

Nº6 | JUNE/JULY 2022

TM

TRENDS

LEGAL MAGAZINE

EMPLOYMENT
LAW

INSIGHTS FROM:

ARGENTINA | BRAZIL | CHINA | CZECH REPUBLIC | HUNGARY
INDIA | INDONESIA | IRELAND | ITALY | NETHERLANDS
POLAND | PORTUGAL | RUSSIA | SPAIN | TURKEY

DATA PROTECTION AND EMPLOYMENT

Volume 1: **The recruitment & on-boarding stage**



The Law Firm **Network**
FAR - REACHING LEGAL SOLUTIONS



PUBLISHER



The Law Firm Network
FAR - REACHING LEGAL SOLUTIONS

Zurich, **Switzerland**

CONTACT

E-MAIL: rafaeltruan@lfnglobal.com

TEL: **+34 9131 06660**

www.lfnglobal.com

Executive Director: **Rafael Truan Blanco**

LFN Chairman: **Peter Krarup** (Mazanti-Andersen)

Regional Directors:

EMEA - **Stephan van de Kant** (Wieringa Advocaten)

The Americas - **Alejandro Fiuza** (Brown Rudnick LLP)

Asia-Pacific - **Dang The Duc** (Indochine Counsel)

LFN Employment Practice Group Co-chairs:

Alice Mlýnková, Ph.D. (LTA Legal s.r.o.)

Andrea Corr (Blandy & Blandy)

Publications Director: **Marek Turcza** (TURCZA Kancelaria)

Employment Publication Officer: **Daniel Vrábel** (LTA Legal s.r.o.)

Graphic design and DTP: **Bartosz Wiczynski** (TURCZA Kancelaria)

Copyright © 2022 The Law Firm Network. All rights reserved.



[linkedin.com/company/the-law-firm-network/](https://www.linkedin.com/company/the-law-firm-network/)

03 INTRODUCTION

Andrea Corr, Attorney-at-law
Blandy & Blandy LLP

LFN

05 BRIEF COMMENTARY ON SENSITIVE INFORMATION AND JOB INTERVIEWS IN ARGENTINA

Pablo Nicastro & Clara Fazio, Attorneys-at-law
Barreiro, Oliva, De Luca, Jaca, Nicastro

ARGENTINA

07 BRAZILIAN EMPLOYERS MUST COMPLY WITH THE PRINCIPLES OF GENERAL DATA PROTECTION LAW DURING HIRING AND ON-BOARDING PROCEDURE

Eduardo Boccuzzi & Gustaff von Baranow Murakami, Ph.D., Attorneys-at-law
Boccuzzi Advogados Associados

BRAZIL

09 TIPS FOR PRE-EMPLOYMENT PERSONAL INFORMATION PROTECTION

Kevin Xu, Craig Zhou & Jackie Gao, Attorneys-at-law
MHP Law Firm

CHINA

11 HIRING AND ON-BOARDING PROCESS UNDER CZECH PRIVACY LAWS

Alice Mlýnková & Soňa Macurová, Ph.D., Attorneys-at-law
LTA Legal s.r.o.

CZECH REPUBLIC

13 CAUTION ADVISED FOR EMPLOYERS WISHING TO OBTAIN INFORMATION ON JOB APPLICANTS AND EMPLOYEES CONCERNING, FOR EXAMPLE, BACKGROUND CHECKS AND VACCINATION INFORMATION

Zoltán Balázs Kovács, Attorney-at-law
Szecska Attorneys at Law

HUNGARY

17 BACKGROUND VERIFICATION BY EMPLOYERS HAS BECOME INCREASINGLY COMMON ACROSS SECTORS IN THE INDIAN MARKET

Siddhartha George, Varnika Sharma & Bhumi Maheshwari, Attorneys-at-law
Poovayya & Co.

INDIA

19 INDONESIA'S CURRENT DATA PROTECTION LEGAL FRAMEWORK REQUIRES THE CONSENT OF THE INDIVIDUAL WHOSE PERSONAL DATA IS COLLECTED AND/OR UTILIZED.

Jonathan M. Streifer & Syahdan Z. Aziz, Attorneys-at-law
SSEK Legal Consultants

INDONESIA

21 DATA PROTECTION IN IRISH RECRUITMENT

Richard Lee & Sinéad Mannion, Attorneys-at-law
BHSM LLP

IRELAND

ITALY

24 HIRING PROCESS AND SENSITIVE INFORMATION IN ITALY

Domenica Cotroneo, Attorney-at-law
Cocuzza & Associati

THE NETHERLANDS

25 THE FAR-REACHING PROTECTION OF THE PERSONAL DATA OF JOB CANDIDATES IN THE NETHERLANDS

Kiki Manse & Annemarie Buwalda, Attorneys-at-law
Wieringa Advocaten

POLAND

27 QUICK GUIDE TO PRIVACY, DATA PROTECTION AND DATA USE IN EMPLOYMENT

Marta Rabe-Kozłowska, Attorney-at-law
TURCZA Kancelaria Radców Prawnych

PORTUGAL

31 ARE EMPLOYEES PRIVATE DATA PROTECTED?

Carla Martins Costa, Attorney-at-law
Abreu & Marques e Associados

RUSSIA

33 LEGAL ISSUES RELATING TO OBTAINING OF SENSITIVE INFORMATION OF A CANDIDATE EMPLOYEE

Natalia Vodolagina, Attorney-at-law
Westside Law Firm

SPAIN

35 QUICK GUIDE TO PRIVACY, DATA PROTECTION AND DATA USE IN EMPLOYMENT

Maria Gomes Sousa, Attorney-at-law
Thomas de Carranza Abogados

TURKEY

36 DATA PROTECTION OF EMPLOYEE CANDIDATES IN THE HIRING PROCESS

Emre Gökhan & Ertuğrul Aksoy, Attorneys-at-law
Pelister Atayılmaz Enkur (PAE)

— INTRODUCTION —

by LFN Executive Director
Rafael Truan Blanco

I am pleased to welcome you all to this issue of TRENDS.

One of the characteristic features of employment law is its wide impact and influence, and its development over a period of time. One of these ever-growing and changing areas, which is of particular interest to HR professionals, lawyers and other legal practitioners alike, is that of data protection.

We have therefore produced this TRENDS issue which includes information on data protection in a number of countries around the world. This first publication deals with the issue of data protection in employment at the recruitment and on-boarding stage. The information is set out as a response to a number of key questions. A subsequent publication will deal with data protection issues in the ongoing employment relationship and the final publication will cover data protection issues at the end of the employment relationship.

This guide has been created thanks to the joint efforts and close cooperation of the members of The Law

Firm Network and their partner law firms. There has never been a better time for close co-operation with colleagues across all jurisdictions and we are very pleased that, despite the many demands of the last 12 – 18 months, we have again been able to gather so many high quality submissions from colleagues for this new TRENDS publication.

We are delighted to be able to deliver this issue of TRENDS and we extend our sincere thanks to all the contributors who made this possible.

We sincerely hope that you will find this a useful guide in your day-to-day work.

Written by:



Andrea Corr
Attorney-at-law

Blandy & Blandy LLP, UNITED KINGDOM
BLANDY.CO.UK



BRIEF COMMENTARY ON SENSITIVE INFORMATION AND JOB INTERVIEWS IN ARGENTINA

by Pablo Nicastro & Clara Fazio



In this article we will make brief comments on the scope and practices regarding the treatment of information in the context of job interviews in Argentina.

How do I handle the issue of background checks, including those involving sensitive personal data such as criminal records?

You cannot request applicants to disclose sensitive data if this is not provided by the law. Sensitive data includes ethnic or racial origin, political opinions, religious, philosophical and moral beliefs, trade union membership, sexuality, and health or medical background.

Health issues and criminal records are particularly delicate issues when recruiting employees. These are dealt with below:

A Pre-employment health examination:

The employer has the obligation and the right to conduct pre-employment health examinations of the applicants. Pre-employment examinations are a series of general and basic medical tests.

The purpose of the pre-employment examinations is: (i) to determine the suitability of the applicant's psychophysical conditions for the work, which in no way can be used as a



discriminatory element for employment; (ii) to detect pre-existing pathologies that might worsen if exposed to risky chemical elements listed by Decree Nro. 658/96; and (iii) to inform the labor risk insurance company for future medical attentions and cover.

Employers may request further examinations other than those provided for by the law for the pre-employment examination, as long as this is justified by the kind of work to be performed by the applicant. Each particular case must be analyzed.

Also, the employer may request self-attestations from applicants informing of diseases, ailments or medical history.

B Criminal Records:

Criminal record checks are not prohibited in Argentina. However, these checks should be carried out in a non-discriminatory manner.

Under Argentinean law, job offers may not contain restrictions for reasons such as race, ethnicity, religion,

nationality, ideology, political or union opinion, sex, gender, economic position, social condition, physical characteristics, disability, residence, family responsibilities or criminal records of persons who served out their sentence.

Are there particular issues in checking candidates' social media profiles?

It is not unlawful to check candidates' social media profiles. This matter is not subject to regularization. If the candidates' social media profiles are public, there are no legal impediments to check them.

Can I ask candidates about their Covid-19 vaccination status?

In Argentina there is no legal obligation to be vaccinated against COVID-19. However, there are conflicting positions regarding this: some argue that, in the exercise of freedom of choice, employees could choose not to be vaccinated, while some others



argue that employees could be forced to be vaccinated to safeguard the health of their colleagues, their own health, and the health of society.

Candidates can be asked to report about their COVID-19 vaccination status, but they are not legally obliged to answer. Since this is sensitive personal data, they are under no obligation to respond, nor can they be forced to respond.

Again, employers may ask employees about their vaccination status, as long as this is justified by the kind of work to be performed by the applicant. Each particular case must be analyzed (eg. medical institutions, adults care).

Are employees entitled to lie or to omit information; if information is subsequently found to be false, what can I do?

Employees are only obliged to provide the information required by law. In case the applicant lies or omits information, it will be necessary to check whether the information omitted or lied about was concerning an essential condition for the job or not.

This will determine whether or not a sanction to the applicant is appropriate and also how serious the such a sanction will be.

Sanctions may include reprimand, suspension, or dismissal with fair cause. Sanctions will be proportional to the seriousness of the lie or omission of information by the employee, mostly if it affects the development of his work.

Written by:



Pablo Nicastro
 Attorney-at-law

Barreiro, Oliva, De Luca, Jaca, Nicastro, ARGENTINA
 BODLEGAL.COM



Clara Fazio
 Attorney-at-law

Barreiro, Oliva, De Luca, Jaca, Nicastro, ARGENTINA
 BODLEGAL.COM



BRAZILIAN EMPLOYERS MUST COMPLY WITH THE PRINCIPLES OF GENERAL DATA PROTECTION LAW DURING HIRING AND ON-BOARDING PROCEDURE

by Eduardo Boccuzzi & Gustaff von Baranow Murakami

Under the Brazilian legal system, the gathering of candidates' personal data in hiring and on-boarding procedure must comply with the Brazilian General Data Protection Law (LGPD), which, inspired by the European General Data Protection Regulation (GDPR), is also applied to the Labor Law.

How do I handle the issue of background checks, including those involving sensitive personal data such as criminal records?

To check candidates' background and gather their personal data, the companies must comply with the LGPD principles, such as: (i) Purpose Principle, concerning the need of defensible, explicit, specific and well-informed objectives for the data processing; (ii) Adequacy Principle, concerning the need of compatibility between requested information and company goals; (iii) Necessity Principle, concerning the need of requesting the least data possible for the shortest time possible; (iv) Transparency Principle, concerning the need of notifying candidates in a clear, precise and accessible way about which data will be collected and how it will be processed; and (v) Non-Discrimination Principle, concerning the prohibition of using the data for discriminatory, illicit or abusive purposes.

In view of the Non-Discrimination Principle, personal data considered to be sensitive or liable of being used for acts of prejudice against candidates shall not be requested. Therefore,

criminal records, toxicologic exams, ethnical origins, sexual orientations, religious beliefs, credit restrictions and political opinions should not be checked. Regarding criminal records, toxicologic exams and religious beliefs, their gathering and use is only defensible, for example, for positions involving, respectively, property security, professional driving and religious education. Anyway, when gathering sensitive personal data, the employers need to take special care in its processing, which is why the companies should carry out an extensive analysis about its real need. Furthermore, the sensitive personal data processing requires a specific and detached consent of its holder for an extremely well-defined purpose.

Regarding criminal records specifically, the Brazilian case-law authorizes its checking not only for positions involving property security, but also for those involving: (i) domestic work; (ii) minors, elderlies and disabled care; (iii) cargo drive; (iv) agro-industrial sharp instruments use; (v) banking activities; (vi) weapons and toxic substances handling; and (vi) confidential information processing.

To keep candidates well-informed about their data processing, the companies should prepare a Hiring Policy with all the information related to data storage, use and sharing. Anyway, applications forms should be brief and simple, asking, at first, only information considered relevant and essential. Besides, when asking or checking candidates' information, the employers must obtain their free, unequivocal and well-informed consent in order to storage, use and share their personal data. Finally, the companies shall always keep a wide communication channel with the data holders, since they are entitled to access, update, delete and revoke the information given at any time.

Are there particular issues in checking candidates'

social media profiles?

