Portugal - Employment

March 26, 2025

Ricardo Henriques

Abreu Advogados

Compare with other jurisdictions

March 2025

1. Laws

1.1. Laws and regulations

1.1.1. What laws and/or regulations apply to data protection in the employment context?

- Law no. 7/2009, of February 12th, as updated (only available in Portuguese here) (the Labor Code);
- The General Data Protection Regulation2016/679 (GDPR);
- Law No. 58/2019 of 8 August 2018 (only available to download in Portuguese here) (the GDPR Implementation Law)

Citation

Not applicable.

1.2. Supervisory authority

1.2.1. Who is responsible for enforcing the law(s) and issuing guidelines?

The Portuguese data protection authority (CNPD) is the National Competent Administrative Authority.

Courts and similar conflict resolution institutions may also enforce data protection statutes.

Citation

Not applicable.

1.3. Guidelines

1.3.1. Have any guidelines been released on data protection in the employment context?

- Deliberation 494/2019, in which the CNPD decided not to apply a set of rules of the GDPR Implementation Law, grounded in the fact that the CNPD considers such rules to be an infringement of the GDPR (only available to download in Portuguese here) (Deliberation 494/2019)
- Deliberation 7680/2014 on principles applicable to processing of personal data arising from the use of geolocation in the employment context (only available in Portuguese here) (Deliberation 7680/2014)
- Deliberation 1638/2013 on principles applicable to processing of personal data arising from the use of communication technologies for private purposes in the employment context (only available in Portuguese here) (Deliberation 1638/2013)
- Deliberation 890/2010 on principles applicable to processing of personal data for preventive medicine, alcohol and drug control made to employees (only available in Portuguese here) (Deliberation 890/2010)
- Deliberation 840/2010 on principles applicable to processing of personal data within the management of information of the Safety and Health at Work services (only available in Portuguese here) (Deliberation 765/2009)
- Deliberation 765/2009 on the Principles applicable to processing of personal data for whistleblowing purposes - Ethic Lines (only available in Portuguese here) (Deliberation 765/2009)
- Deliberation 61/2004 on the processing of data via video surveillance (only available in Portuguese here) (Deliberation 61/2004)
- Guidelines on the processing of biometric data for entrance and attendance control (2004) (only available in Portuguese here)
- Guidelines on the Collection of employees' health data (temperature control and questionnaire in the context of COVID-19 (Coronavirus)) (Guidelines on the collection of employees' health data) (only available in Portuguese here)
- Guidelines on the dissemination of information of persons infected with COVID-19 (only available in Portuguese here)
- Teleworking remote control (in the context of Coronavirus) (only available in Portuguese here) (Teleworking remote control guide)

In addition to the above, the guidelines issued by the European Data Protection Board (EDPB) may also be used by the legal and judicial operators when dealing with privacy matters.

Citation

Deliberation 494/2019

Deliberation 7680/2014

Deliberation 1638/2013

Deliberation 890/2010

Deliberation 840/2010

Deliberation 765/2009

Deliberation 61/2004

Guidelines on the processing of biometric data

Guidelines on the collection of employees' health data

Guidelines on the dissemination of information of persons infected with COVID-19 Teleworking remote control guide

2. Recruitment and selection

2.1. Hiring documents

2.1.1. Is it permissible to collect hiring documents?

It is permissible to collect hiring documents (CV, cover letter, interview notes, evaluations, references, and right-to-work documentation) within the limits identified below.

Citation

Articles 5, 6, and 9 of the GDPR;

Article 28 of the GDPR Implementation Law;

Articles 17 and 32 of the Labor Code

2.1.2. Are there any restrictions on collecting hiring documents?

The following restrictions apply to the collection of hiring documents:

- Article 5 of the GDPR:
    - lawfulness, fairness, and transparency;
    - purpose limitation;
    - accuracy;
    - storage limitation;
    - integrity and confidentiality; and
    - accountability.
- data subject information: data must only be collected in accordance with privacy notice sent/made available to data subjects
- source: hiring documents should be collected directly from the potential worker, recruitment services and/or publicly available databases.
- retention period: employers shall maintain recruitment process records for five years, with a breakdown by gender of the following elements:
    - invitations for the filling of job positions;
    - job offers;
    - number of applications for curricular assessment;

    - number of candidates present in pre-selection interviews;
    - number of candidates waiting for admission;
    - results of tests or admission or selection tests; and
    - social balance sheets for data to analyze the existence of possible discrimination against people of one sex in access to employment, vocational training and promotion, and working conditions; and
- personal life: employers cannot demand a job applicant to provide information related to their private life or to their health or pregnancy status, except if such information is strictly necessary and relevant to assess and check their suitability for the performance of the employment contract (e.g. duties and position) and provided that the employer justifies the need to collect and process such information in writing. these criteria (necessity and relevance) must be analyzed on a case-by-case basis, notably by linking the need to collect said information with the duties to be performed by candidates.

