



Privacy protection in the workplace

Guide for employees

Privacy protection in the workplace

Privacy protection in the workplace



This publication was developed as a result of the Leonardo da Vinci Partnership Project "Raising awareness of the data protection issues among the employees working in the EU" (2012-1-PL1-LEO04-28097 1). The project has been funded with support from the European Commission under the Lifelong Learning Programme.

The guide "Privacy protection in the workplace. Guide for employees" is the result of an international cooperation of experts representing four Data Protection Authorities:

- Bureau of the Inspector General for Personal Data Protection from Poland
- Office for Personal Data Protection from the Czech Republic
- Croatian Personal Data Protection Agency
- Commission for Personal Data Protection from the Republic of Bulgaria.

This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

For non-commercial purposes, a download version of this publication is available at the websites of the partners' Data Protection Authorities.

TABLE OF CONTENTS

	Introduction	5
1.	Job search	7
1.1.	Data necessary for the recruitment procedure	7
1.2.	The importance of consent	8
1.3.	Purposes of job applicants data processing	9
1.4.	On-line job search	10
1.5.	Employment Agencies	11
2.	Recruitment procedure	13
3.	Employment period	15
3.1.	Specific issues connected with data processing during the employment period	15
3.2.	Right of access to information vs. right of personal data protection	17
3.3.	Disclosure of information to the public for raising professional and institutional image	19
3.4.	Sensitive data which the employer is (not) supposed to process	19
3.5.	Utilisation of internal telecommunications resources	20
3.6.	Supervision techniques and methods applied by employers	22
4.	Data protection and termination of the employment relationship	26
4.1.	Processing former employee's data	26
4.2.	Transfer of personal data between the former and the present or potential employer	27
4.3.	E-mail, mobile phones and other electronic devices containing personal data	27
4.4.	Termination of the employment relationship by court decision and data processing	28
5.	Employees rights and supervisory authorities as a helping hand	30
5.1.	General right of employees	30
5.2.	Supervisory authorities as a helping hand	32
	Glossary of terms	35
	Data protection authorities involved in the project	37

INTRODUCTION

The publication “Privacy protection in the workplace. Guide for employees” was developed as a result of international cooperation between four European data protection authorities from Poland, the Czech Republic, Croatia and Bulgaria in the frame of the Leonardo da Vinci partnership project “Raising awareness of the data protection issues among the employees working in the EU” (No 2012-1-PL1-LEO04-28097 1).

Nowadays, personal data are of a great economical value, which can be measured in billions of Euro. Collection, analyzing or transferring of data to other entities within the country or abroad has become a big business, where personal data are the main product. That might be also your data. This is why it is important to know whom you are sharing your personal data with and what is going to happen to all your data.

Therefore, in this publication we tried to compare the different practices implemented in our partner countries and find the general rules which might be common for all or most of the EU countries in the field of data protection from the point of view of a natural person searching for a job or being employed in one of the EU countries.

This publication is targeted to people searching for a job or working in the public or private sector. Bearing in mind that employment in the civil service is under specific regime in every country, the information in this chapter applies to civil servants to the extent that national regulations do not stipulate otherwise.

This publication covers the whole employment period – from job search, through interview, up to the employment relationship itself. It also deals with issues like processing of personal data of former employees as well as the employees’ rights and the role and powers of data protection authorities. At the end, you will find a brief glossary of terms comprehensively explained. The guide provides general principles and rules on the European labour market, but gives attention to important differences in particular EU Member States.

We hope that this guide will enable you to get a coherent view of data protection rules applicable in the employment area, of obligations for the employers and other stakeholders like recruitment agencies, as well as information for data subjects (employees, former employees, job seekers) about their rights and methods of their application. We believe that this publication will become a useful tool for all interested parties.

1. JOB SEARCH

Although data protection regulations in all EU Member States share the same fundamental principles, still specific solutions adopted by each Member State may differ to some extent. For that reason if you plan to look for employment in the European Union, you should also think of becoming familiar with the basic provisions on personal data processing being in force in your future employer's country. Remember, no matter whether you are looking for a job on your own or using the services of employment agencies, you have the legal right to have your personal data protected.

1.1. Data necessary for the recruitment procedure.

Job search, regardless of the method, always involves disclosure of your personal data to various entities and institutions which receive your job application. During this process only data which are necessary for the recruitment procedure should be disclosed. It means that such data should be essential and adequate for the purpose of making a decision on hiring a new employee. In other words, it is unacceptable for the potential employer to require from job seekers too much data or data irrelevant for making recruitment decision, as well as data that are too invasive (disclosing too much), when it is possible to get the necessary information with lesser interference in job seekers' privacy.

What data should I include in my CV?

As a rule people include in their CVs personal data that may be classified as: 1) identification data (name, surname, date of birth); 2) contact data (address of residence, phone no., e-mail address); and 3) information on education, skills, experience and employment history (graduated schools or studies, completed trainings and courses, previous employers, official positions and job descriptions). In general the decision on what specific information should be in your CV is up to you. It is advisable, however, to avoid including in it unnecessary data, which are not relevant for the recruitment procedure (e.g. information on marital status, national personal identification number or tax number, irrelevant interests and hobbies).

Are there any data that your potential employer is not allowed to ask for?

Potential employer cannot require disclosing personal data to the processing of which he has not legal basis (when there are no provisions entitling him to collect such data¹) as well as personal data which are inadequate or unrelated to the purpose of their processing, i.e. making a decision on employing a person (e.g. information on marital status, on your children and on planned children, sexual orientation, previous wages, religion, beliefs, political preferences).

¹ Persons who are looking for job in Poland will find such legal regulations in Article 22¹ § 1 of the Labour Code (Journal of Laws of 1998.21.94 – unified text).

What can I do if the scope of data I am required to disclose is in my opinion too extensive?

If your future employer demands from you to fill in job application form, he should always inform you whether the answers to questions contained in this form are obligatory or voluntary (e.g. he may mark them with an asterisk). If they are obligatory, he should also point out legal grounds for this. On the other hand, you may refuse to disclose such information, if he cannot legally justify his demands or gives you no answer to the above questions.

Where should I search for the information about the processing of my recruitment data?

Every data controller to whom you disclose your personal data (e.g. company that you want to work for, employment agency) is obliged to provide you with the following information:

- his identity (full name and address of its seat),
- the purpose of data collection,
- data recipients or their categories, if known at the date of collecting,
- your right of access to your data and the right to rectify them,
- whether the replies to his questions are obligatory or voluntary, and in case of existence of the obligation - about its legal basis.

The information should be clear and easily accessible (e.g. in a job offer or on the data controller's website).

The same principles shall also apply during job interview. If you have doubts as to why the potential employer demands you to give him certain personal information, do not be afraid to ask questions.

If you are looking for a job in an EU institution or agency you can find all the above information and more in "Specific Privacy Statement on personal data protection within the framework of an open competition" available on the website of European Personnel Selection Office.

Should I respond to Internet job offers where there is no information about the employer and just his e-mail address is available?

No. Employer who is collecting data of job applicants (CVs, cover letters, application forms) is obliged to identify himself.

1.2. The importance of consent².

Consent is one of the legal bases entitling the data controller to process data related to the person who gave the consent. It can be expressed in oral or written form. Some companies may require including in CVs consent for the purpose of data processing during recruitment. But generally, if you are sending your CV directly to your potential employer in response to his particular job offer, you can but do not need to explicitly express in it your consent to data processing. However, there are situations where such consent might be necessary.

² For the definition of consent see the glossary of terms.

In what situations is it advisable to include in my CV consent to personal data processing for the purpose of recruitment?

