

Privacy police compliance

The Italian Legislative Decree no. 196 of 30 June 2003 – **Personal data protection** – has streamlined existing Italian legislation on privacy and personal data protection. It replaces the Italian Law no. 675 of 31/12/1996, the D.P.R. 318/99 and other legal provisions.

Main features of the new law

- Privacy is an individual human right. Fundamental human freedoms include the right to privacy, personal identity and the protection of personal data.
- The new law shifts the burden of proof in the treatment of personal and sensitive data away from the individual and onto the person actually processing the data.
- The new law increases the penalties under the civil and criminal codes for failure to comply.

Personal rights

Candidates have the **right to know**:

- The origin of the data.
- The purposes for which the data is held (mandatory notice, name of data processing manager).
- The methods used to process the data.
- The persons or category of persons to which the data can be communicated.
- The period of time for which personal data will be held.

Candidates have the **right to request**:

- Updating, anonymizing and correction of data.
- Deletion or blocking of data.

Principles of processing personal data

The principle of **data legality and correctness**:

- Personal data may be collected in an honest and legal manner.
- **Purposefulness** – personal data must be pertinent, complete, exact and updated and only collected and processed for the purposes specified.
- Personal data may only be stored for a period of time which does not exceed the time necessary for the purposes for which it was collected and processed.

Processing of **sensitive data**:

- Only the data strictly necessary to establish a hiring agreement may be processed.
- The viewing of personal data is limited to specified persons within the company.

Security measures

Personal data processing using IT or manual methods:

- The following minimum security measures are obligatory: IT authentication; protection against illegal processing; established procedures for data archiving.
- Infringements can result in criminal proceedings. Adopting the most complete set of security measures can limit liability to the civil proceedings.

Documentation

- Security programme document (list of personal data processed; distribution of processing tasks; risk analyses; measures designed to guarantee data integrity).
- Conformity document certifying the conformity of software with the new legal requirements and describing all the measures implemented.
- description of personal data protection activities must now be included in the annual balance sheet reports.



CVweb Privacy

CVweb Privacy is a module supplied with the CVweb suite of programs, designed by the R&D department at Cesop Communication. The module has a wide range of easy-to-use functions designed to ensure that CVweb users comply with the latest legislation on personal data protection during the recruitment and selection process.

The **CVweb Privacy** module makes CVweb the first software system to fully comply with personal data protection legislation.

CVweb Privacy is supplied complete with:

- A declaration of conformity certifying that the software meets all legal requirements.
- A regular system check-up service.
- A manual describing the procedures to be implemented to guarantee conformity with the new legislation.

CVweb Privacy - the main functions:

MANDATORY NOTIFICATION AND SENDING CVs/RESUMES

Candidates wanting to send in their CVs/resumes link up to the Careers section of the company internet site and open the CV/resume data entry form.

The CV/resume entry form contains the new mandatory notification concerning the processing of personal data. The notification includes:

- The references of the new personal data protection law.
- Reference to Law no.125/91 regarding sexual discrimination during the recruitment and selection process.
- The purposes for which the CV/resume is being collected.
- The name of the person processing the data.
- The name of a contact person.
- The email address and/or telephone number to which all enquiries regarding personal data are to be sent.

Before they can send their CVs/resumes, candidates must select the Authorize check box to indicate that they have read the mandatory notice and authorize the processing of their personal data for the purposes indicated.

CVs/resumes which are mailed or emailed to the company can also be entered in CVweb by keying-in, downloading attachments or scanning documents. The system will also automatically produce an email containing the entire text of the mandatory notification present on the web site.

SENSITIVE PERSONAL DATA

The Send CV/resume form is fully customizable. It can be configured to contain only the information strictly necessary for the selection process and only the sensitive data relevant to a particular employment opportunity.

Candidates are not asked for data about their sexual orientation, religion or political preferences.

The mandatory notification on personal data protection includes a warning advising candidates not to provide sensitive data which has not otherwise been requested in the notes and attachments.

Where sensitive personal data is requested by a company, the CV/Resume window has a special section for this type of data; this data can only be viewed by users with the necessary legal authorisation.

UPDATING OR CORRECTING DATA

When a candidate sends in a CV/resume, the system automatically replies with an email confirming that the data has been received. The confirmation email also includes the unique user name and password assigned to the candidate intended for use by the candidate when making modifications at a later date.

Candidates wishing to update or correct their data can do this themselves. They simply have to enter their user name and personal password, access their CV/resume and make the changes. Alternatively, candidates can communicate their change requests to the person responsible for data processing who then uses the Search and Modify functions of CVweb to make the changes specified.

In both cases the changes take immediate effect and within the times specified by the law.



AUTHENTICATION RULES

Corporate users and candidates sending in their CVs/resumes are subject to the authentication and security rules stipulated by law.

With CVweb you can set the following parameters:

- Empty passwords disregarded
- Number of characters per password (min. 8 characters)
- Password expiry date (max. 3 months)
- User account expiry date (max. 6 months)
- Log of main operations performed by users
- Disabling of simultaneous multiple access by the same user
- Session timeout.

To enhance the level of system security it is also possible set up a secure HTTPS connection or an IP address with restricted access.

ADMINISTRATOR FUNCTIONS

The application has the following administrator functions:

- Real time updating of mandatory notification
- Modification of data manager/processor name
- Management of user list and related user identification of users with rights to view CVs/resumes
- Management of system maintenance categories
- Management of user group permissions and segmentation of viewing rights by user group.

INFORMATION LINKED TO CVs/RESUMES

The following functions are designed to enable candidates to receive immediate answers to queries regarding their personal data:

- Search functions used to find a candidate and his/her related data in the archive in a few seconds
- Access List showing all the company users who have viewed a CV/Resume
- and the date and time of viewing
- Candidate Tracking
- with details of all the events linked to a candidate in the selection process
- Curriculum Links, this function is used to view the job postings chosen by the candidate, the tests completed and the related correspondence.

ACTIONS ON CVs/RESUMES

The following functions are designed to simplify complicated manual operations and to ensure that they are performed correctly without errors. The functions are:

- Block CV. The CV is not displayed and cannot be used. Only special users are authorised to release the block following a request from the candidate concerned.
- Anonymize CV. The CV is not deleted but all the personal identification data are automatically replaced with the hyphen ("-") character.
- Delete CV. The CV is deleted from the database.



OPERATOR STATISTICS

The module has an innovative operator console used to control the following privacy settings:

- Corporate data protection manager
- Password protection levels
- Auto-respond email
- Number of CVs sent for a specific job posting and for which no reply has been received
- Periodic deletion of obsolete CVs.

ARCHIVING OF PERSONAL DATA

The mandatory notification indicates the standard period of time for which personal data are stored in an archive; this is usually one or two years.

In order to delete a CV after the period indicated it is possible to manually renew a CV according to dynamic settings or to program a function which automatically renews the archive at preset intervals.

The procedure takes into account how up to date a CV is and how much interest has been shown in it. It takes into account any updates and contacts made after the CV was entered in the archive.

In order to further safeguard company interests during the data archiving period, a special section in the mandatory notification advises candidates that the CV may be considered for posts other than those specified by the candidate.

The mandatory notification also indicates the names of persons other than those specified originally who may also be permitted access to the CV/resume for the purposes and with the methods specified originally. This name could, for example be other companies inside the same group.