Citation

Articles 5, 6, and 9 of the GDPR

Articles 21 and 28 of the GDPR Implementation Law

Articles 17 and 32 of the Labor Code

2.1.3. Which lawful bases can be relied on for the processing of personal information contained in hiring documents?

- Performance of the contract when processing is necessary to enter into the contract at the request of candidate.
- Compliance with obligations of the controller, when processing is necessary for compliance with a legal obligation to which the controller (employer) is subject.
- Legitimate interests, when processing is necessary to pursue a legitimate interest of the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.
- The processing of an employee's personal data must not rely on their consent. In fact, except when otherwise provided by law, consent does not constitute a valid legal ground for employees' data processing, if the data processing results in a legal or economic advantage/benefit for the employee. The CNPD, however, has stated that is shall not apply this rule because it considers that it violates the rule of law of the EU and compromises the effectiveness of the GDPR.

Citation

Articles 6 (1) (b), (c) and (f) of the GDPR

Article 7(4) of the GDPR

Recital 43 of the GDPR

Article 28 of the GDPR Implementation Law

CNPD Deliberation 494/2019

2.1.4. Is it permissible to disclose/share such personal information with third parties?

In some circumstances, employers shall comply with certain reporting obligations (e.g., reporting refusal to concede part-time schedule) to works councils and/or other Authorities, which may lead to personal data processing activities.

Employers shall also comply with state authorities and arbitration courts *ad hoc* individual orders to disclose employees' data.

Such disclosure of candidate records is, however, subject to the general rules and principles for collection, processing, and disclosure of data. The same applies to state authorities. Overall, there shall be no disclosure/sharing unless explicitly required/permissible by law.

Citation

Articles 6(1)(c) and 9(2)(f) of the GDPR

Articles 57(5) and 552(1) of the Labor Code

2.1.5. Is notice required when collecting such data?

Yes. Whenever there is an operation of personal data collection, a privacy notice for that operation must be given/made available to the data subject. The provision of such information by means of a clause included in the employment contract of the concerned employees constitutes a best practice in Portugal.

Citation

Article 12 of the GDPR

2.1.6. What information must be provided with the notice?

The notice must contain the information referred to in Article 13 of the GDPR, as complemented by the information contained in Article 14 of the GDPR if the source of the data is not the data subject.

The notice must contain, specifically:

- the identity and the contact details of the controller/ representative;
- the contact details of the data protection officer;
- the purposes and legal basis for the processing (including, if applicable, the legitimate interests pursued by the controller or by a third party;
- the recipients of the personal data;
- information concerning the transfer of personal data to a third country, if applicable;
- the period (or the criteria to determine the period) for which the personal data will be stored;
- the existence of the right to access, rectify or have erased personal data, as well as to restrict/object processing and the right to data portability;
- the right to withdraw consent at any time, if applicable;

- the right to lodge a complaint with a supervisory authority;
- whether the provision of personal data is a statutory or contractual requirement, as well as possible consequences of failure to provide such data;
- the existence of automated decision-making and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Citation

Articles 13 and 14 of the GDPR

2.1.7. In what format must this information be provided?

The notice must be provided in an easily readable format that complies with the transparency principle.

Citation

Article 12 of the GDPR

2.1.8. When should notice be provided?

The notice must be provided prior to data collection or, at the latest, at the time of data collection. If not all the information on the notice can be provided before or at the time of data collection, the missing information should be made available to the data subjects as soon as possible and without undue delay and, in any case, always within one month counted from data collection.

Citation

Articles 12, 13, and 14 of the GDPR

2.2. Special category data

2.2.1. Is it permissible to collect special category data during recruitment?

It is permissible to collect sensitive data during recruitment within the limits identified below.

Citation

Article 9 (2) of the GDPR

Article 28 of the GDPR Implementation Law

Articles 17 and 18 of the Labor Code

2.2.2. Are there any restrictions on collecting special category data during recruitment?

Overall, the rules set forth in the GDPR with regard to the processing of special categories of personal data shall apply.

In particular, the following rules apply:

- background checks shall not be conducted to verify/ ascertain descent, age, sex, sexual orientation, gender identity, marital status, family status, economic situation, education, social origin or condition, genetic heritage, disability, chronic illness,

nationality, ethnic origin or race, territory of origin, language, religion, political or ideological beliefs, and union membership;