The LGPD does not prohibit checking candidates' social media profiles. However, this data must be made available by its owners or, in other words, must be found in public databases. In these cases, the candidate's permission is not even necessary. Yet, the checking shall not be used for discriminatory purposes, as for "company profile" selections based on age, religious belief, sociability, political opinion, sexual orientation or ethnic origin. Therefore, even when social media profiles are publicly accessible, the gathering of their data shall have a proper purpose for the hiring and on-boarding procedure, such as information and respectful behaviour check or knowledge and technical skills search. Finally, social media's protected and restricted data shall not be pursued or checked.

Can I ask candidates about their Covid-19 vaccination status?

Although the candidates' Covid-19 vaccination status configures sensitive health personal data, it may be requested during hiring and on-boarding procedure, since it has a well-defined and reasonable purpose, namely: the compliance with health, hygiene and safety requirements in the work environment. In this way, the gathering of this data does not depend on the candidate's consent, mainly because, as mentioned before, it serves to protect the life and physical safety of the data holder and third parties. However, it must still be respected the Principles of Effectiveness, Necessity, Proportionality, Confidentiality and, above all, Non-Discrimination. Therefore, to respect, as much as possible, the candidates' privacy and intimacy, the companies shall not disclose this data and must store it in a

safe and secure way.

Regarding the non-discrimination, the lack of Covid-19 vaccination shall not be used as an arbitrary elimination standard. So, before asking candidates about their Covid-19 vaccination status, the employers shall be clear about its purpose, showing them how this information meets the company objectives and goals. Furthermore, this purpose must be fair, defensible, relevant and strictly necessary for a specific and legitimate goal, as the one related to reducing the risk of contamination and death from Covid-19 in the work environment. Therefore, if the company is not able to present a purpose (e.g. it adopts the remote work arrangement) or if its goals can be reached through other means, the Covid-19 vaccination status shall not be asked.

Finally, there is a motion pending in Brazilian Supreme Court in which is being discussed the constitutionality of requiring proof of vaccination when hiring new employees. In the moment, despite there is no final decision, there has already been a precautionary one authorizing the requirement when the candidate does not have medical contraindication.

Are employees entitled to lie or to omit information; if information is subsequently found to be false, what can I do?

Candidates are entitled to lie or omit information. Nonetheless, lies and omissions may lead to just cause termination or to hiring and on-boarding procedure exclusion.

How should I deal with the personal data of unsuccessful candidates?

Curriculum and personal data sent by unsuccessful candidates shall not remain archived indefinitely. However, they should not be immediately deleted, since they could be required in eventual motions challenging the hiring and on-boarding procedure. Therefore, such information must be kept for the period set by the hiring and on-boarding program, which should fix a period of about two years. Anyway, the company will need the candidate's consent, that must be free, unambiguous and well-informed. This consent is essential for the maintenance of a curriculum database, which requires an agreement in proper terms and for a determined time, regardless of whether it is in the candidate's legitimate interest or not. Furthermore, while the data remains stored, the candidate is entitled to know who is responsible for its processing, as well as to access, update, delete and revoke the information given. Finally, when deleting the data, the employers must guarantee that non-authorized third parties will still be unable to access or retrieve the discarded information.

Summary

During hiring and on-boarding procedure, employers should always keep in mind the Principles of Purpose, Adequacy, Proportionality, Necessity, Effectiveness, Transparency, Confidentiality and, above all, Non-Discrimination, since, under Brazilian legal system, they are the basis of LGPD and, thereafter, of personal data protection within the working environment.

Written by:



Eduardo Boccuzzi

Attorney-at-law

Boccuzzi Advogados Associados, BRAZIL
 BOCCUZZI.COM.BR



Gustaff von Baranow Murakami

Attorney-at-law

Boccuzzi Advogados Associados, BRAZIL
 BOCCUZZI.COM.BR



VISIT THE WEBSITE HERE



TIPS FOR PRE-EMPLOYMENT PERSONAL INFORMATION PROTECTION

by Kevin Xu, Craig Zhou & Jackie Gao

China's data protection regime is in a period of change and there has been significant progress in the field of data protection legislation in recent years.

The Civil Code, effective on 1 January 2021, expressly provides the right of privacy and personal information protection. The express protection of personal information under the Civil Code represents a new era of privacy and personal information protection.

The Personal Information Protection Law ("PIPL") entered into effect on November 1, 2021. It is China's first comprehensive personal information protection law, and is modeled after the European Union's General Data Protection Regulation. The PIPL governs personal information processing activities carried out by entities or individuals within China and, once certain conditions are met, processing activities outside China.

There are two other key laws on cybersecurity and data protection, namely the Cybersecurity Law ("CSL") (effective on June 1, 2017) and the Data Security Law ("DSL") (effective on September 1, 2021). The CSL, the DSL, and the PIPL altogether constitute the three fundamental pieces of legislation in respect of cybersecurity and data protection in China. The relevant implementing rules are still in the process of drafting and seeking public opinion.

How do I handle the issue of background checks, including those involving sensitive personal data such as criminal records?

"Personal information" is broadly defined by the PIPL to cover various information, recorded in electronic or any other form, that is related to an identified or identifiable natural person, excluding any information that has been anonymized. Furthermore, sensitive personal information, which refers to any information that may easily result in violation to the personal dignity of any natural person or endanger personal or property safety,

once it is leaked or unlawfully used, enjoys more protections under the PIPL. Personal information generally includes, without limitation, name, date of birth, ID number, address and telephone number of the natural person while sensitive personal information includes without limitation biometric identification, religious belief, particular identity, medical health information, financial accounts, and whereabouts and tracks, as well as the personal information of minors under the age of 14. Compared with processing non-sensitive personal information with informed consents, processing sensitive personal information requires separate consents from individuals. Separate consent means that the data processor shall obtain individual's informed consent for each item of personal information rather than one-off informed consents for multiple items of personal information or multiple processing activities.

An employer, as a personal information processor, shall, before collecting personal information, inform candidates of the following truthfully, accurately and completely in a notable manner and by using explicit and easy to understand languages:

- 1 name and contact details of processor;
- 2 purposes and methods of processing and catalogues and storage period of personal information to be processed;
- 3 methods and procedures through which individuals can exercise their rights granted by the PIPL; and
- 4 other matters that are required to be informed by laws and regulations.

After being fully informed, candidates may give their explicit consents on a voluntary basis or each individual shall give his/her separate consent or written consent if laws and regulations require to do so. In the event of any change of processing purposes, processing methods or catalogues of



personal information to be processed, processor is obligated to reobtain individuals' consents. Even so, each individual has the right to withdraw consent at his/her own discretion. Withdrawal of consent would not affect the validity of personal information processing that has been completed based on individual's consent. Processor should provide to individuals convenient ways of withdrawal.

Generally, under PRC law, background checks for candidates are permitted. It is advisable to notify each candidate of the scope of information that will be collected, the intended purposes of such collection and other required items as outlined above; it is also advisable to obtain written consent from each candidate before such data collection. If background checks will involve collection of sensitive personal information, employers should explicitly list what type of personal information will be collected in their personal information notice and consent form and collect separate consents from candidates.

Are there particular issues in checking candidates' social media profiles?

Candidates' social media profiles fall into the scope of sensitive personal information and, under certain circumstance, may also be protected as candidates' privacy. Generally, obtaining consent from candidates is the prerequisite for processing his/her personal information. However, PIPL additionally provides an exemption to obtain consent if the personal information has already been disclosed by the individual. So, employers may review social media



profiles, which have been disclosed by candidates themselves and can be available publicly online, without obtaining consent, and process such information within a reasonable scope. Additionally, employers should obtain candidates' explicit consents before accessing social media profiles which are not disclosed by candidates no matter they are sensitive personal information or privacy.

Are employees entitled to lie or to omit information; if information is subsequently found to be false, what can I do?

PRC Labor Contract Law entitles employers to enquire of employees about their basic information in direct relation to their labor contracts while it obliges employees to give answers truthfully. If an employee concludes a labor contract by use of fraudulent act, which leads to that his/her employer acts against its real intention, such labor contract may be wholly or partially invalid.

A more common practice is that (I) employers may request their employees to represent and warrant in a written form the authentication, accuracy and completeness of all information they have disclosed; (II) breach of such representation or warranty would be deemed as a serious violation of employers' rules and policies; and (III) employers may take disciplinary actions against employees up to immediate dismissal, subject to specifics of their rules and policies.

Can I ask candidates about their covid19 vaccination status?

Covid-19 vaccination is not mandatory in PRC. Any resident in PRC may receive Covid-19 vaccination on voluntary basis after being fully informed. It is debatable that Covid-19 vaccination information is in direct relation to candidates' labor contracts. Therefore, candidates or employees are not obligated to disclose their Covid-19

vaccination status. However, it does not prohibit employers from collecting such sensitive personal information after they obtain separate consents from candidates and employees.

How should I deal with the personal data of unsuccessful candidates?

Generally speaking, personal information shall be stored for a minimum period necessary for achieving the processing purposes, unless applicable laws and regulations require otherwise.

Moreover, a personal information processor should delete personal information under any of the following circumstances:

- 1** the purposes for which personal information is processed have been achieved or cannot be achieved, or personal information is no longer necessary in relation to the purposes for which it is processed;
- 2** personal information processor ceases services or products supply or the agreed time limit of personal information storage has expired;
- 3** consents have been withdrawn;
- 4** personal information processor processes personal information by violation of laws, regulations or agreements;
- 5** other circumstances as provided by laws and regulations.

Given the above, an employer should delete personal information of unsuccessful candidates upon any of the above circumstances or retain such personal information for a period of minimum necessity as explicitly consented by candidates.

In practice, some employers would retain the personal information of unsuccessful candidates with the

intention that they may provide the appropriate position and recruitment information to the unsuccessful candidates in the future. Under such circumstance, they need to obtain explicit consent from unsuccessful candidates for such retention.

Written by:



Kevin Xu
Attorney-at-law

MHP Law Firm, CHINA
MHPLAWYER.COM



Craig Zhou
Attorney-at-law

MHP Law Firm, CHINA
MHPLAWYER.COM



Jackie Gao
Attorney-at-law

MHP Law Firm, CHINA
MHPLAWYER.COM



HIRING AND ON-BOARDING PROCESS UNDER CZECH PRIVACY LAWS

by Alice Mlýnková, Ph.D. & Soňa Macurová

According to the Czech Labour Code, during a job interview, an employer may seek only such information that is directly linked to the intended employment. No other information may be sought either from the candidate or any third party. Employers are never allowed to inquire about sensitive issues such as pregnancy, family status, sexual orientation, religion, criminal record etc., unless, in some cases, there is a material reason lying in the nature of the job to make such an inquiry and some other conditions are met. These are the general rules employers must adhere to during the hiring process and throughout the employment, while also complying with all their data protection obligations based mostly on the GDPR.

How are employers supposed to handle the issue of background checks, including those involving sensitive personal data such as criminal records?

As explained above, an employer is entitled to request only information that is directly related to the performance of the employee's (job candidate's) work duties and to the establishment, change or termination of the employment.

There are several types of information which the employer is strictly prohibited from requesting. Among these are the following: sexual orientation, ethnic origin, trade union

membership, membership in political parties and religion.

Other sensitive information, such as pregnancy, criminal records, marital status and the employee's financial situation, may be requested in certain cases, provided that such a request is proportionate and reasonable. In some cases, such information may be required based on specific laws (e.g., if the law requires that the job should be performed only by an employee with a clean criminal record or if the work cannot be performed by pregnant women, etc.).

A situation in which an employee (or another person, such as a previous employer) provides sensitive information without being asked is not considered a violation of applicable laws, but an employer shall not keep any records containing such information.

As regards background checks, these

are generally possible, but an employer must comply with the principles above. On the other hand, a person (such as a previous employer) asked for information about a job candidate should consider very carefully whether they are allowed to provide personal data of the candidate in question to third parties.

Are there particular issues in checking candidates' social media profiles?

Again, the employer is entitled only to information directly related to the performance of the employee's work duties or the employment itself. If the employer wants to check a candidate's social media profile, they should check only career-oriented social media such as LinkedIn. Personal social media such as Facebook should not be part of the social media check unless a very specific reason is given. Especially, the employer should not make any records of information which they found on the





social media. If the employer records such information, they may not only violate the GDPR but also, if they select a candidate based on information found on the social media forbidden to the employer, the unsuccessful candidate could have grounds for a discrimination suit.

Can employers ask candidates about their Covid-19 vaccination status?

No. The COVID-19 vaccine is not mandatory in the Czech Republic and therefore, the employer is not entitled to know if its employees are vaccinated against COVID-19 or not. There may exist rare exemptions to this rule based on the specific nature of the work.

Are employees entitled to lie or to omit information; if information is subsequently found to be false, what can employers do?

If an employer requires information beyond the scope allowed (such as family status) and the employee lies, no negative consequences for the employee can be derived based on that.

If an employee provides false information related to the employment (such as qualification, previous experience etc.), the employer needs to assess the intensity of the impact of

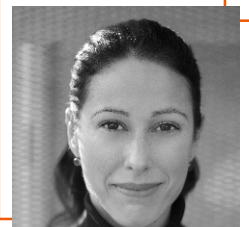
such false information on the performance of the employee's work duties and/or prerequisites for the work performed by the employee (e.g., if a certain qualification or licence is required by the law for the respective work and the employee does not hold it, contrary to their initial statement). Based on such assessment, the employer may have several options on how to handle such a situation. If the employee causes any damage by such a lie, the employer may sue the employee and claim damages in full. In certain cases, the employer could terminate the employment.