It is advisable to give your consent to future data processing, if you want the potential employer to keep your CV and use it in case of future recruitments. Otherwise, data controller may be obliged by the national law or national data protection regulations to destroy your CV when the job offer you have applied for becomes unavailable. Remember that it should always be clear that your consent concerns general approval to enter your personal data into employer's database for the recruitment purposes. Another situation where the consent is required is when you are using the services of employment agency and you want to register in the agency's "job-hunters database" (if the agency has no other legal basis to process your personal data). In such case you should always give the agency your consent to personal data processing. Also if you want to disclose your sensitive data³ (e.g. concerning your health) to your future employer, your explicit consent to their processing is necessary, provided that he has no other legal basis to do so. It is important to know that in some countries, like Poland, consent to the processing of sensitive data has to be expressed in a written form.

How should the consent look like?

Every consent should contain answers to the following questions: what data it concerns, who is allowed to process these data and for what purposes. It is good to know that your consent can have a time limit.

Examples:

"I hereby give X my consent to process personal data included in my CV strictly for the purpose of assistant manager recruitment – job offer no. ABCD."

"I hereby give X my consent to process my personal data, including sensitive data, disclosed in my job application for the purpose of recruitment over a period of one year."

"I hereby give X my consent to process personal data included in my CV for the purposes of its current and future employees recruitment procedures."

"I hereby give my consent for my personal data listed above to be entered in the database of the Employment Agency X and processed by the Agency for the purpose of providing me with employment search related services."

Can I withdraw my consent?

Yes. You can withdraw your consent to personal data processing for the purpose of recruitment at any time! If you decide to do so, data controller (e.g. company to which you applied for a job) will be no longer authorised to use them for that purpose. In this case your data (e.g. your CV and cover letter) must be erased or destroyed unless applicable national law provides otherwise.

³ For definition of sensitive data see the glossary of terms.

1.3. Purposes of job applicants data processing.

Potential employer should use job seekers data only for the purpose of making a decision on employing a person. If this purpose is no longer present, he has to erase or destroy the data. He is not allowed to use the data from their CVs for the purposes other than recruitment, for example for direct marketing.

1.4. On-line job search.

Collecting data over the Internet is nowadays one of the most popular methods of database creation, often used also in the process of employees recruitment. If the potential employer decides to collect job seekers data over the Internet (for example through his official website or by e-mail), he should implement technical and organisational measures to protect them, appropriately to the risks and category of data being protected. This obligation also applies to data controllers other than potential employers e.g. owners of websites where you can post your CV or employment agencies. Regardless of the method of personal data collection, every data controller has to comply with provisions on personal data protection.

What kind of websites should I use to transfer my personal data?

First of all, use only reliable and trusted websites. Remember, personal data contained in your CV disclose a lot of information about you, so they should not reach unauthorised persons. Therefore, do check if the website or e-mail address that you are about to use is the one officially recommended by the company that you want to contact. Always check who is the data controller and make sure that the transfer of data on the website used by you is made by means of secure encrypted connection (search for the https address line of the website in your browser).

What should I consider before uploading my CV on-line?

There are 4 basic rules:

1. Remember that uploading your CV on-line may require setting up your user account as well as expressing consent to the processing of personal data by the website owner. Before doing this you should always carefully read the networking site's regulations and privacy policy⁴. For it may turn out that the site owner is going to use your data also for his own or other entities' marketing purposes.
2. Include in your CV only data that are relevant and necessary for the recruitment procedure.
3. Keep in mind that by uploading your CV on the website you are making your personal data accessible to unlimited number of users. Such data disclosed on the Internet may be used in a way which not necessarily meets your expectations (identity theft, spam, phone marketing). Remember that even if you remove your CV from the website it will still be present in the search engine's archives. For that reason search for services which offer you a possibility to upload

⁴ Site's regulations contain provisions concerning the site's services as well as the duties and rights of the site owner and its users. Most of sites have also so called "privacy policy", a document that provides you with the information on the protection of your personal information.

your CV on their websites in an anonymous form (without giving your identification and contact data) – you may choose an employer whose offer is of interest to you and disclose him your detailed personal data.

4. Always check default privacy settings on a website which you are using for job search. Many websites provide their users with the possibility of adjusting them individually.

1.5. Employment Agencies.

If you are afraid of searching for a job in the EU on your own, you may turn to one of employment agencies to assist you in choosing an appropriate profession or place of employment. Employment agencies can provide you with services such as: career counselling, job search or temporary employment, therefore they can be treated as one of job search channels. This means that if you want to use their services, they will collect and process your personal data as data controllers.

What type of personal data may be collected by an employment agency?

In general employment agencies can collect the same type of your personal data as employers do for the purpose of recruitment. Data processed by employment agency always should be necessary and adequate for the purpose of their processing.

Do I need to give my consent to data processing by an employment agency?

Yes, if the agency has no other legal basis to process your personal data (e.g. in the country of its seat there are no legal provisions permitting the agency to process job seekers' data). It can be withdrawn at any time!⁵

For what purposes can employment agencies use my data?

Employment agencies can use your data for the purpose of providing you with employment search related services of your choice (e.g. career counselling, trainings, job search assistance).

Can employment agency transfer my data to potential employers?

Transfer of data is also data processing. Therefore, employment agency can transfer your data to some other entity (e.g. national or foreign companies searching for employees), only if there is a legal basis for such action (i.e. agency has your prior consent). Every employment agency that collects your data should inform you on data recipients known at the date of collecting or their categories.⁶

⁵ More information and consent examples in the Chapter 1.2.

⁶ See also the problem: "Where should I search for the information about the processing of my recruitment data?"

Recommendations

1. Avoid including in your CV data which are not necessary for the recruitment procedure.
2. Remember that you have the right to refuse disclosing data if there are no legal provisions obliging you to do so.
3. Give your explicit consent in case: 1) you want your data to be processed for the purpose of future recruitment procedures, 2) you are using assistance of an employment agency, 3) you are disclosing your sensitive data for the purpose of recruitment.
4. Remember that you can withdraw your consent at any time!
5. Make sure that you have information on the processing of your data and the data controller before you disclose your personal details.
6. Use only reliable and trusted websites for on-line job searching.
7. Think of the data security before posting your CV on the Internet – once uploaded CV stays on the Internet, even if you remove it from the specific website!

2. RECRUITMENT PROCEDURE

During recruitment your potential employer may want to contact you in person to verify your work experience and check if you are the right person for the job (e.g. during interview, psychological test or test of knowledge). During this process also your personal data are being collected.

What data can be collected during job interview?

During job interview employer may go into detail on information from your CV. Nonetheless, job interview should always relate only to issues relevant to the work at the defined position. All persons applying for a job have the right to be treated equally regardless of gender, age, beliefs and other personal characteristics. Remember that you have the right to refuse a reply to questions which embarrass you or violate your right to privacy or even personal dignity (e.g. concerning religion, political beliefs, marital status, private life, sexual orientation, maternity and family expansion plans).

However, there are situations in which the employer has the right to ask intrusive question (e.g. in Poland women may be asked whether they are pregnant if work they intend to take is not allowed for pregnant women due to the protection of maternity and persons who apply for a position of a public school teacher can be enquired about having criminal records for an offence due to intentional guilt). In general, the obligation to provide such information should result directly from legal provisions.

Can my potential employer contact my former boss and ask about me?

Some employers may want to collect information on job applicants by contacting their previous employers. However, this should not happen without the applicant's consent. If the potential employer wants to get information about you related to your previous job, he can ask you for references. He may also make use of the information contained in your certificate of work.

What should I know about psychological tests?