- criminal records and convictions data must only be processed in limited cases. Otherwise, it is not standard and should only be collected if and to the extent that the information can be justified in terms of the role offered (which would be very difficult to demonstrate if there is no legal obligation). Furthermore, even when collection is legally required, it must be directly adequate to assess the aptitude of the employee/candidate with regard to the execution of the employment contract. This is the case for the following sectors of activity:
- employment involving regular contact with minors;
- professional associations (such as doctors, lawyers, dentists, veterinarians, and acupuncturists, among other);
- public procurement;
- private security;
- professions related to goldsmithing and silversmithing;
- financial sector; and
- the practice of certain activities, such as hunting;
- employers may not require job applicants to provide information regarding their private life (including sensitive data), except when this is strictly necessary and relevant for assessing their respective aptitude with regard to the execution of the work contract and the respective justification is provided in writing. However, concerning employees' health or pregnancy, when particular requirements inherent to the nature of the professional activity so justify, data collection is permissible so long as the sensitive personal information, and the respective justification, is provided in writing. In the latter case, the information must be provided to an occupational doctor/ physician, who can only inform the employer if the employee is fit to perform the activity or not;
- biometric data shall not be collected during recruitment (as the Labor Code states that the processing of this category of sensitive data will only be considered legitimate for controlling attendance and for controlling access to the employer's premises);
- health data shall be processed under the conditions established in Article 9(2) of the GDPR, in particular the conditions foreseen in points (b) and (h) of that article. The GDPR Implementation Law subjects the processing of health data to a 'need-to-know' principle, additionally imposing a duty of secrecy on corporate bodies, employees/staff, service providers of the controller, the data protection officer (DPO), students, health and genetics researchers, and to all healthcare staff regarding health and genetic data. Employers cannot, for the purposes of admission to a job position, require job applicants or employees to undergo or present medical tests or examinations of any nature to prove their physical or mental conditions, except when the purpose of these is the protection and safety of the employee or of third parties, or when particular requirements inherent to the activity justify the provision of such data. Furthermore, occupational doctor/physicians can only communicate to the potential employer if the concerned candidate is or is not able to carry out the activity (and not the actual data

collected). Please also note that the employer is obliged to notify employees of any access to their personal data, which means that the employer will have to implement a traceability and notification mechanism;

- diversity data collection is unlikely to be deemed as being strictly necessary and relevant for the recruitment of the employee's role and, as such, unable to be collected and processed; and
- vaccination status is considered health-related personal data, which constitutes a special category of data, subject to a specially reinforced legal protection regime. Because doctors responsible for the medical tests and examinations may only inform the employer if the employee is or is not fit to perform the activity, through a broad interpretation, it will be possible to argue, through analogical reasoning, that the employer will not have the legitimacy to require the employee to show the employer their vaccination record, especially as regards non-compulsory vaccinations.

Citation

Articles 9 and 10 of the GDPR;

Article 28 of the GDPR Implementation Law

Articles 17, 18, 19 and 32 of the Labor Code

Law No. 12/91 of 21 May (only available in Portuguese here) (the Criminal Identification Law)

2.2.3. Which lawful bases can be relied on for the processing of special categories of data during recruitment?

In addition to relying on at least one of the three general lawful basis for the processing of candidates' data mentioned in section 2.1.3. (i.e., performance of the contract, compliance with obligations, and legitimate interests), the processing of candidates' sensitive personal data is lawful if:

- processing is necessary for the purposes of carrying out obligations and rights of the controller or of the data subject in the field of employment and social security and social protection law, insofar as it is authorized by EU or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject; or
- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of EU or Member State law, or pursuant to a contract with a health professional and subject to secrecy (special categories of personal data).

Citation

Articles 6 and 9 of the GDPR

2.2.4. Is it permissible to disclose/share such personal information with third parties?

Yes, when that possibility is statutorily provided for or ordered *ad hoc*. For more details, please refer to the answer in section 2.1.4.

Citation

Articles 6(1)(c) and 9(2)(f) Article 57(5) and 552(1) of the Labor Code

2.2.5. Is notice required when collecting such data?

Yes. Whenever there is an operation of personal data collection, a privacy notice for that operation must be given/made available to the data subject. The provision of such information by means of a clause included in the employment contract of the concerned employees constitutes a best practice in Portugal.

Citation

Article 12 of the GDPR

2.2.6. What information must be provided within the notice?

The notice must contain the information referred to in Article 13 of the GDPR, as complemented by the information contained in Article 14 of the GDPR if the source of the data is not the data subject.

The notice must contain, specifically:

- the identity and the contact details of the controller/ representative;
- the contact details of the data protection officer;
- the purposes and legal basis for the processing (including, if applicable, the legitimate interests pursued by the controller or by a third party;
- the recipients of the personal data;
- information concerning the transfer of personal data to a third country, if applicable;
- the period (or the criteria to determine the period) for which the personal data will be stored;
- the existence of the right to access, rectify or have erased personal data, as well as to restrict/object processing and the right to data portability;
- the right to withdraw consent at any time, if applicable;
- the right to lodge a complaint with a supervisory authority;
- whether the provision of personal data is a statutory or contractual requirement, as well as possible consequences of failure to provide such data;
- the existence of automated decision-making and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Citation

Articles 13 and 14 of the GDPR

2.2.7. In what format must this information be provided?

The notice must be provided in an easily readable format that complies with the transparency principle.