How should employers deal with the personal data of unsuccessful candidates?

The employer should delete the personal data of unsuccessful candidates without undue delay after the hiring process is completed. If the employer wishes to further process such data, they must have a consent from the data subject (unsuccessful candidate). Such consent must be granted in written form and contain all mandatory elements of a consent required by the GDPR. That means that the consent must be voluntary, the data subject must be informed about the purpose of the consent (future hiring opportunities), the conditions of the processing and about their rights arising from the processing. It is also important to keep in mind that the consent allows for data processing

only for a predetermined period of time (stated in the consent) and that such period of processing must be adequate to the purposes of the processing (we can generally speak about one year in respect to the processing relating to unsuccessful candidates).

Written by:



Alice Mlýnková, Ph.D.
Attorney-at-law
LTA Legal s.r.o., CZECH REPUBLIC
LTAPARTNERS.COM



Soňa Macurová
Attorney-at-law
LTA Legal s.r.o., CZECH REPUBLIC
LTAPARTNERS.COM



CAUTION ADVISED FOR EMPLOYERS WISHING TO OBTAIN INFORMATION ON JOB APPLICANTS AND EMPLOYEES CONCERNING, FOR EXAMPLE, BACKGROUND CHECKS AND VACCINATION INFORMATION

by Zoltán Balázs Kovács

How does the employer handle the issue of background checks, including those involving sensitive personal data such as criminal records?

Under the Hungarian Labour Code, the employer may require an employee to make such a statement or to disclose such personal data which is essential for the conclusion, performance or termination of the employment relationship or for the enforcement of claims arising out of the Labour Code (for this purpose, the employer may request the presentation of a document but may not make a copy of it, only a note that the given document has been duly presented and checked).

It is also important to comply with all data protection principles, e.g. only such data may be processed which are necessary for reaching a legitimate purpose and only for a period absolutely necessary.

Requesting criminal certificate

Under the Labour Code, the employer may process the criminal data of the employee or the person wishing to enter into an employment agreement with the employer for the purposes of examining if an act of law or the employer does not restrict or prohibit the employment of the relevant person in the respective position filled in or wished to be filled in. The employer may set a restrictive or prohibitive condition if the employment of the relevant person in the respective position would pose a risk to

- ① the employer's considerable monetary interest,
- ② secrets protected by law, or
- ③ the safe storage of guns, explo-

sives, poisonous or hazardous chemicals, biological substances and/or nuclear substances.

The employer has to determine in writing in advance (e.g. by way of a specific document) the restrictive or prohibitive condition serving as a basis for the processing of criminal data as well as the conditions for the processing of such data. The request of the presentation of a clean criminal certificate ("hatósági erkölcsi bizonyítvány" in Hungarian) cannot be general, i.e. the respective scope of work has to justify such request.

It is worth noting that pursuant to the Labour Code and the relevant practice of the Hungarian data protection authority (DPA), even if a criminal certificate may be requested, employers may only require employees to show them the criminal certificate but they may not make a copy of the document.

In addition to the above, since it is the employer's legitimate interest (Article 6 (1) f) of the GDPR and Section 11 paragraphs (3)-(5) of the Labour Code) which may serve as a legal basis of the processing of the above data (i.e. the fact that an employee candidate or an employee has a clean criminal record), the employer has to prepare a so-called balancing test (aka proportionality test) prior to any processing taking place and due information must be given to the data subjects of the data processing before the commencement of any data processing.

Education and employment history (CVs)

The employer / potential employer has to provide information on the processing of the applications (including also CVs). As per the DPA, the personal data (including CVs) of

rejected applicants and any notes made by the employer have to be deleted right after the decision on rejection of the applicant. (We note that at this point in time (i.e. when communicating the decision on rejection to the applicant), the employer / company may decide to ask for the consent of the rejected applicant to the further processing of his/her application (for a limited period of time, e.g. a couple of months) so that if there is any vacancy in a position, the employer / company could again evaluate the application and contact the candidate as necessary.

Education and employment history of the applicants who have become employees may be processed if the legitimate interest of the employer justifies it. This means that a balancing test has to be prepared in this regard and due information must be given to the employees in due course.

Credentials (i.e. reference letters from previous employers)

The above apply accordingly (i.e.





processing has to be proportionate, balancing test must be prepared and information must be duly given to the data subjects prior to any processing taking place). The documents can only be checked, and not copied/stored.

The above-mentioned processing activities must be duly incorporated in the registry of processing activities to be kept in accordance with Article 30 of the GDPR.

Are there particular issues in checking candidates' social media profiles?

In line with the practice of the DPA, the employer has to meet the following main criteria in this regard:

- 1** prior information must be given to the job applicants on the fact that checking the publicly available profile of the candidate forms part of the selection process,

- 2** only fully public information can be checked (information which is partially public (e.g. within a specific group only) or fully private cannot),
- 3** only such information can be checked which are relevant from the perspective of the scope of work/job (information on private life, family status, religion etc. cannot be checked),
- 4** the employer is not allowed to download, store or transfer the profile of the applicant.

Since it is the employer's legitimate interest which may serve as a legal basis of the processing of the above data, the employer has to prepare a balancing test prior to any processing taking place and due information must be given to the data subjects of the data processing before the start of processing.

The above-mentioned processing activity must be duly incorporated in the registry of processing activities to be kept in accordance with Article 30 of the GDPR.

Can the employer ask candidates about their Covid-19 vaccination status?

Yes, subject to certain conditions. The DPA issued an information paper in April 2021 on as to whether employers are allowed to get information on the fact if the employees are vaccinated against COVID-19. Below follows a summary of the information paper.

Under labour and, respectively, labour protection laws,

- » the employer is required to continuously maintain a safe and healthy workplace,

the employee's personality rights can only be restricted if the restriction is absolutely necessary for a reason directly connected to the employment and if it is proportionate with the purpose wished to be achieved,

- » the employer must inform the employees in advance and in writing about the method, conditions and expected duration of the restriction and also about the circumstances justifying the necessity and proportionality of the restriction,

- » the employer may require the employee to make such a declaration or to provide such personal data, which is relevant from the perspective of the creation, performance or termination of the employment or the assertion of claims based on the Labour Code. To reach this purpose, the employer may require the employee to show a document.

Requiring an employee to show his/her "immunity certificate" (which is a plastic card proving that the relevant person has been vaccinated against COVID-19) or the app certifying vaccination to the employer qualifies as a restriction of the employee's personality rights.

The DPA stresses that what is included in the opinion paper applies in the then current pandemic situation. In our view, even though, the current situation is much better than it was when the opinion paper was issued, officially, there is still a state of danger in Hungary and we might be facing the next wave in the Fall. Based on this, we are of the view that what is included in the opinion paper likely still holds.

In the DPA's view, under the labour law





regulations mentioned above, based on a so-called labour (health and safety) risk assessment to be prepared by the employer in advance, requiring employees in certain positions (i.e. with a certain scope of work) to present their immunity certificate or show their app to the employer may be a necessary and proportionate measure (the protection of the life and health of employees and third persons getting in contact with the employees may justify the measure). The DPA adds that this kind of data processing can also serve the interest of the public.

As per the DPA's view, the employer can request the employee to present his/her immunity card or the app (i.e. the employer can get the information on whether or not an employee has been vaccinated) if:

- 1 the employer prepares a risk assessment in advance, which is to justify which employees can be requested to show the plastic card or the app (i.e. to get the information if the relevant employee is vaccinated or not). It is important that if an employee works from home and he/she keeps working from home also in the future, no such request can be made to him/her. However, such request can be justified in regard of employees with a number of daily contacts (e.g. receptionists) or employees working mainly outside the workplace and getting in contact with a number of people (e.g. at the sites at other companies),
- 2 the employer gives prior information to the employees affected (i.e. data subjects) in a documented way about a number of factors as required by the GDPR and the Labour Code, including the legal basis (a legal basis from Article 6 (1) of the GDPR and a legal basis from Article 9 (2) of the GDPR has to be named, the latter could be clause b), h) or i), as the case may be) and the purpose of processing, the retention period, the persons having access to the information, rights and remedies available to the data subjects, etc.),
- 3 the purpose of the employer must be real, meaning that if the employer decides to ask for the information (data) in regard of certain employees if they have been vaccinated, then the employer is required to take the necessary measures in light of the information obtained and to duly document them. Also, it is

important that the personal data processed must be capable of reaching the purpose of the employer (no data not necessary for reaching the purpose may be processed),

- 4 the employer can only process (make a brief note of) the following data: the fact that a certain employee has been vaccinated and, if indicated on the immunity certificate or in the app, the duration of the immunity (i.e. no any other data may be processed),
- 5 the employer can only request the respective employees to show their immunity certificate/app and the employer is not allowed to make a copy of the documents, and the data cannot be stored and/or transferred, the employer is only allowed to make a note of the fact that the respective employee has proven that he/she has been vaccinated and, if indicated on the immunity certificate or in the app, the duration of the immunity,
- 6 data protection principles must be respected (e.g. data security (for example, only those persons can have access to the information collected who need to have access to such information for the purposes of performing their work), accuracy of data, etc.).

The opinion paper is silent on the retention period, and there is no specific statutory retention period, thus, the employer is responsible for applying a proper retention period. In our view, keeping the data until the end of the state of danger may seem reasonable.

Are employees entitled to lie or to omit information; if information is subsequently found to be false, what can I do?

Employees are not allowed to lie. Furthermore, if the employer lawfully

requests certain information from the employee, the employee has to provide such information. If it turns out later that the information the employee provided is false, this may have labour law consequences. The consequence depends on the concrete circumstances of the case.

How should employers deal with the personal data of unsuccessful candidates?

As a rule, the employer must delete the data of unsuccessful candidates (i.e. candidates it did not hire) since the original data processing purpose has ceased to exist. However, if there is a legitimate purpose and legal basis for further processing, then the data can be kept for some limited additional time. Namely, when the employer informs the candidate that his/her application has been rejected, the employer may ask for the candidate's consent to the further processing of his/her CV so that the employer can contact the candidate in case of a vacancy. If the candidate gives his/her consent to such further processing (based on proper prior information given on such further processing), then the employer may further process the relevant CV. This processing should normally be limited to no more than about six months.

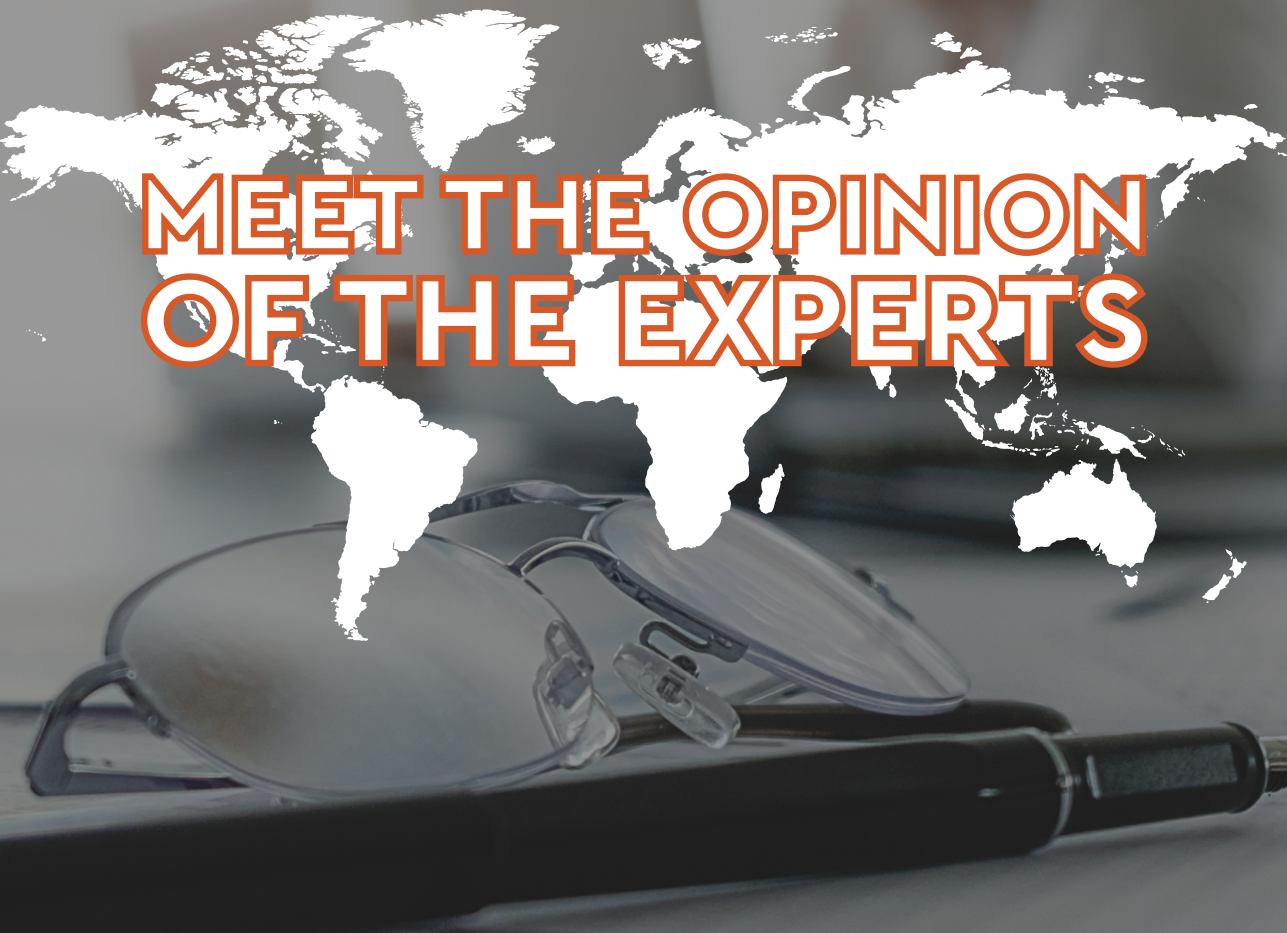
Written by:



Zoltán Balázs Kovács
Attorney-at-law
Szecskay Attorneys at Law, HUNGARY
SZECSKAY.COM



EMPLOYMENT LAWYERS FROM AROUND THE WORLD



MEET THE OPINION
OF THE EXPERTS

TRENDSTM
LEGAL MAGAZINE

BACKGROUND VERIFICATION BY EMPLOYERS HAS BECOME INCREASINGLY COMMON ACROSS SECTORS IN THE INDIAN MARKET

by Siddhartha George, Varnika Sharma & Bhumika Maheshwari

Conducting background verification checks on prospective employees by employers has become increasingly common across sectors in India. While the verification practices differ from sector to sector, some commonalities in background checks include verification of a candidate's educational qualification and previous work experience, identity checks, and checking for criminal records.