Psychological test is a method of psychological evaluation of the candidate used by employers in order to find the most suitable person for the job. Such test also allows the employer to obtain the information which the candidates would not willingly give or which they wish to hide. Therefore, use of psychological tests during recruitment raises a lot of controversy as some of them may reveal not only information on candidates personality traits but also other information that employer should not have. For example, the results of these tests can expose information about candidate's health, his or her views, information from private life and other details. That is why they should be conducted by a psychologist in a professional manner and with regard to professional confidentiality. Also you should be aware of the exact purpose of the study and the extent to which it will interfere in your privacy, and who will have access to the results of the study. Admissibility of psychological tests is treated differently by the laws of individual states. In some countries possibility to examine job applicants by means of psychological test needs to be stipulated in legal provisions. In others the employer must get your permission to conduct research and to inform you of the possibility to refuse to participate in the test.

What is an on-line background search?

Internet and social networking sites are a huge temptation for employers who may this way obtain additional information on job applicants, which they could not officially ask for during recruitment procedure. Keep in mind that even in situation when the employer cannot officially use information obtained thanks to viewing your profile on the networking site or tracking your posts on Internet forum, this information may in practice determine his decision on (not) hiring you. Therefore, it is good to know that you can influence the information that people may learn about you on the Internet. For example, search engines usually offer possibility to delete information about you from search results. However, the most important is to think twice before publishing your private data on the Web. Remember that the way you protect your privacy on the Internet is up to you.

What happens to my personal data if I fail the recruitment procedure?

The data controller has no right to process personal data longer than necessary for the achievement of the purpose of the processing. Therefore, after termination of the recruitment procedure the employer should immediately destroy all applications lodged by candidates who have not been successful (failed the recruitment procedure), regardless of the fact whether they were invited to interview or not. Situation where you expressed consent to the processing of your personal data for the purposes of future recruitment procedures is an exception to the above rule. Basing on your consent the employer can keep your application documents and use them any time he carries out recruitment for the positions relevant to your qualifications.

Recommendations

1. Remember that questions asked by the employer should only relate to issues relevant to the work at given position. You always have the right to refuse a reply to questions which embarrass you or violate your personal dignity.
2. Before taking part in psychological recruitment tests make sure that their conduct is permitted by the Member State's national law. You can refuse to give your consent to participation in such tests.
3. Be aware that your private data shared on the Internet might be misused during the recruitment procedure.

3. EMPLOYMENT PERIOD

In the framework of the labour relationship there is an inevitable need for exchange of information, which is not always of professional nature. This need sometimes arises from the provisions of the national labour legislation and sometimes from the specificities of the professional activity and the interests of your employer. Whether this is legal and lawful should be assessed in every concrete case. Your privacy in the employment period is not absolute. On the contrary, the processing of your personal data does not always depend on your consent.

Labour legislation contains relatively few rules determining the borders of the control exercised by the employer and the cases when the line defining your privacy is crossed. A good practice for employers is the implementation of privacy security policy, which should be transparent and available for the employees at all times. This policy should stipulate: the types of personal data of employees that are collected and further processed, the purposes for this processing, persons (including employees) who possess authorised access to them; information whether the submission of data is voluntary or compulsory and what the consequences in case of a refusal are; the storage period; methods for data erasing after the expiration of the storage period; the rights of employees in the sphere of data protection; possible transfers of data to other countries and information as to why it is necessary; the contact details of data protection official (if there is one).

3.1. Specific issues connected with data processing during the employment period.

Along with establishing employment relationship certain rights and obligations of employer and employee are being created. Their fulfilment begins with the conclusion of an employment contract and it may involve processing of personal data of the employee.

3.1.1. Conclusion of an employment contract and employee's work file.

Conclusion of an employment contract initiates the creation of an employee's work file. It contains the documents needed for concluding and performing a contract. Some of them are submitted by you, others are issued by the employer. Some of them contain your personal data, for example a copy of personal passport or other identity document or education certificate.

The concrete information that is contained in the work file is specified by the respective national legislation.

Are employers allowed to copy my identity card when hiring me?

It depends on the relevant national legislation of the employer. Usually, there is no legally grounded necessity for the employer to make a copy of your identity card, because your identity card contains some information not related to the performance of your work. You have the right to object to having your identity card copied unless the employer is able to prove the presence of legal grounds concerning the particular case.

Is it necessary for information related to my personal life to be stored in my work file?

Your work file might contain only information connected with labour relation. However, your work file may contain data related to your personal life, too. Usually, you are the one to submit these data in order to exercise certain rights and to allow the employer to fulfil certain obligations. The leave for execution of civil, public and other obligations (marriage, blood donation, death of a relative, court subpoena etc.) serves as an example.

What is the time limit for storing of my personal data on behalf of the employer?

The employer may store your personal data only for a period envisaged by the national legislation (e.g. according to the Polish law employee's personal file should be kept for the period of employment and also for 50 years from the date of termination of the employment relationship while in the case of payroll storage term is 50 years from the date of its drawing up). After the end of this period the employer has to erase your personal data

3.1.2. Disclosure of and access to personal data in the employment context.

Your personal data are confidential and cannot be disclosed and accessed without your explicit consent or a legal ground. Your data can be made available to two groups of people: employees working for your employer who have been explicitly authorised to access such data and external subjects, in case there is a legal ground for such disclosure.

Who has access to my work file within the organisation that employs me?

Access to your data within the organisation you work for may have employees whose professional obligations necessitate data processing and are duly authorised by your employer (for instance your senior employee, the human resources units, financial units etc.).

What external subjects may have access to my personal data?

The employer is obliged not to disclose personal data related to the employee to third persons. Access can be granted only when the employer is obliged by law to submit the data to the respective public authorities or such data have been duly required by the competent authorities (for example in cases of financial audits or labour inspections); when you have explicitly consented to disclosing your personal data to a concrete third person; or in any other cases provided for in the national legislation (for instance in a court case for protection of the legal rights and interests of the employer).

3.1.3. International transfer of personal data.

In the present globalised world, where we witness increased exchange of information and human resources, transfer of your personal data to other countries is necessary more and more often. The reasons for this transfer may vary. Transfer of data is usually carried out within multinational companies (between the head office and the affiliates) for globalisation of certain volume and type of data processing or by the power of an outsourcing contract.

Is the transfer of data inside the European Union subject to permission by the Data Protection Authority?

No. The transfer of data from an employer to another entity (other branch of private company, a state authority etc.) in the European Union and the European Economic Area is free and no permission by the national data protection authorities is needed. Whereas data transfer to a third country may require in some situations permission from the respective data protection authority⁷.

Is my consent to personal data transfer always needed?

No. There could be other legal bases for the transfer, e.g. when the employer needs to fulfil his obligations resulting from the labour legislation or has any other legal title for the purposes of human resource management when the transfer is necessary for the performance of a contract between employer and employee, also in cases when there is a necessity for investigating crimes, etc. However, when it comes to the transfer of employees data to a third country employer is obliged to have the legal basis not only for the transfer in general but also for transferring those data to an entity situated in a third country. It is advisory that you are notified prior to the execution of the data transfer.

What information about the transfer of my personal data am I supposed to receive?

It is a good practice that the individuals whose data are transferred are informed prior to the data transfer about the volume and type of data to be transferred, the purposes of this action, the recipients of data as well as their rights concerning data protection including their right to object to the processing of incorrectly collected data related to them and the right to ask for their deletion. This information should include reference to the level of data protection in the country of transfer destination if data will be transferred to a third country.

When is it permitted to transfer sensitive data?

The so called "sensitive data" may be transferred in case there is a need for exercising specific rights and obligations of the employer or there is an explicit consent of the respective employees. You should be informed about transferring these data.

3.2. Right of access to information vs. right of personal data protection.

The right to personal data protection is not an absolute right⁸, thus there are derogations in its application, which must be always laid down by law. For instance in case you hold a post as a public official, it is acceptable for some of your personal data to be made public in connection with the right of access to public information by other individuals. In such situations the balance between data protection and the right of information must be observed in keeping with the principle of proportionality⁹.