Citation

Article 12 of the GDPR

2.2.8. When should notice be provided?

The notice must be provided prior to data collection or, at the latest, at the time of data collection. If not all the information on the notice can be provided before or at the time of data collection, the missing information should be made available to the data subjects as soon as possible and without undue delay and, in any case, always within one month counted from data collection.

Citation

Article 13 and 14 of the GDPR

3. Employee records

3.1. Personnel records

3.1.1. Is it permissible to process personal information contained in personnel records?

It is permissible to process personal records (identification, right to work, bank details, address, contact information, and national identification numbers) within the limits identified below.

Citation

Articles 5, 6, and 9 of the GDPR

Article 28 of the GDPR Implementation Law

Article 17 of the Labor Code

3.1.2. Are there any restrictions on processing such data?

The processing of personal records of the employee is subject to the general restrictions mentioned in section 2.1.2., namely:

- the principles contained in Article 5 of the GDPR;
- the information provided to the data subjects;
- the source of the data;
- applicable retention periods;
- limitations regarding employees' personal lives.

Pursuant to the applicable legislation concerning general employment documents (e.g., personnel records, employment contracts), the maximum period an employer is likely to be able to justify retention is between one year post termination of employment for the purpose of defending court or tribunal claims, and five years corresponding to the statute of limitations of administrative offences for non-compliance with employment regulations.

Citation

Articles 5, 6, and 9 of the GDPR;

Articles 21 and 28 of the GDPR Implementation Law

Articles 17, 22, and 337 of the Labor Code;

Article 52 of Law No. 107/2009 (only available in Portuguese here)

3.1.3. Which lawful bases can be relied on for processing personal information contained in personnel records?

The lawful bases mentioned in section 2.1.3 are also applicable to the processing of employee activity records, namely:

- performance of the contract;
- compliance with obligations of the controller; and
- legitimate interests.

Again, the processing of an employee's personal data must not rely on their consent.

Citation

Articles 6(1)(b), 6(1)(c), and 6(1)(f) of the GDPR

Article 7(4) of the GDPR (with Recital 43)

Article 28 of the GDPR Implementation Law

CNPD Deliberation 494/2019

Article 127 of the Labor Code

3.1.4. Is it permissible to disclose/share such personal information with third parties?

Yes, when that possibility is statutorily provided for or ordered *ad hoc*. In some circumstances, employers shall comply with certain reporting obligations (e.g., reporting refusal to concede part-time schedule) to works councils and/or other Authorities, which may lead to personal data processing activities.

Employers shall also comply with state authorities and arbitration courts' *ad hoc* individual orders to disclose employees' data.

Such disclosure of employee records is, however, subject to the general rules and principles for collection, processing, and disclosure of data. The same applies to state authorities. Overall, there shall be no disclosure/sharing unless explicitly required/permissible by law.

Citation

Articles 6(1)(c) and 9(2)(f) of the GDPR

Articles 57(5) and 552(1) of Labor Code

3.2. Performance records

3.2.1. Is it permissible to process personal information contained in performance records?

It is permissible to process performance records (promotions, grievances, disciplinary records, bonuses, and performance management) within the limits identified below.

Citation

Articles 5, 6 and 9 of the GDPR

Article 28 of the GDPR Implementation Law

Article 17 of the Labor Code

3.2.2. Are there any restrictions on processing such data?

The processing of performance records of the employee is subject to the general restrictions mentioned in section 2.1.2., namely:

- the principles contained in Article 5 of the GDPR;
- the information provided to the data subjects;
- the source of the data;
- applicable retention periods; and
- limitations regarding employees' personal lives.

Additionally, kindly note that video systems or other technological means of remote surveillance can only be used in the context of criminal proceedings or for the purpose of ascertaining disciplinary responsibility insofar as they are within the scope of criminal proceedings. As such, the employer may not resort to means of distance surveillance to control the professional performance of the employee. The use of such technologies is only permissible to protect and safeguard persons and goods or when particular requirements inherent to the nature of the activity so justify. In such cases, the employer must inform the employee of the existence and purpose of the means of surveillance used, and must namely display in the places subject to it the following statements, as the case may be: 'This location is under closed circuit television surveillance' or 'This location is under closed circuit television surveillance, proceeding to image and sound recording,' followed by an identifying symbol. In cases where video surveillance is allowed, sound recording is prohibited.

Pursuant to the applicable legislation concerning general employment documents (e.g. performance records), the maximum period an employer is likely to be able to justify retention is between one year post termination of employment for the purpose of defending court or tribunal claims, and five years corresponding to the statute of limitations of administrative offences for non-compliance with employment regulations.

Citation

Articles 5, 6, and 9 of the GDPR

Articles 21 and 28 of the GDPR Implementation Law

Articles 17, 20 and 21 of the Labor Code

TRP Decision in case No. 6337/21.8T8VNG

3.2.3. Which lawful bases can be relied on for processing personal information contained in performance records?

The bases mentioned in section 2.1.3 are also applicable to the processing of employee activity records, namely:

- performance of the contract;
- compliance with obligations of the controller; and
- legitimate interests.

