

Information on Data Processing for job applicants

INFORMATION PURSUANT TO ART. 13 EU REGULATION 2016/679 "GENERAL REGULATION ON DATA PROTECTION"

This information is provided in compliance with the legislation on the protection of individuals in relation to the processing of personal data, referred to in EU Regulation 679/2016 (hereinafter referred to as "Regulation or GDPR"), connected exclusively with the online platform "Recruiting" for the management of applications.

1. DATA CONTROLLER

The Data Controller of the personal data of candidates who fill out the forms to send their data and their curricula is Autostrade per l'Italia S.p.A., Via A. Bergamini, 50, 00159, Rome; the Data Protection Officer (DPO) can be contacted at the e-mail address dpo@pec.autostrade.it.

2. TYPE OF DATA PROCESSED

The data that can be collected and processed for the purposes detailed below are only those indicated in the forms on this web page as well as those covered by the curriculum vitae ("CV"), uploaded by the Data Subject using the "upload" function.

These data include: "common data" and, where necessary, data belonging to particular categories, pursuant to art. 9 of the GDPR, relating to the registration in the employment lists pursuant to Law 68/99 and/or the certification of the Specific Learning Disorder (SLD), as well as the photographic image in the CV.

The data can be collected directly from the Data Subject.

The Data Controller may not use the platform to process data not deemed strictly necessary for the purposes set out below.

3. PURPOSE OF THE PROCESSING AND LEGAL BASIS

All personal data are processed in compliance with the legal provisions for purposes related exclusively to the selection of staff for recruitment purposes, in the interest of the Data Controller.

The data and information provided spontaneously by the Data Subject in the curriculum are treated in accordance with art. 111-bis of Legislative Decree 196/2003 and subsequent amendments (Privacy Code) and, for special data (art. 9 of the GDPR) relating to registration in the placement lists, pursuant to Law 68/99.

Without prejudice to the freedom for Data Subjects to provide personal data, please note that failure to communicate the data will prevent the Data Controller from considering the application of the Data Subject as part of any staff selection and recruitment procedure, except for the photographic image, the non-provision of which may not prevent the processing from being carried out.

Failure to provide data falling within the particular categories pursuant to art. 9 of the GDPR, referred to in point 2 above, may hinder the selection and recruitment procedure only where the procedure is aimed at filling vacancies reserved for disabled workers pursuant to Law no. 68/99.

4. SPECIAL CATEGORIES OF PERSONAL DATA

Also in compliance with the principle of minimisation, candidates are kindly requested not to enter redundant and/or unnecessary data and information in relation to the purposes of the staff selection and recruitment. Candidates are therefore requested not to indicate personal data belonging to particular categories (relating in particular to health, religious belief and political opinions) other than those possibly provided for in the purpose of the selection (registration in the employment lists pursuant to Law 68/99 o SLD certification data); in this circumstance, the Data Controller shall refrain from using this information.

5. DATA PROCESSING METHODS AND SECURITY MEASURES

Processing methods

Personal data shall be processed through the operations described in art. 4 no. 2) of the GDPR, and more precisely: collection, registration, organisation, storage, consultation, processing, correction, selection, extraction, comparison, use, interconnection, blocking, communication, cancellation, and destruction of data.

Personal data are subjected to electronic processing.

The data will not be subject to fully automated processing as specified in art. 22 of the GDPR.

Security measures

Specific security measures shall be complied with to prevent data loss, unlawful or improper use and unauthorised access. Specifically, this data is encrypted using a security technology called Transport Layer Security (TLS) for data flow and Advanced Encryption Standard (AES) for data stored on servers. TLS technology encrypts information before it is exchanged over the Internet, making it incomprehensible to unauthorised persons and thus ensuring the confidentiality of the information transmitted.

6. PERSONAL DATA RETENTION PERIOD

Data shall be retained for a period consistent with the purposes indicated, in compliance with the principle of minimisation. Specifically, the data shall be retained for no more than two years from the last activity carried out by the Data Subject, or from the last access to the application by the Data Subject.

7. CATEGORIES OF DATA RECIPIENTS

Within Autostrade per l'Italia S.p.A., only the persons tasked with the processing by the Data Controller and authorised to perform the processing operations within the scope of the aforementioned activities may acquire the personal data provided.

Data may be disclosed to third parties (parent companies/subsidiaries involved or third-party companies), required to process the information for the purposes related to the selection and recruitment, referred to in point 3 above, or IT service providers, which allow the operation and maintenance of the platform, required to process the data for the aforementioned purposes, which are, to this end, appointed as "Data Processors" pursuant to art. 28 of the GDPR.

Autostrade per l'Italia S.p.A. may disclose personal data to the ASPI Group Companies based within the European Union, which will process them, as independent Data Controllers, in the event that the data are disclosed for the same selection and recruitment purposes of its staff, ensuring their confidentiality and security.

The complete list of persons appointed as Data Processors is available from the DPO. Under no circumstances will personal data be disseminated.

8. TRANSFER OF DATA OUTSIDE THE EUROPEAN UNION

Data are managed and stored on servers of third-party companies appointed as Data Processors.

The servers used to store the above data are located in Italy and within the European Union. Personal data may not be transferred outside the European Union.

However, where data are transferred to non-EU countries, even if only to move the location of the archives and servers, the Data Controller shall still reassure Data Subjects of the existence of a motivated decision by the European Commission; as an alternative, specific data protection clauses shall be agreed with any third-party recipients. In any case, Data will be processed in the interest of the Candidate.

9. RIGHTS OF DATA SUBJECTS

Pursuant to the Regulations, Data Subjects have the right to access their data, especially to obtain confirmation of their existence/non-existence at any time and to access their content, know about origin, geographical location, as well as to request a copy.

Moreover, Data Subjects have the right to verify their accuracy or request their integration, updating, correction, restriction of processing, cancellation, anonymisation or to request interruption of data processing when such procedure breaches the law, as well as to oppose their processing. Where the Data Subject exercises the right to object to the processing, the Data Controller reserves the right not to process the request, and thus to continue processing, if there are compelling legitimate grounds for processing that prevail over the interests, rights and freedoms of the Data Subject.

Furthermore, Data Subjects have the right to request data portability.

10. EXERCISE OF DATA SUBJECTS' RIGHTS

To exercise the rights referred to in point 9), Data Subjects may contact, through a specific request without formalities, the Data Protection Officer (DPO - address indicated in point 1) of the Data Controller by filling in the specific Forms provided by the Data Controller on the website www.autostrade.it

The deadline for replying to Data Subjects is thirty days, which can be extended for a further two months in complex cases; in these cases, the Data Controller shall provide Data Subjects with at least one interim communication within thirty days.

Data Subjects may lodge a complaint with the Data Protection Authority, which can be contacted at the website <http://www.garanteprivacy.it/>