⁷ Third country – a country that is not a member of the European Union or the European Economic Area.

⁸ Absolute rights apply to all subjects and don't fall under any restrictions.

⁹ The principle of proportionality means a balance between two competing rights, in which case neither has preponderance.

Are the personal data of all employees equally protected?

The level of privacy protection for the persons performing public functions is lower. In respect to these individuals the principles of transparency and accountability are applicable, which do not apply to other individuals. Example of the lower level of protection for the personal data concerning some of them is their obligation to publicly declare their income, property owned, assets, deposits or other protected data in order to prevent the conflict of interest.

Is my consent to disclosing personal data necessary in case the access request is based on the respective Access to Public Information Act?

The European legislations do not provide an explicit answer to this question.

The legislation in some states (like Bulgaria) stipulates that if any given information falls within the category of public information and personal data at the same time your consent is necessary. In case of dissent the information must be released in a way not allowing for the disclosure of your personal data. In other countries (for example in the Czech Republic) consent is not always needed, especially if the personal data belong to individuals well-known to society and disclose information about their public or official activity.

In which cases are my personal data accessible?

In case you are an individual who is a person performing public functions your consent is not necessary to revealing personal data. Examples include:

- Data on your position within the organisation – such information, despite being related to you, is relevant to you in your role as an officeholder;
- Data on the number, goals and longevity of business trips undertaken by you – these are data related to the execution of working obligations;
- Data about the members of commission in a public body – this information does not include identifying data connected with the private life of the data subjects, but merely exposes their working capacity;
- Information on the declared property and income – high ranking public officials have the legal obligation to annually declare their property and income, which comes as an anti-corruption measure;
- Information on the educational and qualification status of high ranking officials and any other information which is a precondition for taking up a public post – instances include ministers, deputy ministers, secretary generals, members of the political cabinets of ministers, members of the local government. This information is needed for forming an opinion as to whether a given member of the political team possesses the necessary academic and professional qualifications for effective implementation of the respective policy.
- Any other information which is connected with the public position and related functional responsibilities or spending of public money.

3.3. Disclosure of information to the public for raising professional and institutional image.

In the process of their everyday work public and private employers make public a certain amount of information about themselves and you. This represents a normal process of disclosure of information with the aim of assuring transparency in the relations with customers/clients and raising their awareness about the way a particular public authority or private company functions. It is generally accepted that the information published by the employer (for instance on the company's website) about the managerial team or the employees belongs to them in their official capacity. For instance a good practice is publishing contact details (work e-mail address and telephone number) of certain employees with the aim of facilitating the contact of external users with the respective public authority/private company. Publishing photographic material for work-related events (e.g. conferences) is a part of the corporate or institutional image of the respective organisation. Publicity is expected in respect to the persons performing high public functions as in the cases of publishing the curriculum vitae of such persons on institution's website.

Apart from a sign of transparency the necessity for disclosing information related to you may stem from a legal provision. For instance Bulgarian legislation requires a list containing the names of the employees who have filled in declarations according to the Conflict of Interest Prevention and Ascertainment Act, to be published on the websites of public authorities.

All these examples of information disclosure are a result of the official capacity of employees and do not represent infringement of their privacy, because they are inextricably bound up with exercising their professional activity.

3.4. Sensitive data which the employer is (not) supposed to process.

The European data protection legislation generally prohibits the processing of personal data which contain information about the race, religion, political or philosophical beliefs, trade unions membership, sex life and orientation and medical condition. The employer has the right to process such data if this is required for the fulfilment of certain rights and obligations in the sphere of labour legislation which are explicitly expressed in the law. Another legal title which in some specific cases allows the processing of such data might be your consent.

For exercising certain privileges you should inform your employer about certain sensitive data. The examples include:

- extra time off for trade union activities;
- utilisation of the authorised leave in particular days for religious holidays, if the religion in question is not the official state religion;
- the employer is obliged to release from work pregnant employees and employees who are in the advanced stages of the in vitro treatment and need to undergo medical examinations (for example in Bulgaria).

Labour legislation provides for different rights of special protection and integration for disabled individuals. If you are disabled, it is in your interest to submit official documents proving your medical condition in order to exercise the rights which have to be granted by the employer.

Is it necessary that my employer receives medical information about me?

The employer has the right to get acquainted with general information on your medical condition when it is necessary for the fulfilment of the obligation of labour safety and observance of the labour and insurance legislation. The employer and any person processing medical information is obliged to provide adequate protection measures¹⁰ of personal data from unauthorised access and abuse.

What documents connected with the social security and health insurance and containing medical information am I obliged to present for receiving compensation?

The leave due to temporary disability is verified with a patient's chart extract, affirmed by the competent authorities and containing data about your medical condition. The patient's chart extract is presented to the employer in case you are absent due to illness for the purpose of receiving compensation.

3.5. Utilisation of internal telecommunications resources

Take into consideration that you should use the internal corporate resources in accordance with the internal rules adopted by the employer. Your employer has the right to check, in an adequate way, whether you fulfil this requirement. Despite this your employer does not have the right to infringe your privacy in the workplace (for example by monitoring phone calls, tracking e-mails or checking mail deliveries addressed to you) without a serious reason connected with the nature of your work.

3.5.1. Monitoring of the Internet and work e-mails.

Nowadays, the utilisation of the Internet and e-mail has become an inseparable part of the work obligations. It is important to know the boundary between privacy and the fulfilment of work duties.

Could my e-mail address be personal data?

There is no unified European practice on this question. In most cases it is generally accepted that the e-mail represents personal data if it contains information which are or might be connected with an individual e.g. John.Smith@cpdp.bg. In Bulgaria e-mails are considered personal data only in combination with other personal information identifying specific person.

Is the monitoring of my work e-mails and Internet access on behalf of the employer processing of personal data?

Monitoring e-mails and Internet use on behalf of the employer unavoidably includes personal data processing. Privacy and data protection do not end on the border of workplace. E-mails and electronic communications benefit from the same protection of fundamental rights as paper mail. In the course of your working life you develop relationships with the outside world. It is hard to distinguish clearly which activities form part of your professional or business life and which fall to your private life, too. For this reason it is accepted that e-mail and Internet access monitoring in the workplace is indeed personal data processing.

¹⁰ Adequate measures depend on the national legislation.

Should I be notified by my employer about possible surveillance and monitoring of work e-mails and Internet access?

In some countries, like Croatia and the Czech Republic, employers have to notify their employees about surveillance and monitoring of work e-mails. In other countries like Bulgaria and Poland this is not stipulated by law, but it is a good practice for employers to implement policy of transparency in regard to their employees. When hired you need to be introduced to the internal rules of the organisation and to be informed of possible monitoring of your work e-mails and Internet access. You have to be informed about the following issues: whether you can use private e-mails during working hours and under what conditions and work e-mail address for private purposes; what the procedure for opening your e-mails in case of prolonged absence is; if you can access the Internet in the working hours, the technical and organisational measures for personal data protection undertaken by the employer.

Is my employer allowed to restrict the Internet use in the workplace?

Yes. The employer has the right to control and arrange the computer systems and Internet access in a way that best suits him. The employer is also interested in assuring that you spend as much time as possible on the execution of your duties, and not on social networks or net browsing for private purposes. This allows for the restriction of certain websites – such as social networks (Facebook, Twitter, G+) or applications (Skype). This restriction needs to be addressed in the so called rules on the internal working order. Employees have to abide by the restrictions which form a part of the internal rules and are duly presented to them (for instance when they constitute a part of the employment contract). Thus in respect to using the Internet the employer should explicitly inform you about the conditions allowing for using the net for private purposes and the types of materials and webpages whose use is prohibited. You should be aware of the systems used for monitoring and control, as well.