Again, the processing of an employee's personal data must not rely on their consent.

For more details, please refer to section 2.1.3.

Citation

Articles 6(1)(b), 6(1)(c) and 6(1)(f) of the GDPR

Article 7(4) of the GDPR

Recital 43 of the GDPR

Article 28 of the GDPR Implementation Law

CNPD Deliberation 494/2019

Article 332 of the Labor Code

3.2.4. Is it permissible to disclose/share such personal information with third parties?

Yes, when that possibility is statutorily provided for or ordered *ad hoc*. In some circumstances, employers shall comply with certain reporting obligations (e.g., reporting refusal to concede part-time schedule) to works councils and/or other Authorities, which may lead to personal data processing activities.

Employers shall also comply with state authorities and arbitration courts' *ad hoc* individual orders to disclose employees' data.

Such disclosure of employee records is, however, subject to the general rules and principles for collection, processing, and disclosure of data. The same applies to state authorities. Overall, there shall be no disclosure/sharing unless explicitly required/permissible by law.

Citation

Articles 6(1)(c) and 9(2)(f) of the GDPR

Article 552(1) of Labor Code

3.3. Activity records

3.3.1. Is it permissible to process personal information contained in activity records?

It is permissible to process performance records (promotions, grievances, disciplinary records, bonuses, and performance management) within the limits identified below.

Citation

Articles 5, 6 and 9 of the GDPR

Article 28 of the GDPR Implementation Law

Article 17 of the Labor Code

3.3.2. Are there any restrictions on processing such data?

The processing of activity records of the employee is subject to the general restrictions mentioned in section 2.1.2., namely:

- the principles contained in Article 5 of the GDPR;
- the information provided to the data subjects;
- the source of the data;
- applicable retention periods;
- limitations regarding employees' personal lives.

Pursuant to the applicable legislation concerning general employment documents (e.g. attendance and annual leave registry), the maximum period an employer is likely to be able to justify retention is between one year post termination of employment for the purpose of defending court or tribunal claims, and five years corresponding to the statute of limitations of administrative offences for non-compliance with employment regulations.

Citation

Articles 5, 6 and 9 of the GDPR

Article 21 and 28 of the GDPR Implementation Law

Articles 17, 131, 202, 221, 225, 231 of the Labor Code

3.3.3. Which lawful bases can be relied on for processing personal information contained in activity records?

The bases mentioned in section 2.1.3. also render the processing of employee activity records lawful, namely:

- performance of the contract;
- compliance with obligations of the controller; and
- legitimate interests.

Again, the processing of an employee's personal data must not rely on their consent.

Citation

Article 6(1)(b), 6(1)(c) and 6(1)(f) of the GDPR

Article 7(4) of the GDPR

Recital 43 of the GDPR

Article 28 of the GDPR Implementation Law

CNPD Deliberation 494/2019

Articles 17, 202, 221, 225, and 231 of the Labor Code

3.3.4. Is it permissible to disclose/share such personal information with third parties?

Yes, when that possibility is statutorily provided for, or ordered *ad hoc*. In some circumstances, employers shall comply with certain reporting obligations (e.g., reporting refusal to concede part-time schedule) to works councils and/or other Authorities, which may lead to personal data processing activities.

Employers shall also comply with state authorities and arbitration courts *ad hoc* individual orders to disclose employees' data.

Such disclosure of employee records is, however, subject to the general rules and principles for collection, processing, and disclosure of data. The same applies to state authorities. Overall, there shall be no disclosure/sharing unless explicitly required/permissible by law.

Citation

Articles 6(1)(c) and 9(2)(f) of the GDPR

Articles 57(5) and 552(1) of Labor Code

3.4. Sensitive records

3.4.1. Is it permissible to process personal information contained in special category records?

It is permissible to process personal data contained in sensitive records within the limits identified below.

Citation

Article 9(2) of the GDPR

Article 28 of the GDPR Implementation Law

Articles 17 and 18 of the Labor Code

3.4.2. Are there any restrictions on processing such data?

Overall, the rules set forth in the GDPR with regard to the processing of special categories of personal data shall apply.

Criminal Records Data

The processing of criminal convictions data is mandatory only in certain limited cases (e.g. security guards or drivers for children transportation). Otherwise it is not standard and should only be performed if and to the extent that the information can be justified in terms of the role offered (which would be very difficult to demonstrate if there is no legal obligation).

Diversity Data

The Labor Code only allows processing of data that is strictly necessary and relevant to the performance of an employee's role. In this context, the processing and storage, of employees' diversity data is unlikely to be deemed strictly necessary and relevant for the performance of the employee's role.

