PARTENA PROFESSIONAL

MEMENTO

OF THE EMPLOYER 05

Monthly review on social and tax regulation | Partena Professional | May 2018

TOPIC

CASE LAW

COLOPHON

Partena – Non-profit-making association – accredited Payroll Office for Employers by ministerial decree of 3 March 1949 under no. 300 Registered office: 45, Rue des Chartreux, Brussels, 1000 | VAT BE 0409.536.968

Responsible editor: Alexandre Cleven.
Honorary editor-in chief: Francis Verbrugge.
Editor-in-chief: Yves Stox, yves.stox@partena.be

Monthly, except in July and August.

40th year – Monthly review

PARTENA PROFESSIONAL

TOPIC PRIVACY IN THE WORKPLACE (PART I)

THE NEW RULES OF THE GENERAL DATA PROTECTION REGULATION (GDPR)

The General Data Protection Regulation (Regulation 2016/679 of 17 April 2016) has been in effect since 25 May 2018. The General Data Protection Regulation is better known by its acronym GDPR.

Does this mean a radical change? Not quite. The GDPR replaces the Data Protection Directive.[1] That Data Protection Directive was implemented in Belgium by the Privacy law.[2] As from 25 May 2018, Belgian legislation is therefore no longer applicable. However, the basic principles of privacy protection are largely retained. The GDPR also allows for specific national legislation to be adopted.

You may be wondering whether the GDPR has an impact on the HR environment in your company. This will undoubtedly be the case if you are now, for the first time, concerned about the protection of your employees' personal data. You may be processing much more personal data than you think. A few examples are the payroll administration, a database of applicants, evaluation and training software, a who's who on the intranet and access control with a badge.

The GDPR has the aim of raising the risk of sanctions. Nevertheless, the Secretary of State responsible in Belgium, Philippe De Backer, argues against a witch hunt by the Data Protection Authority (DPA).[3] [4] Increasing awareness is central to his policy. Partena Professional wants to contribute with this article and supports companies in the development and implementation of an HR policy in line with the GDPR.

THE MANY FACES OF PRIVACY PROTECTION

The GDPR's data protection is relevant at all levels of your company. This article focuses on your employees' data protection. How do you deal with your employees' data? The impact of the GDPR goes even further, however. How do you ensure that your employees deal correctly with the data of third parties, such as customers?

Moreover, in your HR policy, you should not only take the GDPR for data protection into account, the privacy protection you must offer your employees is much broader than data protection. Also consider

- the procedure for the recruitment and selection of workers - CLA no. 38 of 6 December 1983;
- the monitoring of email traffic and internet use - CLA no. 81 of 26 April 2002
- telephony - the Telecommunications law[5];
- camera surveillance - CLA No. 68 of 16 June 1998 concerning the camera surveillance of employees[6];
- exit controls - CLA no. 89 of 30 January 2007 and the Private Security law[7], and
- GPS localisation - CLA No. 81 of 26 April 2002 and the Telecommunications law[8].

The data protection provided by the GDPR is thus part of the much broader privacy protection legislation. In practice, the GDPR must often be applied in conjunction with other legislation and collective agreements. For example, the GDPR stipulates that automated data processing must be documented in the register of processing activities (more about this later). At the same time, for example, you can continue to apply the existing CLAs on recruitment and selection, email traffic and internet use and cameras. Do you not yet have a policy for monitoring email traffic and internet use, for camera surveillance or geolocation? In that case, do not delay the introduction of these policies.

THE NEW DATA PROTECTION

A. WHEN DOES THE GDPR APPLY AND WHICH DATA ARE PROTECTED?

The GDPR applies whenever you process the personal data of natural persons.[9] The GDPR only protects natural persons, regardless of their

nationality or place of residence. A legal entity (for example, a public limited company or partnership under Belgian law) cannot therefore invoke the protection of the GDPR. If you are a natural person, you must always apply the GDPR, including in relation to your employees.

Two elements raise additional questions. 1° What are personal data? 2° What is a processing operation? Both questions are discussed below.

1) What are personal data?