However, it is advisable that the employer places emphasis on the prevention of Internet abuse rather than on monitoring the employees' access. Prevention includes technical measures restricting the access to websites specified by the employer.

Is the employer allowed access to my private e-mails without my authorisation?

No. Private electronic communication (e-mail, sms, chat history) represents correspondence and its secrecy must not be compromised, as long as there is no court decision stipulating the opposite. Privacy of communication is a constitutionally recognised right in Europe. If the employer violates the privacy of communication, he is subject to penalty according to the criminal law. In case the violation has been committed in the official capacity of the employer, then the law provides for even more serious penalty. The matter for the control of correspondence is decided by its nature: in case it is of private nature any interference by the employer or any other individual is illegal.

Is my employer allowed access to my work e-mails without my consent?

Yes, in order to protect certain rights and interests, provide for efficient flow of the work process and to protect himself from possible illegal actions of employees the employer is allowed access to your work e-mails. However, in such cases there must always be a balance between the interests of the employer and the right to privacy of the employees. There are several recommendations in cases when such monitoring activities are being undertaken: there should be a concrete, explicit and legal purpose, the

collected data must be proportional to the purpose of the monitoring activities and the employees must be allowed access to the collected data concerning them.

If the employer plans to monitor your work e-mails, their utilisation for private purposes must be strictly forbidden or organised in such a way that your constitutionally recognised rights are not violated by accessing your personal correspondence. Such provision should be laid down in the internal rules set up by the employer and should be made known to the employees.

3.5.2. Systems for surveillance and control of the company automobiles and vehicles for public transport of goods and passengers.

The employer has the right to install systems for surveillance and control of the company automobiles without your consent only when this is necessitated by the nature of the professional activity performed and security precautions.

The most popular systems for monitoring and control of company automobiles and vehicles for public transport of passengers and goods are the tachograph and the GPS systems.

If such systems are utilised, the employer must notify you about their existence and terms of use. There is also a need for regulating the use of these systems in the form of internal rules and the data must be processed only for the purposes stipulated by the rules. Examples for necessity of installing such systems include companies publicly transporting goods and passengers, performing courier services and also encashment cars. The installation of similar systems allows the employer to receive information of the whereabouts of the vehicle, fuel consumption etc., which leads to optimizing the quality of the performed business activity. There is no obstacle to install similar systems in other vehicles, for example for tracking the whereabouts of the automobile in case of theft.

The use of data from GPS installed in a company car should be regulated in the internal rules of the employer, especially if the employee is allowed to use such car for private purposes.

3.6. Supervision techniques and methods applied by employers.

There is a lack of unified rules for supervision techniques and methods. Every state is currently trying to resolve these issues on its own, in conjunction with the common international rules on privacy.

Recently, there has been a surge in the number of employers using surveillance systems in relation to their employees for access control, work time supervision, protection of corporate property and work discipline enhancement.

Given the existing inequality in the employer – employee relations, in all cases surveillance is not a result of legal obligation. In some states, like in Bulgaria, the employer may use such techniques with your consent which must be given prior to becoming an object of surveillance and must fulfil the following requirements: it must be given freely, be specific and informed as well as explicit.

The employer is the one to prove that an employee, respectively all employees, have actually consented freely and without any external factors of coercion.

Your basic constitutional right is not to be monitored, photographed, filmed, taped or subjected to other actions of this type without your knowledge or despite your explicit dissent, except in cases envisaged by law.

In other states, for example in the Czech Republic, use of those surveillance tools is possible only

in some specific situations explicitly provided for by the labour law and the consent of employee does not play any role.

3.6.1. Using Close Circuit TV¹¹ surveillance techniques.

Video records as means of surveillance contain “personal data” since you can be identified in an indisputable way. Video surveillance represents an act of personal data processing by automated means, only when it is recorded.

Does my employer have the right to carry out video surveillance in the workplace?

When the purpose of the video surveillance is monitoring the work process and observing the working time, the controller may record a video by means of surveillance of its workers/employees only if a legal ground exists. In some states like Bulgaria it is possible upon given explicit consent of the persons subject to video surveillance (for example by a clause in the employment contract). In others, for example in the Czech Republic or Poland monitoring of employees is possible only in serious case consisting in the employer’s nature of activity. If these conditions are not met, employer cannot monitor his employees even if they agree with it.

The employer is also allowed to carry out video surveillance as a measure for working safety of his/her employees or protection of the life and health of individuals, for example in case of remote surveillance of patients in reanimation chambers. Despite this he is not allowed to carry out surveillance in places such as dressing rooms, toilets, or premises where employees socialise.

Some spheres of activity, due to their specificity, require the use of surveillance systems. These include the spheres of national security and defence, the protection of public order, border control, banking, casino activities.

Do I have the right to be notified by the data controller of the video surveillance being carried out?

Yes. You must be notified of the use of technical means for video surveillance and monitoring on the site by information boards placed at easily visible spots, without specifying the location of surveillance devices. They should also contain information about the data controller. This requirement is not considered fulfilled if the information board contains simply a symbol, for example a camera.

In Croatia, for example, the legislation stipulates that the employer has to consult representatives of the employees before the introduction of new technologies, including video surveillance.

Do I have the right to object to being subjected to video surveillance?

Yes, you may object to being filmed by surveillance systems, unless the employer proves that there is legal ground for video surveillance. If your obligations require working in premises or a place which needs to be equipped with video surveillance systems (for example a casino), the employer is supposed to notify you of the obligation for carrying out video surveillance prior to hiring you.

Using surveillance systems in places which are not utilised for work (such as rooms for relaxation of the personnel, toilets, bathrooms, dressing rooms) is generally forbidden.

¹¹ Closed-circuit television (CCTV) is the use of video equipment to transmit a signal to a specific place, on a limited set of monitors.

Do I have the right to access video records related to me and recorded with video surveillance cameras? Yes. Any natural person has the right to access personal data (including video records) relevant to him/her. In cases where in the execution of their right to access employees may receive the personal data of a third person, the controller shall be obliged to ensure that only data related to the respective employee will be disclosed. In this respect the employer should take the appropriate technical measures for blurring/masking the faces of other persons subject to video surveillance. In the absence of such technical possibility access to video records may be provided only with the consent of all persons whose personal data could be found on the video surveillance records.

3.6.2. Biometric data¹².

Does the use of systems using biometrics by the employer represent personal data processing?

Yes. The identification of an individual, for instance through fingerprint scanning, represents automated personal data processing in every situation. Biometric data have a specific nature and in some states, for example in the Czech Republic, they are considered sensitive by law.

Is my employer entitled to utilise as a supervisory tool and discipline enhancing measure systems which use biometric data related to employees?

There are no unified regulations for utilising systems using biometric data for control of labour discipline. However, the utilisation of such systems should be carefully considered in terms of proportionality, e.g. whether the employer has other options for control and monitoring of the working process, which do not interfere in employees' privacy in such an essential way. In Poland the employer is not allowed to use biometric systems based on data from finger prints in order to register working time of the employee.

3.6.3. Using advanced technologies (lie detector).

With technological progress employers tend to use different technologies for examining the loyalty of their employees. These technologies represent a serious intrusion into privacy. Their utilisation poses not only legal but also ethical issues.

Is my employer allowed to subject me to various tests and examinations, including lie detector, with the aim of determining my loyalty or consciousness in carrying out my professional obligations?

If there are no specific legal regulations, these tests and examinations can be implemented only with your informed consent. In the context of their working relations the employer – employee relationship

¹² Biometric data are all data related to physical, physiological or behavioural characteristics of an individual, which allow for their identification, like for example facial images (photographs) or dactyloscopic data (fingerprints). According to the above mentioned principle the different legislations may stipulate different provisions about the entire meaning of the term "biometric data".

is of questionable equality (because of hierarchical structure it is extremely difficult to prove that the consent has been given freely and without any means of external coercion). Subjecting employees to lie detector is excessive, unless provided for by law. For example in Poland you can find specific regulations concerning the use of lie detector in provisions concerning border guard.

