REGISTRATION REQUIREMENTS

Does HR data processing require registration under data protection laws?

Data protection laws sometimes include conformity assessments, which help to ensure businesses follow regulations. Requirements can include registration before the Data Protection Authority and random audits. The General Data Protection Regulation (GDPR), which became effective on May 25, 2018, has helped make the requirements within the European Economic Area more uniform. That said, each Data Protection Authority remains independent and can create their own conformity assessments.

The GDPR is oriented on "privacy by design" and "privacy by default." Controllers (employers) and Processors (subcontractors) must implement all technical and organizational measures necessary to ensure the protection of personal data. In practical terms, the processing of personal data in every instance should be accompanied with the privacy concern in order to limit the amount of data processed from the outset (so-called "minimization" principle). HR teams should think carefully before collecting any new piece of data. Two key considerations are the reasons for collecting the data and the potential consequences (risks) of maintaining and processing this data.

The consequence of this accountability principle is the reduction of required employee notifications, once controllers and processors conclude that processing the personal data does not constitute a risk to privacy. Prior to the GDPR going into effect, processing personal data was subject to authorization from the competent data protection authority. Going forward, the new procedure involves privacy impact assessments.

The GDPR has a few new compliance requirements to demonstrate accountability, such as:

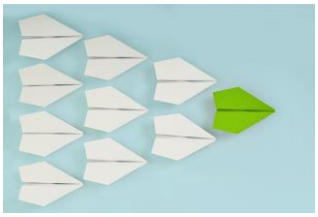
- maintaining a register of treatments implemented
- the notification of security breaches (to the authorities and persons concerned)
- certifications
- adherence to codes of conduct
- the DPO (Data Protection Officer)

- Privacy Impact Assessments (PIAs)

Authorization Requirements in Italy

In Italy, Legislative Decree no. 101/2018, incorporated the new GDPR requirements. Decisions/authorizations previously issued by the Italian Data Protection Authority (DPA) along with existing ethical codes are remaining in-place until they are officially updated by the DPA. Authorization No. 1/2014 concerning the Processing of Sensitive Data in the Employment Context (published in Italy's Official Journal No. 301 of 30 December 2014) allows the processing of "sensitive" data in the employment context without any previous request for authorization. Note that under the Data Protection Code, sensitive personal data outside of the context of employment generally could only be processed with authorization from the Italian DPA.

That said, processing biometric data continues to be strictly controlled under the DPA's regulations. Currently, processing biometric data must be done after filing an application with the DPA to permit the processing. Note that in 2014 the DPA permitted the processing of biometric data without an application in certain circumstances, such as when simplifying access to certain areas via finger/handprints.



HR Best Practices:

Build in privacy considerations and risk assessments for all employee and candidate data collection processes. Follow the principles of "privacy by design" and "privacy by default."

Last updated April 2021.