In the case *K.S. Puttaswamy v. Union of India* ((2017) 10 SCC 1), the Supreme Court of India has recognised the 'right to privacy' as an intrinsic part of the fundamental right to life contained in the Constitution of India, which would extend to personal information being shared by prospective employees with employers. It is however essential to note that fundamental rights are enforceable only against the 'State' or instrumentalities of the State, and might not be enforceable against employers in the private sector, who would not fall under the definition of State.

In India, the codified law on collection of personal information (i.e. anything that can identify a person) and sensitive personal data or information (critical personal information such as financial information, physical, physiological and mental health condition, sexual orientation, medical records and history, and biometric information) is governed by the Information Technology (Reasonable Security Practices and Procedures and

Sensitive Personal Data or Information) Rules, 2011 (the "**SPDI Rules**") and its parent legislation the Information Technology Act, 2000.

It is relevant to note that a draft Personal Data Protection Bill, 2019 is presently pending before the Indian legislature, and will significantly change the position of law with respect to collection, processing, storing, and handling of personal information once passed. However, there is currently no clear indication of when this bill is likely to be codified into law.

How do I handle the issue of background checks, including those involving sensitive personal data such as criminal records?

The SPDI Rules require entities to obtain prior written consent before the collection of sensitive personal data. In the event the information collected during background verification falls within the ambit of 'sensitive personal data or information', prior written consent would be required.

Please note however, that in the event the information collected is 'sensitive personal data or information', but is also publicly available information (such as court records or details of a criminal record), the obligations under the SPDI Rules would not be applicable.

Are there particular issues in checking candidates' social media profiles?

While there is no specific legal restriction with respect to checking a candidates' social media profiles, it is

pertinent to note that the legality of data extraction from public databases using web-scraping and crawling, has not been judicially tested in India.

Can I ask candidates about their COVID-19 vaccination status?

Covid-19 vaccination status would constitute a medical record of the candidate and as such would be covered within the ambit of 'sensitive personal data or information'. Therefore, while collecting, receiving, possessing, storing, dealing with or handling information pertaining to the vaccination status in electronic form, compliance with the SPDI Rules, including obtaining consent of the candidate, would be required.

Are employees entitled to lie or to omit information; if information is subsequently found to be false, what can I do?

In the event an employee lies or omits to provide information which might be relevant for the employer to make an assessment with respect to hiring such an employee, the employer is entitled to terminate the employment of the said employee.

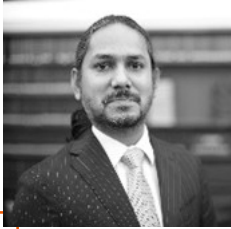
In the event an employee suggests a fact which they know is false or conceals a fact, and the employer, relying on the information executes an employment agreement with the employee, any subsequent discovery with respect to falsification/concealment of the information would amount to 'fraud' under the Indian Contract Act, 1872 and make the employment agreement voidable at the option of the employer, and as such the employer will have the option to terminate the employment agreement. Depending on the nature of and the implication of the falsification/concealment of information by an employee, employers may also have recourse to initiate criminal action against the employee for fraudulent and dishonest inducement by the employee, thereby causing the employer to enter into employment agreement and as such committing the offence of 'cheating'.



How should I deal with the personal data of unsuccessful candidates?

The SPDI Rules stipulates that any 'sensitive personal data or information' collected with the consent of the information provider should be retained only for as long as necessary or the purposes for which the information may lawfully be used, and as such any 'sensitive personal data or information' of an unsuccessful candidate should be removed/deleted from employers' database after a reasonable retention period.

Written by:



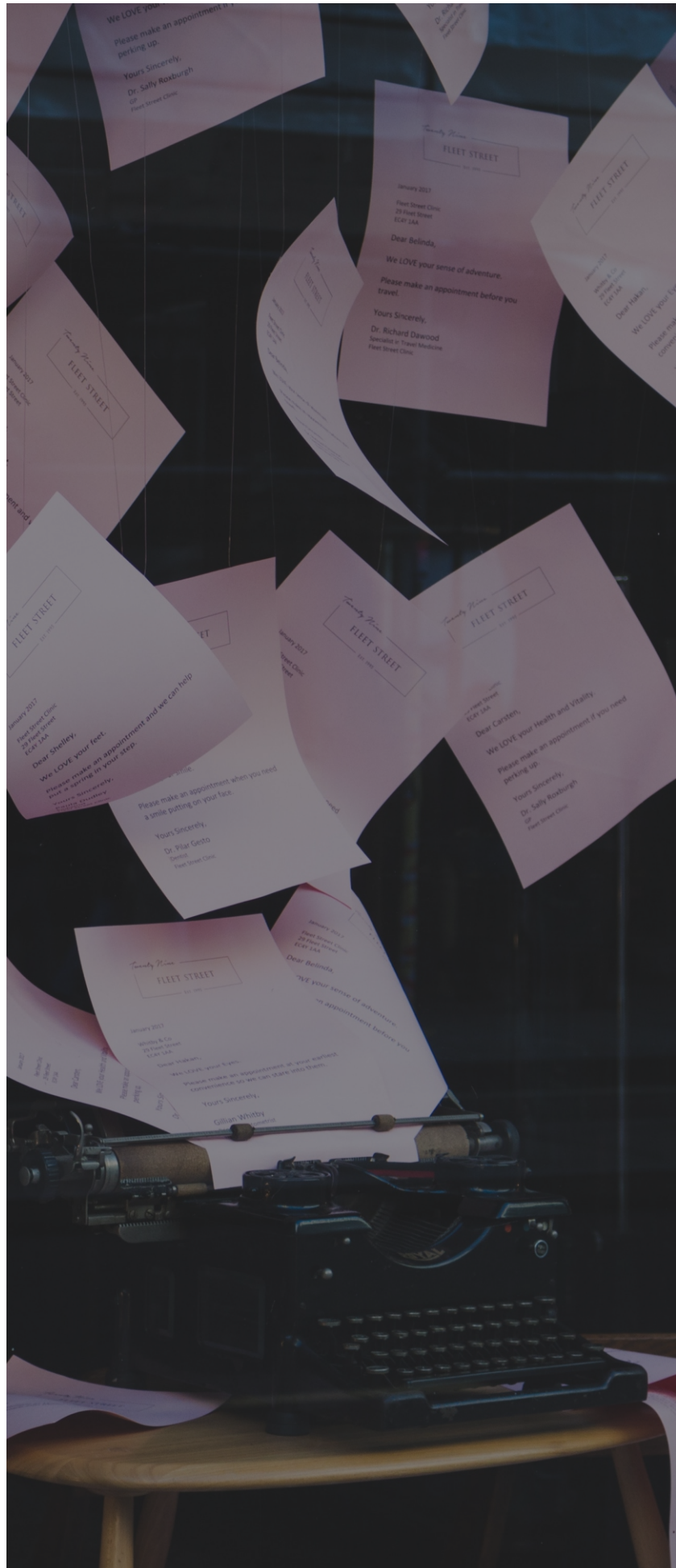
Siddhartha George
 Attorney-at-law
 Poovayya & Co., INDIA
 POOVAYYA.NET



Varnika Sharma
 Attorney-at-law
 Poovayya & Co., INDIA
 POOVAYYA.NET



Bhumika Maheshwari
 Attorney-at-law
 Poovayya & Co., INDIA
 POOVAYYA.NET



VISIT THE WEBSITE HERE



INDONESIA'S CURRENT DATA PROTECTION LEGAL FRAMEWORK REQUIRES THE CONSENT OF THE INDIVIDUAL WHOSE PERSONAL DATA IS COLLECTED AND/OR UTILIZED

by Jonathan M. Streifer & Syahdan Z. Aziz

Quick Guide to Privacy, Data Protection and Data Use in Employment: Hiring and On-Boarding Procedure

How do I handle the issue of background checks, including those involving sensitive personal data such as criminal records?

Indonesia does not have a single comprehensive law governing personal data protection. The relevant laws and regulations are scattered throughout various central and sectoral regulations, with the Electronic Information and Transactions Law ("EIT Law") as the principal law. Pursuant to the current legal framework, the written consent of the individual whose personal data is collected and/or utilized through electronic media is required. This consent must be provided in the Indonesian language. If a foreign individual is involved, the consent can be made in bilingual form with the prevailing language agreed between the parties. The above does not prejudice the possibility of obtaining the consent by other means, such as in an employment application or employment agreement.

Note that the Indonesian parliament is discussing a Personal Data Protection Bill that is targeted for enactment in 2022. One of the key points in publicly accessible draft of the bill is that it would affect personal data irrespective of whether the data is processed through electronic or non-electronic means. The current legal framework only covers personal data processed by electronic means. It is also worth

noting that while the bill is included in the 2022 Priority National Legislation Program, there is no assurance that it will be passed into law this year or the coming years.

With respect to the handling of sensitive information such as criminal records as part of a pre-employment background check, we first note that there is no statutory duty requiring job candidates or employees to inform employers of any criminal records they may have, nor is there a legal prohibition on employers requesting this information. Employees can be placed under a contractual duty to disclose their criminal records by including this obligation in the terms of their signed employment contract, in a separate undertaking, or in the company regulations. And job candidates can be required to disclose their criminal records as part of the application process, provided that the company obtains the candidate's express written consent as discussed above.

Employers may require the submission of a Police Records Statement Letter (Surat Keterangan Catatan Kepolisian or "SKCK") as part of the application process. An SKCK is basically an official letter issued by the Indonesian National Police regarding the relevant individual's involvement in any past or ongoing criminal activities. It is common for companies in Indonesia to require an SKCK as part of the hiring process.

Are there particular issues in checking candidates' social media profiles?

Information obtained from the public domain, such as social media, does not

constitute protected personal data that must be kept confidential. Hence, issues pertaining to the protection of personal data collected from social media should be remote. We view it unlikely that any other issues might emerge insofar as the information obtained from social media is used in a way that does not constitute a violation of prevailing laws and regulations. For instance, using the obtained information for any illegal purposes, such as fraud or document forgery, is subject to criminal penalties.

Can I ask candidates about their covid19 vaccination status?

The prevailing laws and regulations in Indonesia are silent on this matter. Employers may argue that this information is required to comply with the Indonesian Manpower Law, which requires employers to protect the welfare, safety and health, both mental and physical, of their employees. Requesting proof of Covid-19 vaccination may be considered as protecting the health and safety of everyone in the work environment by helping to prevent the transmission of Covid-19 among employees.

Practically speaking, it is also common practice for office buildings in Jakarta to require all visitors, including employees who work in the building, to provide proof of vaccination before entering the building. Considering our discussion above, it is possible for employers to require the same, especially during the pandemic.

Are employees entitled to lie or to omit information; if information is subsequently found to be false, what can I do?



Principally, employees are obliged to disclose their relevant information truthfully. Employees may be placed under a contractual duty to truthfully disclose all relevant information, either under the terms of their employment agreement, in a separate undertaking, or in the employer's company regulations. Any violation of this obligation could result in disciplinary action being taken against the employees, subject to the terms provided in the employment agreement, separate undertaking, or company regulations, and the prevailing laws and regulations. We note that the types of disciplinary action normally taken depend on the seriousness of the violation as governed under the employment agreement or company regulations.

How should I deal with the personal data of unsuccessful candidates?

Indonesian data protection law in general requires that personal data be stored in encrypted form in the electronic system for at least five years or as may be regulated otherwise. Personal data may be erased from the system once five years has elapsed and so long as the erasure is permitted by law, unless the personal data is still being utilized for the original purpose it was collected. In any case, a person can request the erasure of their personal data subject to the provisions of prevailing laws and regulations.

