Guideline for persons authorised to process personal data

DOCUMENT DETAILS:

Date of issue	22.02.2023	**Version**	2.0

I. INTRODUCTION

The purpose of this policy for persons authorised to process personal data is to set out the roles, obligations and instructions that the persons authorised by the company **Schweitzer Project S.p.A.**, as well as the other Schweitzer Group companies associated with it (hereinafter the "**Company**"), to process personal data must know and observe.

Unless otherwise stated, all terms used herein shall be understood in the sense of the definitions of the GDPR and/or the document "Definitions and Acronyms".

To begin with, it is necessary to define:

- Personal data means any information relating to an identified or identifiable living person;
- Importance of the processing of personal data:

  Processing of personal data means, among other things, collecting, recording, organising, storing, modifying, viewing, using, publishing, linking and erasing such data.

II. GUIDELINES FOR THE AUTHORISED PERSONS

The Company has the obligation, unchanged with the introduction of the GDPR, to provide written instructions to any authorised person whom it uses to process personal data and in respect of whom it has the role of controller or processor.

As will be explained in more detail below, each Authorised Individual will be given a "Personal Data Processor Appointment" to sign upon joining the Company. This contains specific instructions for the processing of personal data carried out on behalf of the Company, as a result of which the authorised person assumes a duty of confidentiality that lasts beyond the termination of the employment or cooperation relationship.

Special procedures are provided for so-called system administrators, for whom a separate power to process personal data in the capacity of system administrator is provided.

In addition, the company offers internal training courses with expert speakers in the field of data protection to sensitise authorised persons in this area.

Through the written instructions and internal training, the Company demonstrates that it has taken organisational measures to protect the personal data of the data subjects, whether they are the authorised persons or customers/suppliers of the Company.

In this regard, it is recalled that all authorised persons, in the capacity of *data subjects*, also have the right to request from the Company, at any time, access to their personal data, rectification or erasure of the data or to oppose the processing; they have the right to request the restriction of the processing in the cases provided for by art. 18 of the Regulation, as well as to receive the data concerning them in a structured, commonly used and machine-readable format in the cases provided for by art. 29 of the Regulation. Written requests may be addressed to the Company at the following address: legal@schweitzerproject.com . In any case, you have the right to lodge a complaint with the competent supervisory authority (data protection authority) in accordance with Art. 77 of the Regulation at any time if you consider that the processing of your personal data infringes the applicable regulations.

III. PROCEDURE

When a new Authorised Person joins, the Company shall adhere to the following procedure.

1. For employees of the company

At the recruitment stage, the authorised person receives the authorisation to process personal data directly from the HR department for signature; subsequently, the latter updates the list of authorised persons. The new addition is announced to the IT department via JIRA. For more details on the issue of credentials, please refer to the procedure for issuing credentials and authorised profiles.

2. For System Administrators

1.) The IT department assesses the candidate's suitability to take on the role of system administrator from a technical point of view.
2.) When the IT department and the HR department agree on the recruitment, the candidate is presented with the recruitment contract for signature and the team for which he/she is designated is informed of the new recruitment by also announcing the date on which he/she will start work.
3.) If the authority profile to be assigned is such that the classification of the appointee as a system administrator is justified, the relevant department shall set a meeting date so that the prospective system administrator receives appropriate and documented training on his/her duties and legal responsibilities.
4.) After the training, the HR department has the newly hired employee sign the authorisation to process personal data as a system administrator and retains a copy of it.
5.) The HR office receives the signed appointment, files it, and subsequently updates the directory of system administrators. This specially created directory contains the names and functions of the internal system administrators in the company of the person responsible.

B. PROCEDURE FOR UPDATING THE AUTHORISATION TO PROCESS PERSONAL DATA

In the event of a change in the duties of an authorised person resulting in the assignment of an authorisation profile that differs from the one already assigned, the person in charge of the department shall inform the IT department of the technical changes to be made, as well as the Human Resources department, which shall provide the data subject with the initially signed authorisation to process personal data in duplicate for signature, notifying the change in the authorisation profile; it shall also update the list of authorised persons. For more details on the modification of the authorisation profile, please refer to the procedure for issuing credentials and profiles.

If the change of the authorisation profile results in the authorised person assuming the role of a system administrator, the process described above in section A.2 applies.

C. PROCEDURE IN THE EVENT OF THE DEPARTURE OF THE PERSON AUTHORISED TO PROCESS AND THE SYSTEM ADMINISTRATOR

In the event of termination of the employment/co-operation relationship of the authorised person or the system administrator with the responsible person, the Human Resources Department shall, after taking note of the database and the internal and external applications to which the departing person has access, send a notification to:

- all employees of the human resources (HR) department;
- the IT department;

so that they close the internal accesses of the person leaving.

IV. SYSTEM ADMINISTRATOR

A. DEFINING THE ROLE OF THE SYSTEM ADMINISTRATOR

In anticipation of receiving any updates from the supervisory authority on the figure of the system administrator in line with the new requirements of the GDPR, the Company continues to review its activities against the Data Protection Code (Legislative Decree 196/03) and the orders of the supervisory authority.