The GDPR defines personal data as all information about a natural person who is identified or identifiable. It is clear when a person is identified. But when is someone identifiable? This is the case as soon as someone can be identified directly or indirectly, in particular by means of an identifier or one or more elements that are characteristic of the physical, physiological, genetic, psychological, economic, cultural or social identity of that natural person. An identifier is, for example, a name, an identification number, location data or an online identifier.[10]
An identifiable person is therefore one who can only be identified by the combination of different elements. For example, the place of residence alone is not sufficient to identify an employee, but the combination with, for instance, the date of birth and the position within the company does lead to an identification. That is why an IP address is also personal information that is protected by the GDPR.
Not all personal data are therefore protected by the GDPR. Anonymous or anonymised data are not protected. That is because the employee is then no longer identifiable. This is conditional on the anonymisation being irreversible. If the employee can still be traced by means of a key in one way or another, the anonymisation is insufficiently robust and GDPR protection is fully applicable.

2) What is a processing operation?

The GDPR also only protects the personal data that are processed. This protection applies not only to automated processes - manually processed data and their storage in a physical personnel file also fall within the scope of the GDPR.
The GDPR thus defines processing in a comprehensive manner. Processing is an operation or a set of operations performed on personal data or on sets of personal data, whether or not by automated processes. Examples are collecting, recording, organising, structuring, storing, updating or modifying, retrieving, consulting, using, providing by means of forwarding, distributing or otherwise making available, aligning or combining data. Blocking, erasure and destruction of data are also processing operations.[11]

EXAMPLE

The taking and keeping of notes during an application procedure in order to ultimately be able to make a decision about whether or not to recruit the candidate falls under the application of the GDPR.
It is not always clear where the boundary lies. An example. May you ask for evidence of good character during an application procedure? The GDPR prohibits the processing of criminal data. However, what if you ask a candidate to produce a certificate of good conduct, read it, and then give it back to him or her? The former Privacy Commission was of the opinion that you did not process any criminal data in this way.[12]

The GDPR thus applies if the personal data are (at least) partially automated or are intended to be included in a structured file.

B. WHO IS RESPONSIBLE: THE CONTROLLER AND THE PROCESSOR

The GDPR places the most important responsibilities with the controller. This is the natural or legal person (or public authority) that determines the purpose and the means for the processing of personal data.[13] This means that you as an employer will thus be a controller.

EXAMPLE

You are a controller because you keep electronic payroll and performance data for HR purposes (e.g. payroll and evaluation).

The controller can act alone or together with others. You will often not be the sole controller. This is the case within a group of companies, for example. At the group level, a certain HR software and policy is rolled out.

EXAMPLE

Not only the employer but also the parent company will then be controllers. They both determine the purpose and the means of processing.

In that case, the joint controllers must establish their respective responsibilities for the fulfilment of the obligations under this Regulation.[14] For example, who will provide the employee with all the information to which he or she is entitled under the GDPR? It must be clear to the employee what role the joint controllers play and what their respective relationships are to him or her. For example, one of the joint controllers could act as a contact person.

The processor processes the personal data on behalf of the controller in accordance with the controller's instructions. The processor is a natural or legal person (or a government agency).[15] Very often, the processor will be an external subcontractor to the employer. Will an individual processor go further than the controller's instructions? In that case, the processor will also become a controller, with all the obligations imposed by the GDPR.

EXAMPLE

Who can be a processor of HR personal data? The social secretariat responsible for processing the payroll is a logical example. Other examples include a recruitment and selection office, a bank (e.g. payment of wages), an insurance company (e.g. hospitalisation and group insurance), an external IT provider and a security firm.

The distinction between the controller and the processor is not always easy to discern in practice. As an employer, you choose which subcontractor you want to work with. You are the controller, and the subcontractor is the processor. But what if you can only give instructions within the strict framework provided by that subcontractor? That may well be the case with HR software. In that case, the service provider also becomes the controller. So you will both become joint controllers. That does not relieve you of your obligations: you have to agree on a division of roles. Take this into account when negotiating and concluding new contracts.