Medical Records: Employers cannot, where a contractual relationship has already been established, require employees to undergo or present medical tests or examinations of any nature to prove their physical or mental conditions, except when the purpose of these is the protection and safety of the employee or of third parties, or when particular requirements inherent to the activity justify the provision of such data. In addition, the doctor responsible for the medical tests and examinations may only inform the employer if the employee is or is not fit to perform the activity.

Please refer to section 2.2.2 for more on the collection and processing of employees' criminal, diversity, and medical records.

Citation

Articles 9 and 10 of the GDPR

Article 28 of the GDPR Implementation Law

Articles 17 and 32 of the Labor Code

Criminal Identification Law

3.4.3. Which lawful bases can be relied on for processing personal information contained in sensitive records?

In addition to relying on at least one of the three general lawful basis for the processing of candidates data mentioned in section 2.1.3 (i.e., performance of the contract, compliance with obligations, and legitimate interests), the processing of candidates sensitive personal data is lawful if it observes the limits mentioned in section 2.2.3. Kindly refer to sections 2.1.3 and 2.2.3 for more details on the lawful bases of processing sensitive personal data.

Citation

Articles 5, 6, and 9 of the GDPR

Articles 21 and 28 of the GDPR Implementation Law

Articles 17 and 32 of the Portuguese Labor Code

3.4.4. Is it permissible to disclose/share such personal information with third parties?

Yes, when that possibility is statutorily provided for, or ordered *ad hoc*. In some circumstances, employers shall comply with certain reporting obligations (e.g., reporting refusal to concede part-time schedule) to works councils and/or other Authorities, which may lead to personal data processing activities.

Employers shall also comply with state authorities and arbitration courts *ad hoc* individual orders to disclose employees' data.

Such disclosure of employee records is, however, subject to the general rules and principles for collection, processing, and disclosure of data. The same applies to state authorities. Overall, there shall be no disclosure/sharing unless explicitly required/permissible by law.

Citation

Articles 6(1)(c) and 9(2)(f) of the GDPR

Article 552(1) of Labor Code

3.5. Payroll and pension records

3.5.1. Is it permissible to process personal information contained in payroll and pension records?

It is permissible to process personal data contained in payroll and pension records within the limits identified below.

Citation

Article 6 of the GDPR

Article 28 of the GDPR Implementation Law

Article 17 of the Labor Code

3.5.2. Are there any restrictions on processing such data?

The processing of payroll and pension records of the employee is subject to the general restrictions mentioned in section 2.1.2, namely:

- the principles contained in Article 5 of the GDPR;
- the information provided to the data subjects;
- the source of the data;
- applicable retention periods; and
- limitations regarding employees' personal lives.

Pursuant to the applicable legislation concerning general employment documents (e.g., salary and benefits records), the maximum period an employer is likely to be able to justify retention is between one year post termination of employment for the purpose of defending court or tribunal claims, and five years corresponding to the statute of limitations of administrative offences for non-compliance with employment regulations. On the other hand, records related to payments made (e.g., tax related documents) must be kept for 10 years as of the end of the relevant fiscal year.

Citation

Articles 5, 6, and 9 of the GDPR

Articles 21 and 28 of the GDPR Implementation Law

Articles 17 and 337 of the Labor Code

Article 52 Law No. 107/2009

Article 52 Decree-Law No. 102/2008 (only available in Portuguese here)

3.5.3. Which lawful bases can be relied on for processing personal information contained in payroll and pension records?

Please refer to the answers in 3.3.3.

Citation

Article 6(1)(b), 6(1)(c) and 6(1)(f) of the GDPR

Article 7(4) of the GDPR

Recital 43 of the GDPR

Article 28 of the GDPR Implementation Law

CNPD Deliberation 494/2019

Articles 17, 131, 202, 221, 225, 231 of the Labor Code

3.5.4. Is it permissible to disclose/share such personal information with third parties?

Yes, when that possibility is statutorily provided for, or ordered *ad hoc*. In some circumstances, employers shall comply with certain reporting obligations (e.g., reporting refusal to concede part-time schedule) to works councils and/or other Authorities, which may lead to personal data processing activities.

Employers shall also comply with state authorities and arbitration courts' *ad hoc* individual orders to disclose employees' data.

Such disclosure of employee records is, however, subject to the general rules and principles for collection, processing, and disclosure of data. The same applies to state authorities. Overall, there shall be no disclosure/sharing unless explicitly required/permissible by law.

Citation

Article 6(1)(c) of the GDPR

Article 552(1) of Labor Code

4. Data subject rights

4.1. Access requests

4.1.1. Are there any specific rules for handling employee access requests?

Employees who have provided information of a personal nature shall have the right to control their personal data, being able to take note of its content and the purposes for which it is intended, as well as require its correction and updating.

All information required by the employee in the possession of the employer must be made available to them in an easily machine or manual-readable format.

Citation

Article 15 of the GDPR

4.1.2. Are there any limitations to providing employees access to their personal information?

Employees' right to access their personal information should not harm the protection of third-party data (e.g., other employees).