For the purposes of the *"Provvedimento dell'Autorità di Controllo per la protezione dei dati personali Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008*" (Ital. Official Gazette no. 300 of 24 December 2008; amendment based on the Order of 25 June 2009 - hereinafter: "**Order**") is preceded by the following:

a) In computer science, "system administrator" is generally understood to mean job descriptions whose purpose is the administration and maintenance of a processing system or its components. However, for the purposes of the decree, other job profiles are also taken into account which can be equated with these from the point of view of risks in terms of data protection, such as administrators of databases, administrators of networks and security devices, as well as administrators of complex software systems.

b) In the absence of common definitions of the rules and techniques, the system administrator has been adopted within the framework of the order of the supervisory authority as a job description dedicated to the management and maintenance of processing facilities in which processing of personal data takes place, including the management systems for databases, as well as complex software systems such as the ERP systems, local area networks and security devices, to the extent that they allow intervention on the personal data.

The supervisory authority did not intend to equate "**system operators**" under the articles of the Penal Code relating to IT offences with "**system administrators**": the latter are special system operators endowed with specific privileges. The reference to D.P.R. 318/1999 is also purely descriptive, as the job description defined in that (now abolished) legal act has a narrower scope than the one referred to in the order. The definition does not cover those persons who only occasionally carry out interventions on the elaboration and software systems (e.g. for maintenance purposes after failures or breakdowns).

Currently, the following job profiles are considered system administrators that meet the following criteria:

a) they can change the access privileges to the data of the authorised persons as specified in the order (where the preliminary remarks read: [...] *tasks* [...] *are typically the responsibility of the system administrator: from making security copies (backup and recovery of data) to the custody of the credentials to the management of the authentication and authorisation systems);*

b) they can change the access levels of the system;

c) they can change the configuration of the system, for example by changing the accesses from external networks or by cancelling an authentication system (injunction - preliminary remarks: The *system administrators [...] in their*

usual activities are in many cases concretely "responsible" for specific phases of work that can lead to high criticalities for data protection);

d) they manage the company's policies for backup and backup utilities (transport/exchange/storage).

On the other hand, persons who only occasionally intervene in the elaboration and software systems (e.g. for maintenance purposes after failures or breakdowns) are not considered as system administrators. They must be professionals responsible for the management and maintenance of the processing systems where personal data are processed, including database management systems, as well as complex software systems such as ERP systems, local area networks and security devices, to the extent that they allow intervention on personal data.

B. ANNUAL REVIEW OF THE SYSTEM ADMINISTRATOR'S ACTIVITIES

Point 4.4 of the Order ("**Review of the activity**") requires that the activity of the system administrator be reviewed at least once a year by the controllers or processors to ensure that in doing so he or she is complying with the organisational, technical and security measures in relation to the processing of personal data provided for by the applicable regulations.

The company draws up the following checklist:

1. Regular controls

1.1. Evaluation of the subjective characteristics

The assignment of the functions of a system administrator shall be made after prior assessment of the characteristics in terms of experience, ability and reliability of the designated person, who shall provide an appropriate guarantee that the applicable processing rules are fully complied with, including the security profile.

Even if the functions of system administrator or equivalent are only assigned as part of an appointment to the authorised person, the controller and processor must in any case adhere to assessment criteria that correspond to those required for the appointment of the processor under the GDPR.

1.2. Individual Appointment

The appointment of the system administrator shall be individual and shall include an analytical list of the scope of activities he/she is allowed to perform based on the assigned authority profile.

1.3. Directory of the system administrators

The identification data of the natural persons acting as system administrators, together with the list of functions assigned to them, must be listed in an internal document which must always be up to date and available if the supervisory authority has to carry out investigations.

If the activity of the system administrators also indirectly concerns services or systems that process or allow the processing of employees' personal information, the public and private controllers are obliged to make the identity of the system administrators known or identifiable within their organisation, depending on the characteristics of the company or service and in relation to the different computer services for which they are responsible. For this purpose, they shall use the privacy statement given to the data subjects as part of the employment/co-operation relationship that binds them to the data controller or, alternatively, they shall use the technical specification provided for by Order No. 13 of the Control Authority of 1 March 2007 (published in Italian Official Gazette No. 58

of 10 March 2007) or, alternatively, the internal communication tools (e.g. the company intranet, service instructions issued internally or bulletins) or formalised procedures at the request of the employee. Without prejudice to cases where these forms of publicity or recognisability are incompatible with other requirements of the regulations governing a specific sector.

1.4. Outsourced services

If the system administration services are outsourced, the controller or the external processor must directly and specifically keep the identification data of the physical persons acting as system administrators in case of need.

2. Technical controls

2.1. Checking the correspondence between assigned duties and privileges, at least once a year.

2.2. Spot check, once a year, whether the logs record the activities performed by the system administrators.

2.3. Verification, once a year, that the logs are kept correctly and that the attached digital signature is correct.