Given the foregoing, we view that the personal data of candidates obtained by an employer electronically can be

stored accordingly, regardless of whether or not the candidates are employed. The employer in this case shall be responsible for the security of the stored personal data. Practically speaking, it is common for the personal data of unsuccessful candidates, i.e., their curricula vitae and supporting documents, to be kept by companies for possible future employment consideration.

Summary

Indonesia does not as of this writing have a single comprehensive personal data protection law. Currently, personal data protection is principally governed by the EIT Law and its implementing regulations, and this current legal framework only affects personal data processed by electronic means. Employers that collect and process the personal data of job candidates or employees by electronic means must obtain the prior consent of the candidate or employee for the collection and use of their personal data.

The collection of personal data and the assurance of that personal data's truthfulness can be agreed contractually between employer and employee/candidate in the employment agreement, a separate undertaking, or the company regulations. Employers may utilize the personal data or any information of

employees or job candidates insofar it is made use of as agreed by consent and does not constitute a violation of prevailing laws and regulations.

Written by:



Jonathan M. Streifer

Attorney-at-law

LTA Legal s.r.o., CZECH REPUBLIC

LTAPARTNERS.COM



Syahdan Z. Aziz

Attorney-at-law

LTA Legal s.r.o., CZECH REPUBLIC

LTAPARTNERS.COM



DATA PROTECTION IN IRISH RECRUITMENT

by Richard Lee & Sinéad Mannion

Irish Data Protection legislation and the EU General Data Protection Regulation (GDPR) places obligations on employers when processing personal data of prospective employees in a recruitment process. Employers have the responsibility to be lawful, fair, and transparent and to limit the data processing to what is necessary to fulfil the recruitment purpose.

Richard Lee is a partner of BHSM LLP's Employment & Benefit practice, advising domestic and international corporate clients in contentious and non-contentious issues that arise in all aspects of the employer and employee relationship. Sinéad Mannion is a Senior Associate in BHSM LLP's Corporate Department, specialising in corporate transactions. Sinéad has considerable experience in dealing with all issues relating to data protection and privacy law.

How do I handle the issue of background checks, including those involving sensitive personal data such as criminal records?

Employers should exercise caution when conducting background checks on prospective employees. Background checks typically require employers to liaise with third parties such as previous employers or

recruitment agencies and as such employers are processing applicants' personal data. Often, employers are processing sensitive personal data such as medical records and/or criminal convictions.

It was previously commonplace in Ireland for employers to request prospective employees to submit a data access request for their criminal record to An Garda Síochána (the Police) and to provide the employer with a copy of such record. Save for roles that require Garda vetting (individuals working with or undertaking an activity, of which a necessary and regular part of it consists of having access to or contact with children or vulnerable adults) in Ireland there is no mechanism allowing for criminal records to be accessed by employers during background checks.



Employers can only process criminal offence data if the processing is either under the control of an official authority or authorised by EU or member state law. Section 55(1)(b)(v) Data Protection Act 2018 provides that the processing of criminal offence data is permitted when authorised by the law of the State.

Employers must identify a lawful basis (which may be in pursuance of a legitimate interest of the employer) under Article 6 of the GDPR for any processing of personal data they undertake in relation to a vetting process. Article 6(1)(c) of the GDPR provides that processing is lawful when "necessary for compliance with a

legal obligation to which the controller is subject". Where employers are processing special categories of personal data, they must also identify a lawful basis under Article 9 of the GDPR such as explicit consent or protection of vital interests which would allow such data to be processed. An employer would also be required to carry out a data protection impact assessment ("DPIA") for processing personal special categories of personal data or personal data relating to criminal convictions and offences. There is, however, nothing to prevent an employer from asking a prospective employee to declare that they have no previous criminal convictions or criminal history which might affect their suitability to perform a particular role.

The Data Protection Commissioner (the "DPC") has highlighted the importance of transparency when conducting background checks. It is therefore necessary that employers do not carry out background checks unless you have clearly informed the candidate that you are doing so and have sought consent from the prospective candidate to carry out same. It is furthermore recommended not to carry out background checks prior to the offer stage of the recruitment process.

Are there particular issues in checking candidates' social media profiles?

Employers are conducting social media background screening and using networks such as Facebook, Twitter, and LinkedIn to screen candidates' profiles as part of the recruitment process. Employers should not assume that merely because an individual's social media profile is publicly available, they are then allowed to process this data for their own purposes. Any type of data processing,



including social media background screening, requires a proper legal basis and legitimate interest. The GDPR also requires that employers only view social media profiles when the information is relevant to the position being applied for.

To avoid the risk of any potential legal actions, employers should have a clear policy in place on the use of social media profile screening in recruitment and candidates should be notified in advance of the recruitment process that their social media profiles may be screened as part of the hiring process. Any information obtained by employers should be provided to the candidate for their comments and candidates should also be given the opportunity to respond if any aspect of their social media has negatively influenced their application before a

decision is made by the employer on their application. It is important that employers conducting social media screening limit their data collection on finding relevant and necessary information to the candidate's job performance and recruitment decision rather than a fishing expedition, as employers pose the risk of processing excessive personal information of candidates.

Can I ask candidates about their Covid-19 vaccination status?

The vaccination status of a candidate is health data, therefore special category data under article 9 of the GDPR and it may only be processed on limited grounds.

An employer cannot ask a candidate

their vaccination status in the same sense as they cannot ask a candidate about pregnancy, marital status or sexual orientation. In order to process or collect that data, an employer would need a lawful legal basis to do so. The DPC has published guidelines (last updated November 2021) setting out the DPC's advice on the processing of COVID-19 vaccination data in the context of employment and the Work Safely Protocol. In the guidance notes, the DPC has made it clear that currently, there is no general legal basis for employers to request information on the vaccination status of an individual.

In the absence of specific legislation in this area, an employer could potentially argue that collecting vaccination data is a necessity in terms of maintaining the health of the public or to achieving 'legitimate interests' pursuant to Article 6(1)(f) of the GDPR. However, the employer would be required to show that the aim is both necessary and proportionate, and any data collected must be limited to what is necessary. The DPC considers that the decision to get a vaccine is voluntary and therefore a COVID-19 vaccination should not in general be considered a necessary workplace safety measure. Consequently, the processing of vaccine data is unlikely to be necessary or proportionate in most employment contexts.

The DPC acknowledges some specific employment contexts within which the processing of data revealing vaccination status may be deemed necessary, subject to a risk assessment and with reference to sector-specific public health guidance to determine whether the measures that they consider necessary require knowledge of employees' vaccination status. For example, the Guide to Professional Conduct and Ethics for Registered Medical Practitioners states that medical practitioners "should be vaccinated against common communicable diseases". In those specific situations, it is possible that an employer would be able to establish a lawful legal basis to know whether a person has been vaccinated or not, for the purposes of managing the health of safety of workers and visitors.

The guidance will be subject to review of the public health advice and laws relating to the nature of the virus, the pandemic, and the interplay with any vaccination change. However, until such time that the guidance is revised, it is recommended that employers continue to exercise caution in seeking vaccination status data and should





only process vaccination data where necessary to achieve a specific, legitimate purpose in line with general and sector-specific public health advice as they as they may be exposed to legal risks. The DPC has further cited the principle of data minimisation laid down in the GDPR in its guidelines, it notes that employers should implement all such measures that avoid processing the personal data of employees in the first place.

Are employees entitled to lie or to omit information; if information is subsequently found to be false, what can I do?

If a prospective employee lies or omits information during a recruitment process, this can become problematic for an employer when the individual hired for the role does not have the sufficient qualifications or experience necessary to perform the role. In the event of such misrepresentation by the employee, there are procedures available to the employer to lawfully terminate the employment contract pursuant to those procedures.

How should I deal with the personal data of unsuccessful candidates?

The Data Protection Act 2018 and GDPR requires that personal data be retained “for no longer than is necessary” for the purpose for which the personal data was processed by a data controller. This requirement places an obligation on employers to be clear about the length of time personal data will be retained and the reasons why the data is being kept. In order to be compliant with the data protection legislation, it is advisable for all employers to have a policy in place on retention periods for personal data that is obtained in a recruitment process. This policy must include defined retention periods for personal data (such as cv's, cover letters, and interview notes) and a systematic disposal of personal data within a reasonable period after the retention period expires. The DPC recommends a period of retention of personal data for one year in these situations.

Furthermore, Article 30 of the GDPR, provides for records of processing activities and obliges data controllers (including employers), to set out the envisaged time limits for erasure of the different categories of data. Employers could be liable to a fine up to a maximum €20,000,000 or 4% annual global turnover (whichever is greater) for failure to comply with the GDPR. The GDPR also provides for a right of erasure or the “right to be forgotten”

and data subjects (candidates) have the right to request that personal information be erased where the personal data is no longer necessary for the purpose for which it was obtained by the data controller (the employer). It is recommended to retain interview and other recruitment records of unsuccessful candidates for a period of at least one year following the conclusion of the recruitment process, in order to defend against any potential claims such as discrimination in the recruitment process. It is also common for employers to retain data of unsuccessful candidates for future recruitment purposes, however, in doing so, employers must ensure that they notify the applicants and that the candidates are either given the opportunity to consent or to object to the retention and on objection, the employer disposes of the personal data obtained.

Written by:



Richard Lee
Attorney-at-law

BHSM LLP, IRELAND
BHSM.IE



Sinéad Mannion
Attorney-at-law

BHSM LLP, IRELAND
BHSM.IE

HIRING PROCESS AND SENSITIVE INFORMATION IN ITALY

by **Domenica Cotroneo**

VISIT THE WEBSITE HERE



It is not easy to strike a balance in recruitment: on the one hand, the employer's legitimate interest to know as much as possible about the candidate in order to understand if he/she is the right person; on the other hand, the employees' equally legitimate expectations of privacy.

In this scenario, a new element of destabilisation is represented by new technologies that bring opportunities and risks for both sides.

How do I handle the issue of background checks, including those involving sensitive personal data such as criminal records?

At all stages of the recruitment process, the law requires the employer to refrain from any kind of prejudicial or discriminatory behaviour.

The prohibition covers investigations into political or trade union opinions or facts that are not relevant to the assessment of the employee's abilities.

For example, it is forbidden to carry out preventive checks on pregnancy or HIV status, except in the case of tasks involving a risk to the safety, security and health of the employee or third parties.

The prohibition also applies to criminal record checks, except in the case of specific tasks or the particular nature of the employment relationship.

Are there particular issues in checking candidates' social

media profiles?

Employers are allowed to process the personal data of applicants only to the extent that the processing of such data is necessary and relevant to the performance of the job for which one is applying. The individual must also be properly informed of such processing before engaging in the recruitment process.

Can I ask candidates about their covid19 vaccination status?

The employer is responsible for ensuring health in the workplace (Art. 2087 of the Civil Code) and not for individual employees.

However, even the latter does not have the right to ask questions about vaccinations, either at the time of the job interview or at a later stage. The company doctor is the person in charge of assessing the employee's suitability for the job, and then communicating it to the employer: therefore, the doctor himself can ask the employee for 'health' information.

If, on the other hand, one is in a workplace for which a law requires vaccination against Covid, it is the employer's responsibility to ensure that all his or her employees are vaccinated. So, when it comes to categories of employees for whom the mandatory vaccine has been provided, the employer's request is entirely legitimate. And this also applies in the job interview before recruitment: the employer or employee may well ask for a vaccination certificate if the candidate is on the list of those for whom the vaccine is mandatory.

Are employees entitled to lie or to omit information; if information is subsequently found to be false, what can I do?

In the case of lies during the application process, when these were decisive for recruitment and are relevant to the

continuation of the employment relationship, the employer is free to exercise disciplinary power and thus: formally challenge the circumstances to the employee, asking for justification; wait for the justification and adopt the disciplinary sanction deemed most appropriate (including dismissal).

How should I deal with the personal data of unsuccessful candidates?

Data collected during the recruitment process should generally be deleted as soon as it becomes clear that a job offer will not be made or is not accepted by the person concerned.

Written by:



Domenica Cotroneo
Attorney-at-law

Cocuzza & Associati, ITALY
COCUZZAEASSOCIATI.IT

THE FAR-REACHING PROTECTION OF THE PERSONAL DATA OF JOB CANDIDATES IN THE NETHERLANDS

by Kiki Manse & Annemarie Buwalda

Hiring and On-boarding Procedure in the Netherlands

How do I handle the issue of background checks, including those involving sensitive personal data such as criminal records?

Legal framework

In the Netherlands, a selection procedure is restricted by fundamental rights of privacy, non-discrimination, and equal treatment. Also important are the European Privacy Regulation, the General Data Protection regulation ("GDPR") and the Medical Test Act (in Dutch: "Wet medische keuring"). Furthermore, various rules of conduct regarding recruitment and selection have been drafted by Dutch (professional) associations, for example the (non-binding) recruitment code of the Dutch Association for Personnel Management and Organisational Development (in Dutch: "Nederlandse Vereniging voor Personeelsmanagement &

Organisatieontwikkeling", "NVP"). Finally, Collective Labour Agreements may contain binding rules on selection and recruitment.

Background checks in general

In general, based on the Dutch constitutional principles and the GDPR an employer wanting to carry out background checks on applicants, may do so with the prior unambiguous and explicit permission from the applicant. As a general rule, the employer should restrict its enquiries to information which is necessary and relevant for the assessment of the suitability for the particular applicant for the job. This means that an employer can only ask about, for instance, nationality, if this is relevant for the position.