C. WHAT PROTECTION DO YOU PROVIDE? SIX BASIC PRINCIPLES

What protection must the controller provide? All of the concrete obligations derive from six basic principles.[16]

1) **Lawfulness, fairness and transparency**
   Personal data must be processed in a manner that is lawful, fair and transparent with regard to the data subject.
2) **Purpose limitation**
   The personal data are collected for specific, explicitly defined and legitimate purposes. They may not subsequently be further processed in any way incompatible with those purposes.
3) **Data minimisation**
   Personal data must be adequate, relevant and limited to what is necessary for the purposes for which they are processed.
   ➜ Minimise the number of processed personal data wherever possible.
4) **Accuracy**
   Personal data must be accurate and, where necessary, kept up to date. The controller takes all reasonable measures to immediately erase or rectify the personal data that are inaccurate, having regard for the purposes for which they are processed.
   ➜ The personal data must thus be updated regularly.
5) **Storage limitation**
   Personal data are retained in a form that makes it possible to identify the data subjects for no longer than is necessary for the purposes for which the personal data are processed.
   ➜ The duration of retention of personal data is therefore limited.
6) **Integrity and confidentiality**
   Personal data are processed in such a way that - by taking appropriate technical or organisational measures - an adequate level of security is ensured. For example, personal data must be protected against unauthorised or unlawful processing and against unintentional loss, destruction or damage.
   ➜ It is therefore important to protect personal data.

D. THE RIGHTS OF EMPLOYEES

The GDPR innovates when it comes to the rights that employees have. Each of these rights is briefly explained below.

1) **The extension of the obligation to provide information**[17]
   Transparency means that you inform employees when you process their personal data. This obligation was already effective but has now been extended. The most important questions that you must answer:
   - Who is the controller (or the latter's representative) and how can this person be contacted? (If there is a data protection officer, which is not always mandatory, employees must also know his or her contact details. More about the DPO in Part II.)
   - For what purposes do you process the personal data and on what is the legal basis for that processing (see also the register of processing activities in Part II)?
   - Who receives the personal data? (This can also be by means of categories.)
   - Do you transfer your personal data outside the European Union?
   - How long do you retain personal data? Or do you determine the period of time according to criteria, and if so, which ones?
   - Is the provision of personal data a legal or contractual obligation or is it a necessary condition to conclude the employment contract? Is the employee obliged to provide personal data and what are the possible consequences when he or she does not do so?

The GDPR obliges you to inform employees about their rights:

- The right of access and copy;
- The right to rectification,
- The right to erasure of data;
- The right to restriction of processing;
- The right of objection and automated individual decision making;
- The right to transferability;
- The right to lodge a complaint with the Data Protection Authority

You must inform the employees at the time when you collect the personal data from the person concerned. This obligation to provide information therefore applies not only to employees who are already employed but also to future employees and even applicants.

2) The right of access and copy[18]

Employees have the right to access the personal data you process, the reason why you process them, how you obtained them (possibly from a third party) and who receives the data. Employees also have the right to know how long you want to keep personal data, whether you use them in automated decision-making and how it takes place, and whether you want to pass them on to a country outside the European Union (e.g. a head office in the USA).

Employees also have the right to request a copy of the personal data that you process. You can only charge a reasonable fee for the administrative costs of additional copies. If the data subject submits his or her request electronically and does not request any other arrangement, you also submit the information to him or her electronically.

3) The right to rectification[19]

Employees have the right to have incorrect personal data rectified. The right to rectification goes beyond correcting substantive errors.

The employee also has the right to have the data supplemented.

EXAMPLE

How far does this right go? Can an employee also ask for the evaluation to be supplemented by his or her own opinion on the grounds that the manager may not be objective? Yes, and most HR tools now also offer that possibility. The replacement of the (possibly negative) evaluation, on the other hand, goes too far. The employee does not have that right.

4) The right to erasure of data[20]

Employees can oblige you to delete the personal data. Do you have to react immediately? You must react without unreasonable delay. Do you always have to agree to the request? No. The right to erasure of personal data applies, for example,

- if the personal data are no longer required;
- the data subject withdraws his or her consent (and there is no other legal basis for processing, see also Part II);
- the employee objects to the processing;
- the personal data have been processed unlawfully.

