Employee Data Privacy – Serbia

Employee Access Rights

Do individuals have the right to access their personal information?

Data protective jurisdictions tend to guarantee the right of individuals to contact an organization directly and find out whether personal data is being tracked. Access procedures and acceptable exceptions (such as business secrecy) are determined by law and may be subject to the control of data protection authorities. In the context of HR, personal data access requests can include information tracked by the company as well as data tracked by third-party solutions, such as background check vendors.

Serbia's Data Protection Law gives employees and other data subjects the right to:

- access their personal data;
- have their personal data corrected when inaccurate;
- erasure, if: (a) personal data is no longer necessary for the original purpose of the data collection, (b) consent is withdrawn, (c) the employee objects to the processing, (d) the data was unlawfully processed, (e) the data must be erased to execute legal obligations or, (f) the personal data was collected relating to the offer of information society services;
- restrict processing when: (a) the employee contests the accuracy of the processing; (b) the data was processed unlawfully; (c) the data is no longer needed for the employer's original purpose, but the data is still required for the establishment/exercise/defense of legal claims; or, (d) the employee objects to the processing pending the verification of whether the employer's grounds for processing override those of the employee;
- portability (i.e. the employee can receive their personal data in a commonly used, machine-readable format and has the right to transmit the data to another controller);
- object to their personal information being processed if: (a) the data is being used for direct marketing or, (b) the legal basis for processing personal data is the execution of duties in the public interest, the employer's (controller's) authorizations prescribed by law or the performance of legitimate interests of the employer/processor/third-party;

- not be subject to automated processing, including profiling which can significantly impact the individual or produces legal effects concerning the individual.

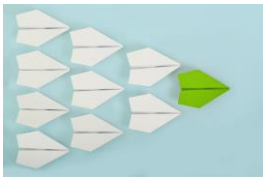
Employee Requests

When an employee, job applicant or other data subject exercises their rights by submitting a request to the employer, the employer must respond within 30 days. This can be extended by 60 days when necessary, depending on the complexity and number of requests.

Employers can refuse employee requests and rights in certain situations. When an employee's rights as a data subject are refused, the reason for the refusal must respect the employee's fundamental rights and freedoms and be necessary and proportionate to safeguard things such as: national or public security; the prevention/investigation/detection/prosecution of breaches of ethics for regulated professions; the protection of the employee or the rights and freedoms of others; the enforcement of civil law claims, etc.

When determining how to respond to an employee or other data subject's request, consider the:

- purposes of processing;
- categories of personal data;
- scope of any restrictions;
- safeguards to protect the data from abuse or unlawful access or unlawful transfer;
- specification of the employer or categories of controllers;
- the storage period and applicable safeguards, considering the nature, scope and purpose of the personal data processing;
- risks to the rights and freedoms of the individuals;
- right the data subjects have to be informed about any restriction, unless that could be prejudicial to the purpose of the restriction.



HR Best Practices:

When processing an access request from an employee, make sure not to disclose information connected to other employees. Employers should establish official procedures and contacts for employee requests.

Last updated August 2022.