Criminal background checks

An applicant is in principle not obliged to answer questions about his criminal background. An employer is however entitled to investigate the criminal background of an applicant of this is relevant for the performance of the job. The applicant is obliged to inform the employer in this respect. This information obligations for example applies for an accountant who was convicted for fraud or for a primary school teacher who was convicted for child abuse.

Under Dutch law, certain public positions (e.g. at the police, army, civilian airports, or department of foreign affairs) are considered positions which require a security investigation. With permission of the applicant, the Dutch General Information and Safety Department may investigate whether any objections exist against the hiring of the applicant for national security reasons.

An employer may further request the applicant for a Certificate of Conduct (in Dutch: "Verklaring omtrent gedrag", "VOG"). It is allowed to make a job offer contingent upon the applicant submitting such certificate at the start of employment. The applicant has to apply for the certificate. The employer will have to answer certain questions

with respect to the position of the applicant and the type of crimes that would be relevant to the performance of the job concerned. The Ministry of Justice will then investigate whether the applicant has a criminal record, including pre-trial diversions, relevant to the performance of the position for which the certificate is requested.

Processing personal data

When performing a background check, an employer should ensure that personal data is transferred in a secure manner and that the applicant is informed about the possibility that his personal data might be processed. In the Netherlands, most employers inform their applicants about this possibility in a data protection notice on their website.

In principle no sensitive personal data (e.g. criminal records or data concerning health or a person's sexual orientation) may be screened. This is only allowed if there are exceptional requirements for the vacancy that make this type of screening necessary. In addition, stricter rules apply for the processing of sensitive personal data. Sensitive personal data can only be processed if a specific legal exception, such as the protection of the vital interests of the data subject, and a general legal basis in the GDPR is applicable.

Consequences of violating Dutch laws and regulations

It is not always clear what the consequences are of violating Dutch laws and regulations while recruiting new employees. Applicants may bring





claims for unlawful discrimination against a prospective employer, based on one of the characteristics protected by equality legislation. The protected characteristics are for example, gender, pregnancy or maternity, sexual orientation, race, disability, age and religion or belief.

Apart from going to court certain institutions exist, such as the Committee for Human Rights (in Dutch: "College voor de Rechten van de Mens"), where applicants can file complaints. The rulings of the Committee are non-binding to the parties, but, if published, could cause a bad reputation for the employer.

Are there particular issues in checking candidates' social media profiles?

It is unclear whether employers may use information on the applicant that is in the public domain. In practice employers tend to use this information. As it is not yet clear whether this is permitted, an employer should avoid citing this as the reason for a possible rejection. Employers should reference the potential use of public information in the job advertisement and should also attempt to verify the accuracy of any such information before relying on it.

It is permissible to search for an applicant on social media, provided there is a legitimate purpose relating to the position the applicant is applying for. The employer must inform the applicant in advance when it carries out a social media check, explain the reasons for it, and discuss the information with the applicant.

LinkedIn is considered the only suitable business-related social media source to check an applicant.

Can I ask candidates about their Covid-19 vaccination status?

The Dutch government, and subsequently the Dutch Data Protection Authority, have taken the position that an employer is allowed to ask applicants whether they have been vaccinated. However, employees are under no obligation to answer. In addition, it is not possible for the employer to directly process (i.e. register) this data.

Are employees entitled to lie or to omit information; if information is subsequently found to be false, what can I do?

Under Dutch law an applicant should provide the employer with information that gives a true and fair picture of his professional competence (education, knowledge and experience) and should not withhold information that he knows or should know to be important to the fulfilment of the vacancy for which he is applying.

Providing false information can - depending on the circumstances - have consequences for applicant's employment later on and could even be a ground for a summary dismissal. An example from case law shows that a musician working with a theatre group was allowed to be summarily dismissed when it turned out he could not read sheet music.

However, any questions that cannot be considered relevant for the position do not have to be answered by an applicant. An applicant may even lie in response, for example, when asked if the applicant is pregnant or wants to have children in the near future.

How should I deal with the

personal data of unsuccessful candidates?

All the personal data of an unsuccessful candidate - such as the application letter, references and correspondence with the applicant - should be deleted within 4 weeks after finishing the application process, unless the applicants consents with longer retention, in which case the details can be kept for a maximum of 1 year after finishing the application process.

Written by:



Kiki Manse
Attorney-at-law

Wieringa Advocaten, THE NETHERLANDS
WIERINGA-ADVOCATEN.NL



Annemarie Buwalda
Attorney-at-law

Wieringa Advocaten, THE NETHERLANDS
WIERINGA-ADVOCATEN.NL

VISIT THE WEBSITE HERE



QUICK GUIDE TO PRIVACY, DATA PROTECTION AND DATA USE IN EMPLOYMENT

by **Marta Rabe - Kozłowska**

How do I handle the issue of background checks, including those involving sensitive personal data such as criminal records?

A certificate of clean criminal record is classified as a document containing data on criminal convictions, offenses or related security measures. These are data that, in accordance with Art. 10 of the GDPR are subject to special processing conditions.

The processing of such information may only be carried out under the supervision of public authorities or if the processing is permitted by law providing for adequate safeguards for the rights and freedoms of data subjects.

The scope of personal data that an employer may require from a job applicant, and then from an employee, has been specified in Art. 22(1) § 1 (candidate) and art. 22(1) § 3 (employee) of the Polish Labor Code.

The employer may request the provision of personal data other than those specified above, only when it is necessary to exercise the right or fulfill the obligation resulting from the law.

The Polish Labor Code does not mention information about a clean criminal record among the data that can always be requested during recruitment or employment. This means that the employer, in order to obtain them legally, must be entitled or obliged to do so under specific provisions.

Are there particular issues in checking candidates' social media profiles?

The Polish Office for Personal Data Protection in the guide for employers (Personal data protection at the workplace: A Guide for Employers) gave a clear opinion: the collection by employers and recruiters of information posted by candidates about themselves on social media is in principle unacceptable, and this also applies to publicly available information.

The Polish Personal Data Protection Office indicated that such action may have a negative impact on the candidate's assessment and may lead to profiling a candidate on the basis of these publicly available data. It is difficult to say whether the Office sees exceptions to this rule, because this topic has not been elaborated on either in the guide or in the positions taken later.

A somewhat less stringent approach is presented by an important body for data protection - the Article 29 Working Party (Opinion 2/2017 on data processing in the workplace). It indicates that browsing candidate profiles should not be a common practice, but it may already be acceptable when, due to employment needs, it is necessary to review information about a candidate that is posted on social media. In such a situation, the Article 29 Working Party allows the possibility of viewing profiles based on the legitimate interest of the controller. Therefore, it would be necessary to weigh the interests of the employer and the

candidate beforehand, and if it turns out to be acceptable, then it will be necessary to inform the candidate about browsing their profiles on social media.

The opinion was issued on the basis of Directive 95/46 / EC, but under the GDPR, the legitimate interest of the controller could also constitute a legal basis for this action. This opinion is not a legal source, but can be used as a reference.

The Article 29 Working Party draws attention to the most important issue - the nature of the profile. Before reviewing the candidate's profile, the employer or recruiter should assess whether it is a private or professional profile. The private profile should not be checked. The mere assumption that we can use information about the candidate because he has made his data public is insufficient. In this way, the employer crosses the border of privacy and enters the sphere to which he should not have access. This is problematic especially when the recruitment is carried out by representatives of the employer, and not by an external recruiter, and obtaining private information about the candidate may result in assessing him through its prism already at the stage of employment.

Therefore, a simple assumption can be made - browsing profiles on LinkedIn is acceptable because they are professional in nature.



It is good to use the description criterion - when in the description of the profile we find information that proves its professional character (e.g. a photographer, HR specialist, PR specialist, social media ninja), it is very likely that this person makes public content of a professional nature, unrelated to his life private. In the case of running a fanpage on Facebook, it seems obvious that such a profile is not private and that it is also possible to view it during the recruitment process. It has become a regularity to have two separate accounts in some portals - private and public. We observe this practice, for example, on Instagram. A public account created there may be a specific portfolio for some professions (e.g. in the creative industry) and the employer or recruiter should be able to freely browse this content.

Can I ask candidates about their Covid-19 vaccination status?

The current regulations do not provide for the possibility of employing only people vaccinated with COVID-19 or asking during an interview about the vaccination. This type of practice is discriminatory, and therefore it violates the provisions of the Labor Code, which in Art. 113 states that any form of discrimination in employment is unacceptable.

Pursuant to the Polish Labor Code, the employer requires the job applicant to provide personal data including:

- 1 first name (names) and surname;
- 2 date of birth;
- 3 contact details indicated by such a person;
- 4 education;
- 5 professional qualifications;
- 6 the course of previous employment.

The abovementioned list is closed and the request for health or vaccination data at this stage is unacceptable as there are no health and vaccinations in the primary data catalog. On one hand Article 22 § 4 of the Polish Labor Code slightly opens the way to include obtain some sensitive data from the candidates: "The employer requests other personal data than those specified in § 1 and 3, when it is necessary to exercise the right or fulfill the obligation resulting from the law". Unfortunately, also in this case the employer has his hands tied, because COVID-19 vaccinations are not



obligatory in Poland, and thus - there is no reason to ask whether the candidate or employee is vaccinated or not. The provision would be treated differently if vaccination were compulsory for everyone.

Are employees entitled to lie or to omit information; if information is subsequently found to be false, what can I do?

Pursuant to Art. 61 § 1 of the Act of May 20, 1971 – the Polish Code of Minor Offenses, a person who appropriates a position, title or rank to which he or she is not entitled, shall be liable to a fine of up to PLN 1,000 or to a reprimand. Such a situation will take place when an employee lies in the CV that he or she has worked in a given place or that he has a specific professional or academic title (without presenting any supporting documents).

On the other hand, when an employee presents, for example, a false employment certificate or a diploma of graduation, it fulfills the criteria of Art. 270 of the Act of 6 June 1997 – the Polish Criminal Code. According to this provision, anyone who, in order to be used as authentic, forges or forges a document or such document as authentic, is subject to a fine, restriction of liberty or imprisonment for a period of 3 months to 5 years.

In addition, if an employee, despite the lies in the CV, is employed and is paid remuneration for work, and therefore gains financial benefits from misleading the employer, then he fulfills the features of fraud defined in Art. 286 of the Polish Criminal Code. Pursuant to this provision, anyone who, in order to gain financial benefits, causes another person to disadvantageously dispose of his own or someone else's property by misleading him or by exploiting an error or inability to properly understand the action taken, shall be subject to the penalty of deprivation of liberty for a term of between 6 months and years. 8.

As a rule, the employee is entitled to remuneration for the work performed (Article 80 of the Polish Labor Code), which results directly from the employment relationship between the parties (Article 22 § 1 of the Polish Labor Code). Moreover, the employee may not waive the right to remuneration (Art. 84 of the Polish Labor Code). In the light of these provisions, it can therefore be assumed that the employee is entitled to remuneration because he has performed work.

Remuneration for work, however, is not due, in accordance with Art. 82 § 1 of the Polish Labor Code, for defective performance of products or services due to the fault of the employee. If, as a result of defective work due to the fault of the employee, there has been a reduction in the quality of the product or service, the remuneration shall be reduced accordingly.

What is more, the defrauded employer may seek to recover the salary paid as a consequence of the falsified CV, which, unfortunately, may involve filing a lawsuit. However, it is worth knowing that the employer, pursuant to Art. 88 of the Act of 23 April 1964 – the Polish Civil Code, has the option to evade the legal consequences of a declaration of will that was submitted to an employee under the influence of a mistake. For this purpose, the employer should submit a written declaration to the employee together with a request for the return of the paid benefit in the form of remuneration for work - in whole or in part.

In the light of Art. 78 § 1 of the Polish Labor Code, remuneration for work should be determined in such a way as to correspond in particular to the type of work performed and qualifications required for its performance, as well as to take into account the quantity and quality of work performed. It can therefore be assumed that if the employer had known about the lack of qualifications on the part of the employee, he would have set a lower salary or would not have employed the



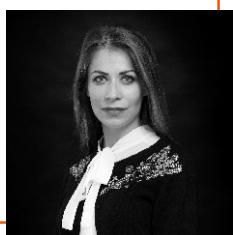
employee at all.

How should I deal with the personal data of unsuccessful candidates?

The period of storing personal data of candidates will depend on the result of a given recruitment. If a specific person is not selected, then there are no grounds for further processing of their personal data (application documents), therefore they should - as a rule - be removed immediately after the completion of this recruitment, unless the candidate has consented to the processing of such data on account for future recruitments for a specified period of time. In certain circumstances, however, and especially when there is a high probability that the unsuccessful candidate will pursue claims, referring to the alleged discrimination in the recruitment process, the employer may retain the personal data of such a candidate until the claims are time-barred, relying on his legitimate interest (Art. 6 (1) (f) of the GDPR). However, such a situation should be considered an exceptional and properly justified course of a specific recruitment.

It should also be remembered that the processing of personal data of candidates may be performed by employees who have the appropriate authorization to process them granted by the employer and related to their professional duties. They should also undertake to keep these data confidential. Only in the case of processing sensitive data, the confidentiality obligation does not have to arise from the content of the authorization, because it is a statutory obligation arising directly from Art. 221b § 3, second sentence, of the Polish Labor Code.