Could the results of such tests be used as a premise or a motive for imposing penalties or unilateral termination of the employment contract?

No. In the legal framework on labour results obtained through such tests are not a legal basis for assuming disciplinary responsibility or for termination of the employment contract.

Recommendations

1. Your employer cannot demand from you more information than envisaged in the legal labour framework as a requirement for hiring you.
2. Your employer does not have the right to disclose your personal data to third persons without your consent, except in cases where the law stipulates otherwise.
3. Your employer must inform you about the purposes of the surveillance and monitoring technologies, the rules for their use, scope and methods, prior to their instalment.
4. Your employer has to ensure adequate technical and organisational measures for the protection of your data processed in the employment context.

4. DATA PROTECTION AND TERMINATION OF THE EMPLOYMENT RELATIONSHIP

4.1. Processing former employee's data.

After the termination of the employment relationship the legal basis for processing the former employee's personal data significantly reduces. However, often the former employer still keeps personal data related to the former employee. Such processing of personal data is allowed only if it has a legal basis such as pension regulation, healthcare regulation, tax regulation, archive regulation, etc.

Furthermore, in case of legal dispute before the court the employer can keep the employee's data until he has a legal interest to do so.

It is important to point out that according to different national legal provisions the former employee's data might be kept even up to 50 years in some countries.

What can my former employer do with my data once the labour relationship ends?

Your personal data may be kept only if there is a legal or valid basis for it, in any other case the personal data must be deleted. One of the principles for the collection and use of personal data is the proportionality principle. That means the collected and used personal data should be relevant for achieving some valid purpose and it shouldn't be collected and used excessively.

Also, your data should be kept only in accordance with the regulations on pensions, health care, taxes, etc. for the time necessary to fulfil the purpose of those regulations. Moreover, in order to fulfil those obligations your former employer might be obliged or allowed to disclose your personal data to different recipients pursuant to the law.

Can I access my personal data which my former employer still processes?

Yes, regardless of the fact that the employment relationship is over, your former employer is still the data controller in relation to your personal data which were not erased. The right of access to your personal data means that you have the right (as data subject) to get a confirmation as to whether or not data relating to you are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed.

What can I do if I presume my former employer is not fulfilling all his obligations with regard to my personal data?

Since you are still a data subject and your former employer is still a data controller (with regard to your personal data), you have the right to lodge a complaint to the competent data protection authority if you consider your former employer keeps or processes your personal data longer or in wider scope than the minimum necessary for achieving a valid purpose.

4.2. Transfer of personal data between the former and the present or potential employer.

Sometimes the former and the present or potential employer would share information about employees.

Can my former employer forward my personal data to my current or potential employer?

Your former employer can forward your personal data to a (potential) new employer only if there is a legal basis for such action. The legal basis could be your consent or former employer's legal obligation. For example, in many countries the distraint provisions oblige the former employer to send your personal data related to your debts and distraint proceedings to the new employer.

Your former employer (as well as the actual or potential one) is not allowed to disclose your data which is not related to the employment relationship, except with your consent.

It is important to point out that in some countries (e.g. Croatia) the employee's personal data may be transmitted to the recipients only by the employer himself or by the person who is especially appointed by the employer to do it. The aim of that provision is to keep the secrecy of the employee's personal data within the working place, and to unveil the employee's personal data only to the minimum necessary for working colleagues.

4.3. E-mail, mobile phones and other electronic devices containing personal data.

Often the former employee had a job related e-mail account as well as the right to use mobile phones and other electronic devices of the employer. Once the employment relationship ends it is important to know how to proceed with the former employee's former e-mail address and with the personal data contained in the devices he used at work in order to protect the former employee's privacy and the legal rights of the former employer.

What happens with my work e-mail account once I stop working?

If the e-mail account that was given to you by your former employer contains your name or nickname then it is your personal data and nobody else has the right to use that e-mail address without your consent. In addition, this e-mail address should be deleted once you quit the employment.

It is important to remark that your former employer has the right to ask you to contact all his costumers/partners you have been communicating with, to inform them on the closing of the e-mail address and on the new ways of contacting him. Also, you should transfer all the work related data to your former employer before the closure of your e-mail address.

In case your work phone number, fax number, mobile phone number, etc. are registered to you, your employer should make the necessary changes in the proper registers. Exercising your right to ask for the deletion of inaccurate data you could avoid misunderstandings and complications in the future.

What will happen with my undeleted personal data in the electronic devices of my former employer that I have been using while working for him?

The data related to your personal life which has not been deleted and is still stored in the electronic devices you used (e.g. private photos) belong to you and nobody has the right to process it in any way without your consent or without any other valid legal basis.

Once your former employer finds out your data is still stored on his devices he should contact you; also if you recall that your private data is still contained in the devices you used for your work do not hesitate to ask for a copy of the data and then the deletion of such data. Remember that once you were notified by your former employer on the existence of such data he is obliged to keep it only for a reasonable period of time; after it had passed he has the right to delete the data even without your consent.

Since you can never be sure in whose hands your private data might end up, do not forget to check the electronic devices you have been using before leaving your job and delete the unnecessary personal data. Be careful when deleting data, keep in mind that the deletion of data related to work might be punishable.

4.4. Termination of the employment relationship by court decision and data processing.

If the former employee had a legal dispute with the former employer that ends up in court, it is important to bear in mind that generally the labour related trials are public. The personal information expressed in court decisions generally must be anonymised.

If I have a dispute versus my former employer before the court, can my personal data end up in public? The court is allowed to independently determine which evidence shall be accepted, and the court might decide to accept evidence that includes your personal data. In that case, your personal data might be published if the public and media are interested in the content of the trial which has been open to public. Such collecting and processing of your personal data is legal and your personal data exposed in the trial could be made public. In some countries like Croatia and Bulgaria the personal data are to be made anonymous when published on the Internet website of the relevant court.

How can the bankruptcy of my employer affect my personal data?

As it was mentioned, the bankruptcy is a legal procedure which might affect your employer in case he is not able to pay his debts properly. In that case the company you have been working for may close down; nevertheless, your personal data shall be collected, processed and used only when it's necessary according to the applicable law provisions (e.g. tax, healthcare, pension, bankruptcy, archive and other provisions) or with your consent.

Recommendations

1. Before the termination of your employment relationship make sure that you have deleted or removed all your personal data not related to your job.
2. Your employer does not have the right to store your data for an indefinite period of time. He has to define a storage deadline in accordance with the provisions in the respective national legislation. After the expiration of the deadline the employer has to delete these data.
3. When in doubt on the extent to which your former employer processes your data, remember you have the right to be informed on the purposes of the processing, the categories of data concerned, and the recipients (right of access to data).
4. The employer is obliged to delete your former e-mail account, as well as your personal information from different registers (e.g. phonebooks, etc.). Feel free to remind him on that obligation.

5. EMPLOYEES RIGHTS AND SUPERVISORY AUTHORITIES AS A HELPING HAND

Your personal data has value that you might not be aware of. Unlawful processing of your data by either your employer or other subjects could have a significant impact on your privacy, not only in subjective or psychological sense, but also in terms of material damage.

Even if you personally would act in accordance with our recommendations presented in this guide, the processing of your data might be accompanied by misconduct on the side of your employer. Such failure, no matter if accidental or intentional, could have different forms such as transmission of your data to third parties without your knowing about the reasons or ways of their further handling. Unauthorised persons, for example your colleagues, could gain unlawful access to your personal information, for instance the height of your salary, or your personal file could get lost with all the sensitive details. Other example is monitoring of your movements at workplace through a video surveillance system of which you haven't been informed by your employer, or justification of which you do not agree with.