Must you always comply with an employee's request to delete personal data? No, you can refuse with a view to instituting, exercising or substantiating a legal claim.[21] For example, you may refuse to agree to a former employee's request to delete individual accounts. Disputes over pay and working conditions can still arise after the employment relationship has ended. In any case, you must keep social documents for five years.[22]

5) The right to restriction of processing[23]

After the termination of the employment contract, as employer-controller, you no longer need the personal details for the payroll administration. You still want to keep the data in order to institute, exercise or substantiate a legal claim. The employee can then oblige you to mark the personal data. The processing of that data can then be limited. You may then only process the personal data with the consent of the employee, for the purposes of instituting, exercising or substantiating a legal claim, or for the purpose of protecting the rights of another natural or legal person.

The employee may invoke the right to restrict the processing if he or she contests the accuracy of the personal data by the data subject, the processing is unlawful and the employee objects to the deletion of the personal data or the employee has objected to the processing (and is awaiting your reply).

6) The right of objection[24] and automated individual decision-making[25]

An employee has the right to object to the processing of personal data at any time, also when you, as the employer, act as the controller. You must then stop processing. The right to object can only be exercised in specific situations, usually outside the context of an employment relationship.

An employee or applicant can oppose automated individual decision-making. Consider, for example, the processing of applications via the internet without human intervention.[26] Automated individual decision-making is possible when the data subject has given his or her explicit consent.

7) The right to transferability[27]

The right to transferability must allow transfer of one's own personal data from one controller to another, including from one employer to another employer. The controller must provide the personal data in a structured, common and machine-readable form.

However, the right to transferability is not absolute. The employee can only invoke it if the processing is carried out by means of automated processes, such as payroll administration, and is based on his or her consent or a contract (see also Part II). The right to transferability is also limited to the personal data that the employee himself or herself has provided to you as an employer-controller.

The concrete consequences in the context of an employment relationship therefore probably do not extend as far as they might seem at first sight. It is advisable to analyse whether the employee can invoke the right to transferability for each type of personal data.

EXAMPLE 1

Can an employee request the transferability of the entire personnel file?
Possibly not. Part of the personnel file may not be automated yet, but still in paper form. Other personal data were not provided by the employee, but by a third party. Consider, for example, the evaluation by a supervisor.

EXAMPLE 2

Can the employee request the transferability of the details of professional contacts he or she has built up during the employment relationship?
Here, the GDPR does not provide a clear-cut answer. These data primarily relate to the confidential personal details of third parties. The data transfer must not affect the rights of these third parties. In any case, the employee must not disclose business secrets or engage in unfair competition.[28] Professional use of these data with a new employer is therefore excluded.

WHAT FOLLOWS IN PART II

In the next part, the practical implementation of the GDPR will be discussed. Which crucial steps should you definitely not skip? With which formalities must you comply? Which documents do you have to prepare? Sanctions and the right to compensation are also discussed.

Yves Stox, Senior Legal Counsel

1 Directive 95-46 EC on the protection of natural persons regarding the processing of personal data and on the free movement of such data.

2 Law of 8 December 1992 on the protection of privacy with regard to the processing of personal data.

3 As from 25 May, the successor of the Commission for the Protection of Privacy.

4 Trends 29 April 2018, Philippe De Backer (Open VLD): "Geen heksenjacht bij controle nieuwe privacyregels" [No witch hunt when checking new privacy rules] (http://trends.knack.be/economie/bedrijven/philippe-de-backer-open-vld-geen-heksenjacht-bij-controle-nieuwe-privacyregels/article-normal-1141465.html).

5 Art. 124 of the law of 13 June 2005 on electronic communications; Art. 314 bis criminal code.

6 Law of 21 March 2007 on the regulation and use of surveillance cameras.

7 Law of 10 April 1990 regulating private and special security.

8 See also the Commission for the Protection of Personal Privacy Opinion 12/2005, 7 September 2005.

9 Art. 2.1 GDPR.

10 Art. 4.1 GDPR.

11 Art. 4.2 GDPR.

12 Commission for the Protection of Privacy Opinion 08/2002, 11 February 2002, 3: "In the absence of appropriate regulation, the employer or the intermediary agency may only take cognisance of the contents of the certificate with the consent of the person concerned without taking note of it or keeping a record in this regard, since the presentation and reading of a document do not, in principle, fall within the scope of the law".