Written by:



Marta Rabe-Kozłowska

Attorney-at-law

TURCZA Kancelaria Radców Prawnych, POLAND
TURCZA.COM.PL



The Law Firm **Network**
FAR - REACHING LEGAL SOLUTIONS

A large, stylized blue globe is centered in the image. It is overlaid with a white network of lines and dots, similar to the logo. The globe is set against a background of classical columns, which are slightly blurred and in a dark, muted color. The text 'FAR-REACHING LEGAL SOLUTIONS' is written in large, bold, white capital letters across the center of the globe.

**FAR-REACHING
LEGAL
SOLUTIONS**

ARE EMPLOYEES PRIVATE DATA PROTECTED?

by Carla Martins Costa



In Portugal, although the major developments in Labor Law began in collective phenomena, it should be retained, especially in today's reality, that underlying the execution of an employment contract, there is an agreement of wills between individually considered subjects, the employer on the one hand and the employee on the other.

Despite the employer's apparent supremacy, through the years, the law has come to continuously increase a wider protection of employees' rights, namely personality rights, and data, including the enhancement of the right to information to and by the employee to the employer, leading to the question whether the employee is allowed to lie or omit relevant information to the employer and under what circumstances.

How do I handle the issue of background checks, including those involving sensitive personal data such as criminal records?

When checking the backgrounds of an employee, there are two moments and two types of employee data to be considered:

- Prior to hiring, and for the purposes of selection and recruitment: identification data, curricular data, family information, and sometimes criminal record data, psychological

profile data, and health data are processed.

- During the employment agreement: employee's data is processed to ascertain its productivity, health conditions, and compliance with the rules established by the employer.

As this data falls within the scope of constitutionally protected rights (right to privacy and right to personality), and in accordance with the principle of proportionality, its access must obey to three sub-principles: necessity (indispensability), adequacy (compliance with its purpose), and

strictu sensu proportionality.

In Portugal, the Labour Code prevents the employer from obtaining information from either the job applicant or the employee:

- on its private life, except when strictly necessary and relevant to assess its suitability; and,
- on its health or pregnancy, except when requirements related to the nature of the professional activity are justified, in which case the motivation must be reduced in writing.

In conclusion, access to sensitive personal data, for example, health, criminal record, religion, among others, can only be collected if personally provided by the employee and processed exclusively for the purposes for which they are intended, and under no circumstances may they be requested by the employer, except when strictly necessary and indispensable to the execution of the employment agreement.

Are there particular issues in checking candidates' social media profiles?

Given privacy of private life is protected, as is access to information related to it, it will be relevant to ascertain in the analysis, when evaluating the profile of candidates through social networks, whether the information that is collected compromises the candidate's access to employment or the maintenance of the employment agreement.

The employer, when accessing such information, even if it is of public access, will not be able to use it against the employee or candidate. If the employer uses the collected information on social media, it compromises the freedom of expression, religion, among others established in the law and Constitution.



Can I ask candidates about their Covid-19 vaccination status?

In Portugal, by law, the employer cannot for the purpose of admission to or continued employment, require to the applicant or employee to undertake or present medical tests or examinations of any nature.

In this regard, as vaccination against the COVID-19/SARS-CoV-2 virus is not yet mandatory, the employer cannot substitute itself for the Portuguese Government. By law, it is forbidden to question the employee or impose vaccination, either when hiring or in the maintenance of employment agreements, under the consequence of assuming an illicit and highly discriminatory behaviour, which constitutes a very serious misdemeanour.

Are employees entitled to lie or to omit information; if information is subsequently found to be false, what can I do?

The Labour Code foresees that the employee must inform the employer about relevant features for the provision of the employment activity, namely, his academic and professional training and qualifications, as well as his practical experience in the activity to be hired, in which situations the employee cannot lie and/or omit relevant information for the conclusion and/or maintenance of the employment agreement.

Parties must therefore act in accordance with the principle of good faith, which includes the duty to inform. However, it is understood that in exceptional situations, it is assumed that the employee may lie or withhold information if the questions addressed to him by the employer are unlawful, in which case he cannot terminate the employment agreement on the grounds of malice.

Regarding the right to lie by the employee, doctrine has been divided. One part considers it admissible in the pre-contractual stage, while the other considers it inadmissible. A converging point for both is the admission of the right to lie and/or omit during the execution of the employment agreement, only in case of unlawfulness of the questions placed by the employer.

In view of the above, and in the event of the employee omitting relevant information or providing false information during the employment

agreement, the employer may:

- declare the employment agreement null and void or voidable
- sue based on liability and of guilt in contrahendo
- initiate disciplinary proceedings that may lead to dismissal with just cause

How should I deal with the personal data of unsuccessful candidates?

In Portugal, the labour law foresees that the data recorded during the recruitment process, whether successfully concluded or not, must be kept on file for five years, thus allowing the inspection entities to verify the



employer's compliance with equality and discrimination regulations.

The above record must be made by gender separation and must contain the following information:

- A** Invitations to fill positions
- B** Job offers announcements
- C** Number of applications for curricular assessment
- D** Number of candidates attending pre-selection interviews
- E** Number of candidates awaiting admission
- F** Results of admission or selection tests or exams
- G** Social balances concerning data, which allow the analysis of the existence of possible discrimination against people of one of the genders in access to employment, professional training, and promotion, and working conditions.

Written by:



Carla Martins Costa
Attorney-at-law

Abreu & Marques e Associados, PORTUGAL
AMSA.PT

VISIT THE WEBSITE HERE



Legal issues relating to obtaining OF SENSITIVE INFORMATION OF A CANDIDATE EMPLOYEE

by **Natalia Vodolagina**



How do I handle the issue of background checks, including those involving sensitive personal data such as criminal records?

In case the work is not connected with the state authorities or with the commercial or sensitive secrets the background check of a candidate is made according to his education (confirmed by the diploma) and records of previous work. In Russia every employee has a work record book, which is now maintained either electronically or on paper. It contains records for all places of work of an employee, dates of employment, of termination of employment and reasons for termination of employment. Above that a special certificate is usually required from the candidate/onboarding employee. Such certificate can be provided to the employee by the employer at termination of employment. It shows the salary actually paid to the employee and all social security payments made for the employee.

In case a deeper check is needed (for example, where the employee will

have access to sensitive information, money etc.), a certificate of no criminal record can be obtained (issued by police). Obtaining of such certificate, however, takes 30 days.

Some positions require access to classified information (not only for service in state bodies; such access is required, for example when a private company is producing some categories of equipment for the state needs or constructs buildings for the state). In this case a relevant certificate (issued by the Federal Security Service) is to be provided by the candidate.

Are there particular issues in checking candidates' social media profiles?

Obviously, there are no restrictions for checking "open" social media profiles. Normally, a candidate would choose whether to open the access to the profile. Information obtained from such profile can be used for evaluation of professional competence of the candidate. A candidate cannot be refused for reasons (including sources from the social media profile) other than inconsistency with professional standards, no discrimination of any

type is allowed. E.g. poor moral qualities of a candidate may be the reason for non-employment where conformity to ethical standards is required by law (state civil service, police, judges, etc.).

In reality information from social media may be a reason for refusal to employ a candidate and such refusal will be difficult to challenge in case the non-employment is formally motivated by other grounds.

Can I ask candidates about their Covid-19 vaccination status?

At present in some cases the employer is obliged to check the COVID19 vaccination status and arrange the vaccination in case required by the law (e.g. medical service workers, teachers). Therefore, in these cases the question is legitimate. If there is no prescription of the law for an employee to be vaccinated (e.g. where a person is required to work from home), refusal to employ motivated by the candidate being vaccinated/non-vaccinated may be treated as a discrimination. The above conclusion is more of a theory since no case law regarding this issue has been elaborated by today.

Are employees entitled to lie or to omit information; if information is subsequently found to be false, what can I do?

Provision of forged documents at signing of the labour contract is the ground for termination of the labour contract by the employer. The same relates to provision of false information on incomes and assets where provision of such information is required by law (for employment in state bodies).

The provision of false information which relates to working skills of the employee may be checked during attestation. If in course of attestation the employee is found unsuitable for the position he is employed at, this is a ground for termination of the employment by the employer.

Therefore, provision of false information relating to the requirements for the job or qualification can have effect on the employment status.

How should I deal with the personal data of unsuccessful candidates?

For storing of personal data, a permit from the candidate needs to be obtained. All measures must be taken to protect personal data from unauthorized or accidental access to them, destruction, modification, blocking, copying, provision, distribution of personal data, as well as from other illegal actions in relation to personal data. Therefore, permits for personal data storage and processing of personal data when a candidate is interviewed. Regardless of whether the candidate is successful or not, such permit in writing should be stored by the employer.

Summary

The Russian legislation provides requirements to the employer for protection of personal data and sanctions against unauthorized use of such data. At the same time the interests of both parties are balanced and there are no excessive requirements or issues which would lead to regular abuses of rights by the employees.

Written by:



Natalia Vodolagina
Attorney-at-law

Westside Law Firm, RUSSIA
WSLAW.RU



VISIT THE WEBSITE HERE



Data Protection: THE RECRUITMENT AND ON-BOARDING STAGE

by **Maria Gomes Sousa**

How do I handle the issue of background checks, including those involving sensitive personal data such as criminal records?

In Spain, one of the novelties included in the Personal Data Protection Regulation is proportionality.

Personal Data may only be requested if it is strictly necessary for the provision of the intended service.

Therefore, the only case in which the employee may be asked for a negative criminal record certificate is if the job in which the service is to be provided is regulated by a specific regulation that makes it essential to have this certificate, for example, in jobs that involve dealing with minors or exercising a public function.

Are there particular issues in checking candidates' social media profiles?

The Spanish Data Protection Agency (AEPD) stresses that, even if it is publicly accessible, the company cannot search candidates' social media profiles and use the data thus obtained "if it does not have a valid legal basis for doing so". Similarly, it rejects companies sending out friend requests to their candidates in order to access the content of their profiles, or directly ask them to show the content they share with third parties in networks.

But when is there a legal basis? The AEPD considers that the investigation

would be justified if it is related to professional purposes. As a general rule, companies cannot review the digital activity of their candidates, but there are exceptions and nuances, one of which would be if the search on social networks serves to check whether the candidate meets certain qualities strictly related to the position. For example, if you are looking for an expert for a Communication or Marketing Department, it would make sense to check their Twitter account to see if they have the required communication skills

Can I ask candidates about their Covid-19 vaccination status?

Vaccination against the Covid-19 virus is not compulsory in Spain, which also applies to all other vaccines.

Vaccination is not compulsory in the workplace either, not even in the health sector (doctors, nurses), so it is not possible to dismiss a worker for not being vaccinated, nor can he/she be penalised. In these cases, in the event of dismissal, it would normally be considered unfair or even null and void, as fundamental rights could be violated in this process, such as the right to privacy. Nor would it be legal to keep a register of vaccinated and unvaccinated employees, as this is protected personal data that the employee is not required to communicate to the company. In the same way, a prospective employee cannot be asked whether he or she is vaccinated against the Covid-19 virus -

much less could this be made a condition of employment. This applies regardless of the inoculation status (first, second or third dose). The fact that a candidate is excluded from a job because of his or her vaccination status constitutes a violation of the right not to be discriminated against on the grounds of birth, race, sex, religion, opinion or any other personal or social condition or circumstance, as recognised in the Spanish Constitution, and also the right to privacy.

Are employees entitled to lie or to omit information; if information is subsequently found to be false, what can I do?

If the employee lies or omits information, the Company may apply the penalty regime stipulated in the applicable Collective Bargaining Agreement

How should I deal with the personal data of unsuccessful candidates?

Regarding the processing of unsuccessful candidates' personal data, the Spanish Data Protection Agency (AEPD) clarifies that the data may only be retained with the candidate's consent, unless the employer can demonstrate a legitimate interest. If this is not the case, the CV must be destroyed, and the personal data must be deleted and blocked.

Written by:



Maria Gomes Sousa
Attorney-at-law

Thomás de Carranza Abogados, SPAIN
TC-ABOGADOS.ES

VISIT THE WEBSITE HERE



DATA PROTECTION

of Employee Candidates in the Hiring Process

by Emre Gökhan Atayılmaz & Ertuğrul Aksoy



The purpose of this article is to give a brief summary of the privacy, data protection and data use in employment specifically in terms of hiring and on-boarding process under Turkish Labour Law ("Labour Law") and Personal Data Protection Law ("PDPL") from an employer perspective.

According to PDPL, personal data is defined as any information relating to an identified or identifiable real person. Data such as photos, identification information, phone numbers, e-mail addresses

will be considered as personal data and the storage process in question will be considered as personal data processing activity.

Companies are keen to collect more information about the employee candidate for evaluating whether he/she is the right person for the position. Even though PDPL provides no specific rules in the employment context, it is crucial to determine the rules for the processing of employee candidates' personal data by taking Turkish Labour Law,

Personal Data Protection Law and applicable legislation together.

How do I handle the issue of background checks, including those involving sensitive personal data such as criminal records?

Background check is a common way for a company to learn more about an employee candidate. In most circumstances, since the company can decide whether to enter into an employment contract with a candidate at the recruitment stage even without background check information, it will be arguable to consider that background check information of the candidate is necessary for conclusion of an employment contract.