5.1. General right of employees.

Whenever concerned about your privacy and personal data you can have recourse to your rights in relation to your employer. It is especially your active approach by which in a number of cases you can prevent unlawful interference with your privacy, bring end to such an undesirable situation, or help terminate an ongoing impact. You will protect your rights in such a way.

If you think that personal data your employer holds about you have been or still are being misused or otherwise processed unlawfully, you can exercise your rights directly towards the employer. You can make a request to your employer who is obliged to provide information about the processing of your data. Moreover, you can get the employer to correct your data he is processing about you if you provide evidence that they are inaccurate.

What information must my employer give me about the processing of my personal data?

The employer, upon your request, must provide you with information about the essential parameters of the data processing such as what data or categories of data are processed (e.g. name and surname, home address, date of birth, employment history, information needed for taxation or other legal obligations). You are also entitled to get information about the source of those data. Moreover, the employer must inform you about the purposes for which your data are processed (taxation, payroll, personnel matters, etc.) and whom they have been or could be passed on.

Is the employer allowed to charge me for the information?

As a general rule employer may not charge you for access to information about processing of your personal data, in other words this request should be free.

Different regulation applies for example in the Czech Republic where the employer may charge a fee, however only in case where specific and quantifiable costs would arise for him. The compensation must not exceed these costs. It is usually difficult to enumerate these expenses, so as a rule employers do not require any fees.

Does any deadline apply for the employer to provide the requested information?

The employer must reply without undue delay which usually means within a few days.

How often may I ask the employer for the information?

Generally, there is no limitation how often you may ask your employer for information about processing of your personal data. This means that you may ask him in every situation when you think it is necessary. Generally, it is free of charge, but in Poland you can ask for information free of charge only once in 6 months. On the other hand, in Czech Republic employer may request for covering expenses of providing information (ex. copy of documents, searching for information, cost of sending etc.).

Can I explicitly demand the controller to give me information in paper form?

The employer may provide you relevant information in oral or in written form. When you explicitly ask for information in paper form, for example for obtaining an evidence of unlawful data processing, your employer should give you requested information in paper form.

Do I have the right to directly access my personal file?

This issue is treated in regulations related to the labour law and can vary from country to country. In the Czech Republic, for instance, each employee is entitled to look into his personal file and to get copies of all documents therein on the employer's costs.

How shall I proceed if my employer processes inaccurate information about me?

Employers are obliged to process only accurate and up-to-date personal data. If you find out that your employer processes inaccurate data about you (incorrect date of birth or account number, wrong information about marital status, etc.) and you notify the employer of this fact, the organisation is obliged to correct or destroy the data. Such request should preferably be supported by documents proving the facts (marriage certificate, proof of residence, and so forth).

Who and how shall I turn to when requesting information, rectification, or deletion?

You can contact your superior or the personnel department unless the employer's internal regulations state otherwise. You can do it by word of mouth, electronically, or in writing. It is best to use recorded delivery or electronic mail. You should keep a copy of the request for later evidence.

How shall I formulate the information or rectification request? Shall I use exact quotations from the law?

You do not need to use legal language. Your employer must assess the content of your request. Except identifying yourself it is sufficient to state that you are asking for information about the processing of your data or request to rectify of a particular data or set of data held by the employer.

What shall I do in case the information provided is not satisfactory, incomplete, or the employer refused to respond at all? What if the employer refused to rectify or delete inaccurate data held about me?

You can either repeat your request addressing it to higher instance than previously (to top management instead of your superior, for instance). In exercising your rights you can also turn to a lawyer or the trade unions, if applicable. Furthermore, you can seek help with public authorities. In this case, where personal data and privacy are at stake, the independent data protection authority of your country may be most appropriate.

Do I have the same rights to my former employer?

Your former employer is obliged to process some of your personal data even after your employment relationship is over (for example for taxation or social security system purposes). You may ask him as well as your present employer and the former one is obliged to give you appropriate information about processing of your data, too.

5.2. Supervisory authorities as a helping hand.

You can turn to the competent data protection authority in the country in which you are working, if you believe that the employer has infringed your privacy rights or processed your personal data unlawfully. Data protection authorities have several legal instruments to protect your privacy and to remedy the unlawful conditions of data processing.

How do I complain?

You can lodge a complaint in writing, via electronic mail or in person. It is necessary to describe all relevant facts underpinning your assumption that your rights have been violated. You should support these facts by tangible evidence whenever possible (if the documents or other piece of evidence substantiating these facts are at your disposal) and you should not forget to provide your contact details.

Do I have to pay for submitting a complaint?

Submitting a complaint is usually free of charge. There might be some exemptions, for example in Poland you have to pay for submitting a complaint an administrative fee.

Can I submit anonymous complaint?

Anonymous complaint, that means notice without information that can directly identify its author, cannot be handled as official complaint. Moreover, the authority would not be able to ask for additional information if necessary for assessment of your case and you would deprive yourself of the possibility to get notified of the outcome. On the other hand, when the anonymous complaints would contain reasonable suspicion about a systematic breach of law the competent authority may take it as a signal of serious problems and deal with it.

How shall the DPA act on my complaint?

The authority looks into your complaint and, if need be, requests additional information. Subsequent-

tly, you shall be generally informed of the next steps. The authority can either start an administrative proceeding with the employer or launch an inspection. Your complaint can also be forwarded to other competent authority. Your complaint could also be deemed unsubstantiated and for this reason the authority could postpone it, a fact which you would be notified of.

Do I have to cooperate with the DPA after my complaint has been found justified?

You should not be required to actively cooperate in most cases. You could be asked for assistance only exceptionally, in situations related typically to evidence gathering like hearing of a witness. There are no other obligations on your part ensuing from the complaint.

What is the outcome of administrative proceeding or inspection?

Remedial measures such as blocking or destroying the data implementing appropriate security measures can be imposed in case the inspection reveals that the employer processed personal data unlawfully. If the administrative proceeding proves that legal obligations have been violated during the processing of your personal data, in some Member States the employer shall be fined financially within the limits set by the law just after this finding (for example in Bulgaria and the Czech Republic). In other states, for example in Poland or in Croatia, the inspected body may be fined only when it does not fulfil measures for remedy imposed by DPA.

Shall I be notified of the result of administrative proceeding? In what time?

You shall be informed about the result of the administrative proceeding as soon as the final decision becomes effective. The duration of such proceeding may vary depending on the periods set by legal provisions in individual states as well as on the employer's ability to make use of legal remedies against the issued decision. In the Czech DPA's practice an administrative proceeding takes three months in average.

What can I do if I am not satisfied with the decision taken by the DPA concerning my complaint? Can I appeal against the decision?

If you are not satisfied with the results of DPA's activities dealing with your complaint (you do not agree with the findings of inspection or administrative proceeding), you may appeal against the results in the court. In some legal systems, for example in the legal system of the Czech Republic, you are - as complainant - not considered as a party of procedure conducted by the DPA, therefore you are not legitimised to take any legal action. Nevertheless, you can use here some extraordinary remedies as the general complaint against public administrative modified in Administrative Act or submit your case to the ombudsman.

Which authorities are competent apart from the DPA?

Work inspectorates have supervisory powers in the area of workplace privacy, too. They can carry out inspections at work premises, impose remedial measures as well as financial sanctions for breach of law.

How shall I proceed if my employer's unlawful handling caused me a damage that I demanded to be financially compensated by the employer?

Cases of damages award or compensation are processed by general courts, not by data protection authorities. Should you demand financial satisfaction from your employer for reasons of unlawful interference with your privacy and the employer would not agree with it, please turn to general court.

Where should I complain in case I work for the EU institutions and my rights for personal data protection are violated?