Citation

Article 15(4) of the GDPR

CNPD Deliberation 61/2004

4.2. Privacy policies

4.2.1. Is there a requirement to provide employees with a privacy policy?

Yes. Employees must be provided with a Privacy Policy.

Citation

Article 12 of the GDPR

4.2.2. What information must be provided to employees regarding the processing of their personal information?

All the information mentioned in section 2.1.6 above.

Citation

Articles 13 and 14 of the GDPR

4.2.3. When must this information be provided?

Before data collection or, if impossible then without undue delay. For more details, please refer to section 2.1.8 above.

Citation

Articles 13 and 14 of the GDPR

4.2.4. In what format must this information be provided?

Easily readable format. Please refer to section 2.1.7 above.

Citation

Article 12 of the GDPR

5. Use of AI and automated decision-making

5.1. Recruitment

5.1.1. Are there requirements regarding the use of automated decision-making and/or AI during recruitment?

Yes. Kindly refer to section 5.1.2. below.

Citation

Articles 13, 14, 15s and 22 of the GDPR

Articles 9-15 of the EU Artificial Intelligence Act (AI Act)

5.1.2. What are the requirements regarding the use of automated decision-making and/or AI during recruitment?

Using automated decision-making systems in the context of recruitment requires employers to inform candidates of the existence and necessity of automated decision-making and provide

meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Additionally, the employer shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view, and to contest the decision.

Kindly note that unless the use of automated decision-making systems is necessary, has been authorized by the law of the Member-State or is based on the candidate's explicit consent, the candidate shall be allowed to refuse being subjected to an automated decision.

Using AI systems in the context of recruitment, in turn, likely constitutes a high-risk AI use case according to the recent EU AI Act, meaning that such AI system must have been designed, implemented, and certified according to the rules laid down in that Act. In this case, the requirements mentioned in reference to the use of automated decision-making systems shall also apply.

Citation

Articles 13, 14, 15, and 22 of the GDPR

Articles 9- 15 of the EU AI Act

5.2. Employee performance

5.2.1. Are there requirements regarding the use of automated decision-making and/or AI to evaluate employee performance?

Yes. Kindly refer to the answers below.

Citation

Articles 13, 14, 15, and 22 of the GDPR

Articles 9-15 of the EU AI Act

5.2.2. What are the requirements regarding the use of automated decision-making and/or AI to evaluate employee performance?

The requirements for the use of automated decision-making systems and/or AI systems in the context of assessment/evaluation of employees' performances are the same as for their use in the context of recruitment. Where that advice reads 'candidate' it should be replaced with 'employee.' For more details, please refer to answer 5.1.2.

Citation

Articles 13, 14, 15, and 22 of the GDPR

Articles 9-15 of the EU AI Act

6. Teleworking

6.1. Policy, procedures, and guidance

6.1.1. Are there any specific requirements for employers with employees that work remotely?

Yes. Kindly refer to section 6.1.2. below.

Citation

Article 165 to 171 of the Labor Code

Teleworking remote control guide

6.1.2. What are the requirements for employers with employees that work remotely?

The Labor Code states that the employer must respect the employee's privacy, their working hours, and the rest of their family, as well as provide them with good working conditions, both from a physical and psychological point of view. Thus, whenever telework is performed at the employee's home, visits to the workplace require prior notice of 24 hours and the agreement of the employee, and this visit must only have the purpose of controlling the work activity, as well as the work instruments, and can only be made in the presence of the employee during the agreed working hours. Furthermore, it is forbidden to capture and use images, sound, writing, or history, or to use other means of control that may affect the worker's right to privacy.

CNPD's Guidelines on Teleworking furthermore prohibit the use of these technological solutions for remote control of employee performance. Examples of this are software that, in addition to tracking work and inactivity time, records the internet pages visited, the location of the terminal in real time, the use of peripheral devices (mice and keyboards), etc.

A different situation is the one regulating the need to record working time, which can be done by using specific technological solutions in this regime of telework. Such solutions must be designed in accordance with the principles of Privacy by Design and by Default, not collecting more information than necessary for the pursuit of that purpose. Similarly, the employer is in no way prevented from monitoring the employee's availability and compliance with working hours by means of telephone or electronic contact.

Citation

Articles 165-171 of the Labor Code

Teleworking remote control guide

7. Training and awareness

7.1. Employee training

7.1.1. Are there any requirements for training employees on data protection compliance?

Yes. Kindly refer to section 7.1.2. below.

Citation

Article 39 of the GDPR

Article 11 the GDPR Implementation Law

7.1.2. What should employee training programs encompass?

Employee training programs should ensure that all employees have a comprehensive understanding of the GDPR. In particular, controllers who are employers should provide onboarding training on data protection and the GDPR to all employees.

The employer should also organize regular training sessions to ensure that all employees have a solid knowledge of data protection laws, and are aware of the company's data protection policy.

