmation as to whether or not their Personal Data are being processed. If Personal Data are being processed, Data Subjects shall have the right to obtain a copy of their Personal Data and be provided with the following information:

(a) Purposes of the processing;

(b) Categories of Personal Data concerned;

(c) Recipients or categories of recipients (including service providers and affiliates) of the relevant Personal Data, in particular recipients in third countries;

(d) Envisaged period for which the Personal Data will be stored, or, if not possible, the criteria used to determine that period;

(e) Existence of the right to request from the Controller rectification or erasure of Personal Data or restriction of processing of Personal Data concerning the Data Subject or to object to such processing;

(f) Where the Personal Data are not collected from the Data Subject, any available information as to their source;

(g) The existence of automated decision-making (if any), including profiling, which have a significant effect on the Data Subject and information concerning the logic involved and the envisaged consequences of such processing for the Data Subject; and

(h) The right to lodge a complaint to the competent authority.

Data Subject Restrictions: Adverse effects on rights and freedom of others. For instance, if the source of the Personal Data is a notification in a whistleblowing system, information about the source shall be redacted.

Actions: The SPOC shall provide the Data Subject with the information set forth above, and with a copy of the the personal data undergoing processing, free of charge and, if the request has been submitted in an electronic form, in a commonly used electronic format which can be a Microsoft Word or Excel file. Additional copies may be provided against a charge within the limits of administrative costs. Where a large quantity of data has been processed, the SPOC can request the Data Subject to specify the information or processing activities to which the request relates. Such request for clarification shall be included in the acknowledgement of receipt of the request from the Data Subject and, in any case, within the time frame set forth in points 3.7 and 3.8 above. When the SPOC believes that a restriction applies, it shall consult the legal department.

4.2 **Right to Rectification**: Data subjects shall have the right to obtain the rectification of inaccurate Personal Data without undue delay. Data Subjects shall have the right to have incomplete Personal Data completed, including by means of providing a supplementary statement.

Actions: Communicate the rectification to entities which have received the relevant Personal Data (including affiliates and service providers) and inform the Data Subject about those recipients if the Data Subject requests this.

4.3 **Right to Erasure**: Data Subjects shall have the right to request their Personal Data to be erased and no longer processed to the extent:

(a) They are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) The Data Subject withdraws consent on which the processing is based and there is no other legal ground for the processing (i.e. legitimate interest, legal obligation, or ability to perform a contractual obligation); the SPOC shall contact the legal department to assess whether other grounds for processing apply;

(c) The Data Subject objects to the processing and there is no overriding legitimate grounds for the processing.

(d) Personal Data have been unlawfully processed;

(e) Personal Data have to be erased for compliance with a legal obligation under applicable laws or collective bargaining agreements;

Restrictions: The right to erasure shall not apply when processing is necessary for:

(f) compliance with a legal obligation which requires the processing under the applicable law of the Controller; or

(g) establishment, exercise or defense of legal claims.

Actions: Contact the IT department to implement appropriate technical measures. Communicate the erasure to entities which have received the relevant Personal Data (including, affiliates and service providers) and inform the Data Subject about those

recipients if the Data Subject requests this. If the SPOC believes that a restriction applies, it shall consult the legal department.

4.4 **Right to Restrict Processing**: The Data Subject shall have the right to restrict the processing of Personal Data where one of the following applies:

(a) The accuracy of the Personal Data is contested by the Data Subject, during the period enabling the Controller to verify the accuracy of the Personal Data;

(b) The processing is unlawful and the Data Subject opposes the erasure of the Personal Data and requests the restriction of the processing;

(c) The relevant Personal Data are no longer needed for the purposes of the processing, but they are required by the Data Subject for the establishment, exercise or defence of legal claims; or

(d) The Data Subject has objected to the processing, pending the verification whether the legitimate grounds for the processing override those of the Data Subject.

Actions: Contact the IT department to implement technical modalities to move selected data to another processing system, or making the selected Personal Data unavailable to users, or temporarily remove such data from the relevant processes or label the selected data so they are no longer processed. In such circumstances Personal Data subject to the request may only be processed (a) upon consent of Data Subject; (b) for the purposes of establishing, asserting or defending a right or a legal claim in judiciary proceedings; or (c) to protect rights of another natural or legal person.

4.5 **Right to Data Portability**: The Data Subject shall have the right (i) to receive their Personal Data (including pseudonymized data, and data deriving from the Data Subject's activity, but excluding data inferred or elaborated by the Controller), which the Data Subject has provided, in a structured, commonly used and machine-readable format, and (ii) to transmit and/or – where technically feasible – have directly transmitted such data to another enterprise without hindrance, subject to the following requirements:

(a) Processing is based on consent or contract (including an employment agreement); and

(b) Processing is carried out by automated means (such as, by merely way of example, an HR portal to which the Data Subject have access).

Please note that the right to portability does not apply to processes that are based on data that is not collected from the Data Subject or that rely on a legal basis other than consent or contractual obligation. For instance, performance reports or disciplinary documents drafted by the Controller in respect of Data Subject's performance under legitimate interest are not subject to the right to portability. A case by case analysis is required. In case of doubts, the SPOC shall consult the legal department.

Restrictions: Adverse effects on rights and freedom of others (e.g. the communication of data to other enterprises would result in a processing of third party data without any legal grounds, in such case SPOC shall contact the IT department whether technical measures can be implemented to fulfill the request without affecting third parties).

Actions: Contact the IT department to support the provision of data in a structured, commonly used and machine-readable format and to assess the technical feasibility of

transmitting the data directly to another enterprise. When the SPOC believes that a restriction applies, it shall escalate to the legal department.

4.6 **Right to Object**: The Data Subjects shall have the right to object at any time to the processing of their Personal Data on grounds relating to their particular situation, when the processing is based on public interest or legitimate interests of the Controller.

With regard to the right of objection for processing relying on the legitimate interest of the Controller, the right should be explicitly brought to the attention of the Data Subject and presented clearly and separately from any other information, and can be exercised at any time and free of charge.

Restrictions: The right to object shall not apply when there are compelling legitimate interests of the Controller override the interests or the fundamental rights and freedoms of the Data Subject.

Actions: Contact the IT department to implement technical measures allowing the exercise of the right to object. When the SPOC believes that a restriction applies, it shall escalate to the legal department.

4.7 **Right not to be Subject to a Decision Based Solely on Automated Data Processing Activity**: Such right only applies when:

(a) Automated decision making does not involve human intervention or such intervention does not have any impact on the final decision; and

(b) The decision might have legal effects on or similarly significantly affect the Data Subject (such as in case of automated background checks that may entail decisions to hire or not to hire a Data Subject).

Such processing can be considered lawful when:

(a) It is based on the necessity to enter into or perform a contract;

(b) The Data Subject has explicitly consented to such processing; or

(c) The automated decision making process has been authorised by the European Union or national law.

When the circumstances above apply, the Data Subject shall always have the right to request human intervention or to express their point of view.

Actions: Consult the legal department to assess whether such rights apply.

5. RESTRICTION TO DATA SUBJECT REQUESTS UNDER NATIONAL LAW

National laws may now or in the future provide further restrictions of the listed rights of Data Subjects. Please consult with the legal department for further assessment in case of a request from a Data Subject.