Personal data processing within the EU institutions is under supervision of the European Data Protection Supervisor. When you work in the EU institution and you have reasonable suspicion that your employer does not process your data correctly and according to the law, you may directly complaint to the European Data Protection Supervisor¹³.

Recommendations

1. Be cautious about processing of your personal data, about their accuracy and range.
2. You have the right to ask your employer (or other controller such as job agency) about the way he is dealing with your personal information.
3. You have the right to submit a complaint to the DPA if you suspect that your personal data are not processed correctly.

GLOSSARY OF TERMS

Personal data

any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity; personal data could be for example name and surname, date of birth, address, number of bank account, information about education and work experiences, telephone number, e-mail address, record from video recording facility etc.;

Sensitive data

personal data revealing national, racial or ethnic origin, political opinions, trade union membership, religious or philosophical beliefs, conviction of a criminal act, health status and sexual life;

Data subject

a natural person to whom the personal data pertain, simply „you“;

Processing of personal data

any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction; even one separate operation (e.g. collection) is personal data processing;

Data controller

any entity that determines the purpose and means of personal data processing, carries out such processing and is responsible for such processing, or subject which is obliged to undertake certain personal data processing by specific law, for example employer is obliged to process several categories of data about his employees for the reasons of social and health insurance or tax control;

Data processor

any entity different from the data controller that processes personal data on behalf of the controller and in his name, for example job agency seeking for the employee a specific job, external company ensuring the salary agenda for employer etc.;

¹³ For more information see EDPS website [http:// edps.europa.eu](http://edps.europa.eu).

Consent	free, specific and informed manifestation of will of the data subject the content of which is his agreement to personal data relating to him being processed;
International transfer of personal data	free movement of personal data within the EU, EEA or any forwarding personal data to third countries. Within the EU and EEA this movement cannot be restricted and is not subject of approval of data protection authorities. Data can be forwarded to third countries if special conditions are met.
Data protection authority	is an independent body which shall perform supervision over the observance of the obligations provided for by law on personal data processing, among others receives incentives and complaints concerning breach of obligations provided by law on personal data processing and inform of their settlement.

DATA PROTECTION AUTHORITIES INVOLVED IN THE PROJECT

POLAND

Bureau of the Inspector General for the Protection of Personal Data

The Inspector General for Personal Data Protection, established in 1998, is an independent supervisory authority with powers in the broad area of data protection. The responsibilities of the Inspector General for Personal Data Protection include: overseeing compliance of data processing with the Protection of Personal Data Law, issuing administrative decisions and considering complaints relating to the enforcement of the provisions on the protection of personal data, keeping a public register of data filing systems, issuing opinions on bills and regulations, participating in the work of international organisations and institutions involved in personal data protection, and last but not least, initiating and undertaking activities to improve the protection of personal data by publishing leaflets and other education activities.

The Inspector General has the authority to issue administrative decisions and consider complaints about the implementation of provisions on the protection of personal data.



Contact

ul. Stawki 2
00-193 Warszawa
Phone: (+48 22) 860 70 81
Fax: (+48 22) 860 70 90
E-mail: kancelaria@giodo.gov.pl
Website: www.giodo.gov.pl
Office hours: 8.00 – 16.00 Monday to Friday

THE CZECH REPUBLIC

Office for Personal Data Protection

Founded in June 2000, the Office for Personal Data Protection is an independent supervisory body vested with numerous competences. Its mission is to ensure that businesses and public authorities come to terms with the principles of data protection and to endeavour that individuals are aware of their rights ensuing from the data protection law. The Office's activities are manifold, ranging from handling complaints and investigations, consultancy and promotion to maintaining a register of notified processing operations, authorization of international data transfers, or preparation of positions on specific subject matters. Activities of the Office are governed by the Czech data protection law.

The Office is a respected player in the law-making process where it is involved as consultant always trying to promote the observance of the data protection requirements in the bills submitted by the government.

The Office offers to both professionals and the public advice and support and disseminates a number of valuable publications. Beside the regular Official Journal, Bulletin and Annual Report, readers may profit from different leaflets and brochures focused on interesting topics.



Contact

Pplk. Sochora 27

170 00 Prague 7

Phone: +420 234 665 111

Fax: +420 234 665 444

E-mail: posta@uouu.cz

Website: www.uouu.cz

Office hours: 7.30 – 16.15 Monday to Thursday

7.30 – 15.00 Friday

CROATIA

Personal Data Protection Agency

The Croatian Agency for Protection of Personal Data (CAPPD) is an independent legal entity with public authorities. In carrying out its activities the Agency is independent in the framework of the competence established according to the Act on Personal Data Protection (Official Gazette, No. 103/03).

Agency is structured into 5 departments:

Director's Office,

Department of Personal Data Protection,

Department of International cooperation, EU and Legal Affairs,

Department of Supervision and Central Registry

Department of Common Affairs.

The Activity of the Agency is carrying out administrative and professional tasks regarding to personal data protection. In the framework of public tasks the Agency:

- supervises implementation of personal data protection,
- indicates the violations noticed during personal data collecting,
- compiles a list of countries and international organizations which have adequately regulated personal data protection,
- resolves requests to determine possible violations of rights guaranteed by the Act
- maintains the Central Register.

The Agency has established helpdesk due to which citizens and organizations can report the violation of right in collecting and processing personal data, as concerns the following:

- use of the citizens' ID numbers as personal data (by the banks, by the administration, in retail trade, etc.);
- copying and scanning of ID cards;
- application of biometry in personal data processing;
- disclosures of students' personal data at public places

Cooperation with other countries and counterpart organizations allow the Agency to keep up with the latest trends in data protection issues and developments.

CAPPD participated so far in a number of domestic and EU projects related with protection of personal

data of citizens and particularly children and youth.

In recent years AZOP is particularly focused on taking proactive steps to inform public on emerging privacy issues regarding digital media, Internet and social networks. Internet assures very fast information exchange but on the other hand it offers huge possibilities for privacy violation and the Agency will work hard to raise public awareness on this matter. This demand becomes urgent when journalistic practice of some media disregards their ethic, moral and legal responsibilities.

BULGARIA

Commission for Personal Data Protection

The Bulgarian Commission for Personal Data Protection is the data protection supervisory authority in Bulgaria. It is an independent public authority and was established in 2002 with the enactment of the Law for Protection of Personal Data. The Commission is a collegiate body, consisting of a chairperson and 4 members. The chairperson and the members are proposed by the Council of ministers and are elected by the National Assembly. Their term of office is 5 years.

Acting as a data protection authority in Bulgaria, the Commission handles complaints and conducts hearings, issues permits for data transfers and legal opinions on matters concerning privacy and data protection, performs inspections on data controllers to verify whether they abide by the law, defines the minimal technical and organizational measures for data protection that need to be implemented by data controllers, issues mandatory instructions etc.

One of the key directions over the work of the Commission is the conduct of effective international cooperation and training programs according to different aspects and among specific target society groups. In this respect very important and institutional Commission's authority is the possibility to conclude international agreements for cooperation with similar Supervisory authorities for personal data protection.

The Commission is supported by staff administration comprised of 4 directorates (1 general and 3 specialized). The total number of the administration, including the members of the Commission, is 87 pay-roll employees.



Contact

Fra Grge Martića 14
HR - 10 000 Zagreb
Phone: 00385 (0)1 4609-000
Fax: 00385 (0)1 4609-099
E-mail: azop@azop.hr
Website: <http://www.azop.hr>
Office hours: 07:30 - 16:30 Monday to Friday



Contact

№ 2 Prof. Tsvetan Lazarov Blvd.,
Sofia 1592
Phone: 3592/91-53-518
Fax: 3592/91-53-525
E-mail: kszld@cpdp.bg
Website: www.cdpd.bg