Having said that, it should be underlined that, there is no law that



image: Freepik.com



specifically regulates conducting background checks on employee candidates. However, PDPL and the Labour Law should be taken into consideration when conducting these background checks. For background checks that concern the candidates' sensitive personal data such as health, criminal records, political opinions, association or foundation memberships or any other sensitive personal data, the candidates should be informed, and their prior consent is required. However, for background checks concerning the candidates' previous work experience, educational background or any other non-sensitive personal data consent may not be required.

By taking the above into consideration, it should be kept in mind that such records cannot be used for discriminatory purposes and in any case the employer must process the personal data lawfully ensure the security of the personal data, in accordance with PDPL and the applicable legislation.

Are there particular issues in checking candidates' social media profiles?

There is no specific regulation in relation to checking on candidates' social media profiles. Furthermore, to the best of our knowledge there is no court decision in that respect. Hence, the issue is not crystal clear. Nevertheless, PDPL and the Labour Law should be taken into consideration while determining the limits and methods of checking candidates' social media profiles.

In most cases, social media functions as an open area that is available for the

search on the potential employees including substantial information on their background. Hence, it is an encouraging subject for the employers when it comes to finding out the content and information provided by the candidates.

As for carrying out a search on the candidates' social media profiles, it is substantial to request the relevant information (i.e., social media profile information) directly from the candidates (via online application platform) unless it is provided by the employee on his/her CV. Hence, carrying out a search on the private information without the candidates' consent is not advisable. Carrying out a background search is arguable, if the employee's profile is not open and available for anyone checking it. We are of the view that in such a case, the employer should act prudently and refrain from carrying out a search.

In any case, information provided by candidates through social media platforms should not be used as a discriminatory tool when assessing the candidates during the recruitment process.

To be on the safe side we are of the view that the employer should ask for the consent of the candidate for carrying out on candidates' social media accounts. Nevertheless, the risk would be low in the event that candidates' social media accounts are open to the public.

Can I ask candidates about their Covid-19 vaccination status?

Yes, however, under PDPL, health data is deemed to be the sensitive personal

data. Therefore, an employer cannot ask whether its applicants have been vaccinated without having their explicit consent regarding the retention and processing of this health data.

However, it would be possible to ask the question if (but not risk free for an employer): (i) the question is asked and the data is collected on a completely anonymous basis, without it being possible to link the answers back in any way to the relevant applicants; and (ii) as long as it is made clear to the applicants that the question is being asked on this basis. However, there still remains a risk if someone could find out the relevant employee's identity; for example, by checking the employer's records.

Are employees entitled to lie or to omit information; if information is subsequently found to be false, what can I do?

During the recruitment process, the employer often requires the employee to provide certain information on the employee's skills and qualifications such as the employee's age, educational background, foreign language skills, work experience, etc. Accordingly, the employee should provide the relevant information which would constitute a part of the contract. The employee shall provide accurate information. Failure to do so would entitle the employer to terminate the employment contract unilaterally and rightfully.

Under Turkish Labour Law, an employer may terminate an employment contract with immediate effect (i.e.,



without a notice), provided that such termination is based on rightful reason. In such a case, employer is not obliged to pay a statutory severance pay or payment in lieu of notice.

In connection with the above, if the employee misled the employer by providing the employer with substantial information on his/her background and qualifications such as having a degree, ability to speak a foreign language etc. then this would cause a rightful reason for the employer to terminate the employment contract.

How should I deal with the personal data of unsuccessful candidates?

In principle, any personal data shall be erased, destroyed or anonymised by the controller, ex officio or upon demand by the data subject, upon disappearance of reasons which require the process unless otherwise

allowed by PDLP. The obligation of the controller is to erase, destroy or anonymise personal data in cases where the reason for processing disappears. It is not necessary for the data subject to separately apply for this.

The Data Protection Board ("The Board") has issued the Regulation on Erasure, Destruction and Anonymisation of Personal Data ("Regulation"). Under the Regulation, every data controller must prepare and put into force an internal policy for the erasure, destruction and anonymisation of personal data. This internal policy should create a regular monitoring system for the entire personal data kept by the data controller. Regular monitoring should be made at intervals of six months or less. At each monitoring session, the data controller must determine whether the legal grounds for keeping the personal data are still in place. If there is any personal data for which there is no legal ground for keeping, the relevant personal data must be erased, destroyed or anonymised.

In connection with the above, the employer can keep the details of unsuccessful candidates on file, provided that it complies with its duties in relation to the retention of personal data under the Turkish data protection legislation. There are no pre-defined general periods envisaged for the retention of specific categories of data. Thus, the main rules and principles set forth regarding data processing activities within the PDLP must be taken into consideration in

order to determine lawful retention periods for the processed personal data. In that regard, it is advisable to inform and obtain the consent of the employees for keeping their personal data to be used for potential hirings in the future.

Written by:



Emre Gökhan Atayılmaz
 Attorney-at-law
 PAE Law Office, TURKEY
 PAE-LAW.COM



Ertuğrul Aksoy
 Attorney-at-law
 PAE Law Office, TURKEY
 PAE-LAW.COM



OUR AUTHORS

  Pablo Nicastro ATTORNEY-AT-LAW (54 11) 4814-1746/8 goliva@bodlegal.com Av. Córdoba 1309 3ºA. Ciudad de Buenos Aires ARGENTINA	  Clara Fazio ATTORNEY-AT-LAW (54 11) 4814-1746/8 goliva@bodlegal.com Av. Córdoba 1309 3ºA. Ciudad de Buenos Aires ARGENTINA	  Eduardo Boccuzzi ATTORNEY-AT-LAW San Paolo Building Av. Bridadeiro Faria Lima 2055 – 10o Andar Sao Paulo, 01452-001 BRAZIL	  Gustaff von Baranow Murakami ATTORNEY-AT-LAW San Paolo Building Av. Bridadeiro Faria Lima 2055 – 10o Andar Sao Paulo, 01452-001 BRAZIL
  Kevin Xu ATTORNEY-AT-LAW +86 21 6113 2988 martin.hu@mhplawyer.com 7/F, Wheelock Square 1717 Nanjing West Road Shanghai, 200040 CHINA	  Craig Zhou ATTORNEY-AT-LAW +86 21 6113 2988 martin.hu@mhplawyer.com 7/F, Wheelock Square 1717 Nanjing West Road Shanghai, 200040 CHINA	  Jackie Gao ATTORNEY-AT-LAW +86 21 6113 2988 martin.hu@mhplawyer.com 7/F, Wheelock Square 1717 Nanjing West Road Shanghai, 200040 CHINA	 NIETO ABOGADOS Luis E. Nieto ATTORNEY-AT-LAW +57 1 3453663 (Ext - 108) luisnieto@nietochalela.com Calle 72 No. 5-83, Piso 2 Bogotá COLOMBIA
 NIETO ABOGADOS Manuela Chavarro ATTORNEY-AT-LAW +57 1 3453663 manuela.chavarro@nietolegal.com Calle 72 No. 5-83, Piso 2 Bogotá COLOMBIA	  Alice Mlýnková, Ph.D. ATTORNEY-AT-LAW +420 605 759 032 alice.mlynkova@ltapartners.com Anglická 140 120 00 Praha 2 CZECH REPUBLIC	  Soňa Macurová ATTORNEY-AT-LAW +420 605 759 032 alice.mlynkova@ltapartners.com Anglická 140 120 00 Praha 2 CZECH REPUBLIC	 SZECISKAY ATTORNEYS AT LAW Hédi Bozsonyik ATTORNEY-AT-LAW +36 1 472 3000 hedi.bozsonyik@szeciskay.com Kossuth Lajos tér 16 1055 Budapest HUNGARY
 SZECISKAY ATTORNEYS AT LAW Zoltán Balázs Kovács ATTORNEY-AT-LAW +36 1 472 3000 hedi.bozsonyik@szeciskay.com Kossuth Lajos tér 16 1055 Budapest HUNGARY	 Poovayya & Co. ADVOCATES SOLICITORS Siddhartha George ATTORNEY-AT-LAW +91 80 4656 3000 siddhartha@poovayya.net 121 Dickenson Road, Bangalore 560 042, Karnataka INDIA	 Poovayya & Co. ADVOCATES SOLICITORS Amit Kiran ATTORNEY-AT-LAW +91 99016 70055 amit@poovayya.net 121 Dickenson Road, Bangalore 560 042, Karnataka INDIA	 Poovayya & Co. ADVOCATES SOLICITORS Varnika Sharma ATTORNEY-AT-LAW +91 99016 70055 amit@poovayya.net 121 Dickenson Road, Bangalore 560 042, Karnataka INDIA
 Poovayya & Co. ADVOCATES SOLICITORS Bhumika Maheshwari ATTORNEY-AT-LAW +91 99016 70055 amit@poovayya.net 121 Dickenson Road, Bangalore 560 042, Karnataka INDIA	  Jonathan M. Streifer ATTORNEY-AT-LAW +62 21 5212038 jonathanstreifer@ssek.com 14th Floor, Mayapada Tower I Jl. Jend. Sudirman kav. 28 Jakarta, 12920 INDONESIA	  Syahdan Z. Aziz ATTORNEY-AT-LAW +62 21 5212038 jonathanstreifer@ssek.com 14th Floor, Mayapada Tower I Jl. Jend. Sudirman kav. 28 Jakarta, 12920 INDONESIA	 bhsm Richard Lee ATTORNEY-AT-LAW +353 1 440 8300 rlee@bhsm.ie 6-7 Harcourt Terrace, Dublin 2 IRELAND



bhsm

JJ McLoughlin
SOLICITOR

+353 1 440 8300
jjmcloughlin@bhsm.ie
6-7 Harcourt Terrace, Dublin 2
IRELAND



bhsm

Sinéad Mannion
ATTORNEY-AT-LAW

+353 1 440 8300
rlee@bhsm.ie
6-7 Harcourt Terrace, Dublin 2
IRELAND



COCUZZA & ASSOCIATI
Studio Legale

Domenica Cotroneo
ATTORNEY-AT-LAW

+39 02-866096
dcotroneo@cocuzzaeassociati.it
Via San Giovanni Sul Muro 18
20121 Milano
ITALY



COCUZZA & ASSOCIATI
Studio Legale

Jacopo Desimoni
ATTORNEY-AT-LAW

+39 02-866096
jdesimoni@cocuzzaeassociati.it
Via San Giovanni Sul Muro 18
20121 Milano
ITALY



mhp 君悦
LAW FIRM 律師事務所

Kevin Xu
ATTORNEY-AT-LAW

+86 21 6113 2988
martin.hu@mhplawyer.com
7/F, Wheelock Square
1717 Nanjing West Road
Shanghai, 200040
CHINA



W
WIERINGA ADVOCATEN

Kiki Manse
ATTORNEY-AT-LAW

+31 (0)20 624 68110
bink@wieringa.nl
Ijdok 17
Amsterdam, 1013 MM
THE NETHERLANDS



W
WIERINGA ADVOCATEN

Annemarie Buwalda
ATTORNEY-AT-LAW

+31 (0)20 624 68110
bink@wieringa.nl
Ijdok 17
Amsterdam, 1013 MM
THE NETHERLANDS



TURCZA
Kancelaria Radców Prawnych

Marta Rabe-Kozłowska
ATTORNEY-AT-LAW

+48 61 666 37 60
kancelaria@turcza.com.pl
ul. Grochowska 56
60-347 Poznań/Poznan
Poland



ABREU & MARQUES
ABOGADOS

Carla Martins Costa
ATTORNEY-AT-LAW

+351 21 330 7100
carla.costa@amsa.pt
Rua Filipe Folque, nr 2-4
1069-121 Lisboa
PORTUGAL



20 WESTSIDE
LEGAL SERVICES

Natalia Vodolagina
ATTORNEY-AT-LAW

+7 (499) 608 06 01
info@wslaw.ru
Office 303, «The Yard» Business Centre,
at No.11, bld.1,
1st Magistralnyi tupik
Moscow, 123290
RUSSIA



THOMÁS DE CARRANZA
Abogados

Maria Gomes Sousa
ATTORNEY-AT-LAW

(+34) 91 310 66 60
maria.gomes@tc-abogados.com
Paseo de la Castellana,
116, 9ª Planta, 28046 MADRID
SPAIN



PAE

Emre Gökhan Atayılmaz
ATTORNEY-AT-LAW

+90 212 351 88 86
emre.atayilmaz@pae-law.com
Ebulula Mardin Cad. Akatlar Maya Sitesi
PAE Binasi Z Blok
Akatlar Istanbul 34335
TURKEY



PAE

Ertuğrul Aksoy
ATTORNEY-AT-LAW

+90 212 351 88 86
info@pae-law.com
Ebulula Mardin Cad. Akatlar Maya Sitesi
PAE Binasi Z Blok
Akatlar Istanbul 34335
TURKEY



PAE

Ramazan Burak Karagöz
LEGAL TRAINEE

+ 90 212 351 88 86
info@pae-law.com
Ebulula Mardin Cad. Akatlar Maya Sitesi
PAE Binasi Z Blok
Akatlar Istanbul 34335
TURKEY



BLANDY & BLANDY
SOLICITORS

Laura Binnie
ATTORNEY-AT-LAW

0118 951 6939
laura.binnie@blandy.co.uk
One Friar Street, Reading RG1 1DA
UK



LFINGLOBAL.COM

TRENDSTM
LEGAL MAGAZINE