The content of the training sessions should vary, taking into account the departments or job positions of the employees.

For example, the marketing department should benefit from a training session that focuses more on the legal grounds for processing related to direct marketing practices and cookies.

However, all employees should be aware of the definition of a personal data breach and how to report it internally to the company's data protection officer (DPO).

Citation

Article 39 of the GDPR

Article 11 the GDPR Implementation Law

8. Enforcement

8.1. Liability

8.1.1. What are the penalties for violation of the applicable laws?

Non-compliance with GDPR rules may result in an application of fines up to €20 million or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Data subjects may also claim compensation for damages caused by an unlawful data processing activity in civil proceedings.

The GDPR Implementation Law provides for additional administrative offences to those provided for in the GDPR. However, the CNPD has decided that it will not apply some of these in future cases, due to the fact that it has considered that they violate Articles 83(4) and 83(5) of the GDPR.

The GDPR Implementation Law also establishes the possibility that the CNPD may waive the application of fines for a period of three years as from the entry into force of the same, upon a reasonable request made by public entities addressed to the CNPD.

Finally, the GDPR Implementation Law specifies several crimes with regard to personal data, such as:

- the use of data incompatible with the purpose of the collection;
- improper access;
- data diversion;
- data corruption or destruction;
- insertion of false data;
- breach of the duty of confidentiality; and
- failure to comply with obligations under the GDPR or the GDPR Implementation Law.

Citation

Articles 83 and 84 of the GDPR

Articles 37-54 of the GDPR Implementation Law

8.2. Enforcement decisions

8.2.1. Has the supervisory authority issued any enforcement decisions on data protection and employment?

Deliberation 2021/1566 (only available in Portuguese here): On May 7, 2018, a complaint against the Agency for Administrative Modernization, I.P (AMA) was filed with the CNPD. In this participation, it was reported that the AMA employees, assigned to the Citizens' Space of the Braga Citizen's Shop, in order to assign a Mobile Digital Key (CMD) to citizens, in the back-office, would have to authenticate themselves with their citizen's card (CC) or with their own personal CMD. Following the normal procedures, the CNPD issued a Project of Deliberation under which it ordered the AMA to provide an alternative means of authentication of its employees that complied with the requirements of the GDPR. The CNPD believes that the employer cannot require employees to use their personal identification documents as a professional tool on a daily basis. At the end of the process, the CNPD determined that the AMA should, within six months, make available an alternative means for the certification of employees when such means is necessary for the exercise of functions by employees.

Citation

Deliberation 2021/1566

8.3. Case law

8.3.1.

Are there any relevant decisions on data protection and employment from judicial courts?

- On November 28, 2022, Relation Court of Porto (which is Porto''s appeals court) ruled regarding the usage of employee video recordings for disciplinary and right-cause through its ruling in case No. 6337/21.8T8VNG (only available in Portuguese here) (TRP Decision in case No. 6337/21.8T8VNG). In general terms, and according to the GDPR Implementation Law, images that result from video surveillance in labor relations can only be used as proof in a criminal proceeding (Article 28(4) of the GDPR Implementation Law). Article 28(5) of the GDPR Implementation Law adds that those same images can also be used for labor disciplinary purposes, as long as there is a criminal proceeding pending for the same facts. Naturally, this provision greatly limited the possibility of using video footage for termination purposes, since the employer would always need to proceed criminally or the crime to be prosecuted (which may involve costs and takes time) in order to be able to use such footage for said disciplinary purposes. On the contrary, the court's ruling attempts to interpret the GDPR Implementation Law in a more liberal manner and as such states that 'video surveillance methods can be utilized as means of proof for labor disciplinary purposes if the control of the employee's performance is not at stake and the facts may be criminally relevant, regardless of the existence of a criminal proceeding.'
- In September 2023, the Portuguese Supreme Court of Justice (the Court) issued a Decision No. 1570/18.2T8TMR-B.L1.S1 (only available in Portuguese here) (STJ Decision in case No. 1570/18.2T8TMR-B.L1.S1) regarding the prohibition on processing personal

data provided for in Article 9(1) of the GDPR, which is excepted if the processing is necessary for the defense of a right in legal proceedings or whenever the courts act in the exercise of their judicial function. In the present case, the objective criteria for assessing the performance of comparable employees had not been included in the collective dismissal decision, which would have limited the employee's right to defense and prevented the court from assessing and deciding on the grounds for dismissal. There was thus a personal and legitimate interest on the part of the employee and the Court itself that conflicted with the data protection regime. As such, the Court ruled that since the Constitution of the Portuguese Republic prohibits dismissals without just cause or on political or ideological grounds, the exception to the prohibition on processing personal data in the context of an action to contest dismissal is justified.

Citation

TRP Decision in case No. 6337/21.8T8VNG

STJ Decision in case No. 1570/18.2T8TMR-B.L1.S1