13 Art. 4.7 GDPR.

14 Art. 26 GDPR.

15 Art. 4.8 GDPR.

16 Art. 5 GDPR.

17 Art. 13 GDPR.

18 Art. 15 GDPR.

19 Art. 16 GDPR.

20 Art. 17 GDPR.

21 Art. 17.3.e GDPR.

22 Art. 25 Royal Decree of 8 August 1980 concerning the retention of social documents.

23 Art. 18 GDPR.

24 Art. 21 GDPR.

25 Art. 22 GDPR.

26 Art. 71 GDPR.

27 Art. 20 GDPR.

CASE LAW

FISCAL: LOWER VALUATION OF AN ACCOMMODATION PROVIDED BY A LEGAL ENTITY

An accommodation provided by a legal entity to an employee or a company manager now benefits from a lower tax valuation. This was decided by the FPS Finance pending an amendment to the legislative text.[1]

1 Circular 2018/C/57 of 15 May 2018 on the flat-rate estimate of benefits in kind for the free provision of an accommodation.

VALUATION OF THE BENEFIT

When an employer provides an accommodation to an employee or a company manager, a taxable benefit in kind arises.
The benefit is estimated on a flat-rate basis and varies depending on whether the accommodation is allocated by a natural or a legal person:

Allocation by a natural person	Allocation by a legal person
100/60 of the indexed cadastral income	If cadastral income ≤ € 745: 100/60 of the indexed cadastral income x 1,25
	If cadastral income > € 745: 100/60 of the indexed cadastral income x 3,8

In the case of a furnished accommodation, the benefit shall be increased by 2/3.

ELIMINATION OF THE DISTINCTION

Case law has already ruled on several occasions that the distinction in the calculation of the taxable benefit according to the person providing the accommodation is unconstitutional.
In order to eliminate this difference in treatment, the legal text establishing this distinction is amended.

Pending this amendment, the FPS Finance decided to follow the aforementioned case law. If a legal entity provides an accommodation to an employee or a company manager, the taxable benefit is 100/60 of the indexed cadastral income.

This results in a lower valuation of the taxable benefit when the accommodation is provided by a legal entity.

Example: A legal entity provides an unfurnished accommodation to one of its executives. The indexed cadastral income of the accommodation amounts to € 2,200.00.

Under the old calculation method, the annual taxable benefit amounted to € 13,933.33 (= (€ 2,200 x 100/60) x 3.8).

When applying the new administrative point of view, the annual taxable benefit amounts to € 3,666.67 (= € 2,200 x 100/60).

DISPUTES

Until the new amendment of the law enters into force, the Federal Public Service for Finance decided that at all stages of the procedure the benefit would be determined in accordance with the flat-rate valuation that is applicable when the accommodation is provided by a natural person, irrespective of the person providing the accommodation.

Peggy Criel, Legal Counsel

CASE LAW

NSSO: AMOUNT OF GIFTS IS INCREASED

You can offer your employees a gift on certain occasions (in kind, cash or in the form of gift vouchers). Under certain conditions, these gifts are exempt from NSSO (National Social Security Office) contributions. One of these conditions is the amount of the gift. A draft Royal Decree increases these amounts, with retroactive effect from 1 January 2017.[1]

1 Draft Royal Decree amending article 19, § 2 of the Royal Decree of 28 November 1969 implementing the Act of 27 June 1969 amending the Decree-Law of 28 December 1944 on social security for employed persons; National Labour Council opinion No. 2077.

Type of gift	Amount allowed by the NSSO	
	until 31.12.2016	from 01.01.2017
Saint Nicolas, Christmas, New Year	Maximum € 35/year + maximum € 35 per dependent child	Maximum € 40/year + maximum € 40 per dependent child
Honorary distinction	Maximum € 105/year	Maximum € 120/year
Retirement	€ 35/year of service with the employer	€ 40/year of service with the employer
	Minimum amount: € 105	Minimum amount: € 120
	Maximum amount: € 875	Maximum amount: € 1000
Marriage or declaration of legal cohabitation	€ 200	€ 245

These amounts are provided subject to publication in the Belgian Official Gazette.

Moreover, they are not yet adapted in the field of tax legislation.

The NLC (National Labour Council) asked in its opinion that the maximum amount exempt from social security contributions that you can grant to your employees for their membership of a trade union organisation be increased from € 135/year to € 145/year.

Anne Ghysels, Legal Counsel


PART&NA
PROFESSIONAL