PARTENA PROFESSIONAL

MEMENTO

OF THE EMPLOYER 06

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

TOPIC

Privacy in the workplace (part II)

NEWS

Starters wages: deferral

Company smart phone and split bill: clarification from the tax authorities

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

PRIVACY IN THE WORKPLACE (PART II)

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

In the May edition you can find the first part about the General Data Protection Regulation (Regulation 2016/679 of 17 April 2016). The General Data Protection Regulation is better known by its acronym GDPR and came into force on 25 May 2018. In this second part, we look in particular at how you can get started on the practical implementation of the GDPR.

A. WHERE TO START? THREE CRUCIAL STEPS[1]

Three steps are crucial in the implementation of the GDPR.

1) Identify what personal data you are keeping. Where does it come from and with whom do you share this personal data?
2) Analyse which types of data processing take place.
3) Identify the legal basis for each type of data processing

The reason is twofold.

- As an employer-controller, you must always have a legal basis in order to be able to process personal data.
- Some personal data is sensitive. In principle, it is forbidden to process this.

We elaborate on these two elements below.

B. THE LEGAL BASIS OF THE PROCESSING

As an employer-controller, you must always have a legal basis in order to be able to process personal data:

1) dthe consent;
2) the performance of a contract;
3) a legal obligation; or
4) legitimate interests.

Thus you do not always need the consent of the individual data subject. That is only the case for sensitive personal data. One legal basis is sufficient to be able to process personal data. There is nothing to prevent you always to ask for consent, even if you already have another legal basis. You have to make that assessment. By always asking permission you play safe. But bear in mind that not every employee will necessarily consent. Will you then still carry out the processing on the basis, for example, of the performance of the contract, even if you do not have the employee's consent?

1. THE CONSENT

You may process the personal data if the data subject, employee or applicant, has given his or her consent for the processing.[2] However, this consent must satisfy four cumulative conditions:[3] As employer-controller, the burden of proof that the data subject consents to the processing is on you.[4]

1) **The data subject must be informed**
   The employee or applicant must know what he or she is consenting to. The GDPR does not specify the way in which you must inform the data subject. You must have informed the data subject before you obtain the consent.

2) **Consent must be freely given**
   In the context of an employment relationship, the question arises of whether an employee can give his or her consent freely. Does the employer's authority prevent the employee from giving consent freely? The consent of an employee given to his or her employer within the context of the GDPR can be given freely.[5]

In any event, you may not force the consent. Furthermore, employees must also be able to withdraw their consent at any time.[6] The withdrawal only has an effect for the future. "Freely" means that no sanction may be imposed on whether or not consent is given or withdrawn. This means that in certain circumstances you must provide an alternative workplace or working conditions for the employee who refuses to give his or her consent to the processing.

Belgium can lay down specific rules regarding the conditions under which personal data in the context of an employment relationship may be processed on the basis of the consent. Before the GDPR came into force, the Belgian privacy regulations stipulated that an applicant or employee cannot, as a rule, give his or her consent freely. This prohibition did not apply when the processing was focused on providing a benefit for the data subject.[7] It is not clear whether this rule shall continue in the future.

3) The consent must be specific

This means that you cannot just process the request for consent as part of a text that also contains other elements. You must formulate the request for consent in such a way that it is comprehensible and easily accessible and is in clear and plain language. You need to formulate the text in such a way that the data subject can clearly distinguish the request for consent from other matters.[8]

4) The consent must be unambiguous

The employee or applicant gives his or her consent by means of an explicit statement or an unambiguous and active action. This can be a signed declaration, although that is not the only way to obtain consent. Filling out a form online or sending an e-mail will also be accepted. A selection box or check box that has already been checked is not adequate.

2. THE PERFORMANCE OF A CONTRACT

The processing is also lawful if it is necessary for the performance of a contract for which the data subject is a party. The processing is equally lawful if the data subject requests that measures be taken prior to entering into the contract.[9] In practice, this legal basis provides a broad legal basis for most forms of employee data processing. However, this legal basis is not a permit for any form of data processing. The processing must be necessary for the performance of the contract.

EXAMPLE 1

You do not need to ask the employee for consent to process his or her data in the payroll administration. This is necessary for the proper execution of the employment contract.

EXAMPLE 2

You can rely on this legal basis for the processing of personal data via evaluation and training software without having to obtain the individual consent of the employee. The performance of the employment contract becomes impossible if you do not have the opportunity to mull over the strengths and weaknesses of an individual employee and to adjust training opportunities accordingly.

3. A LEGAL OBLIGATION

You can also justify the processing of personal data on the basis of a legal obligation. You have to process the personal data because the regulations require you to do so.[10]

VOORBEELD

You must process the family data of an employee and pass it on to the tax authorities within the context of the payroll administration. Thus you can perform this processing without the consent of the employee.

4. LEGITIMATE INTERESTS

This is perhaps the most complex way to justify the processing of personal data. You may process personal data if it is necessary to protect your legitimate interests as a controller or the interests of a third party.[11] This means that you have to weigh the interests of the employees against your own interests as controller. This is difficult and the outcome is uncertain.

EXAMPLE

You may wish to consider basing the processing of personal data within the context of a whistle-blower scheme on this legal basis. Such an internal reporting system allows employees to report their suspicions or information related to fraud and corruption.[12]

C. SENSITIVE PERSONAL DATA

In principle, you may not process sensitive personal data.[13] This concerns:

- the personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership,
- genetic data, biometric data for the purpose of uniquely identifying a person,
- data concerning health, or data concerning a person's sexual behaviour or sexual orientation.

EXAMPLE

The processing of photographs should not be considered systematically as the processing of sensitive personal data. Photographs may fall within the definition of biometric data when the processing makes possible the unique identification or authentication of a natural person.[14]

Photos included on the intranet in a who-is-who are thus permitted even without the consent of the individual employee. As an enterprise, you have a legitimate interest in keeping a photo book. It helps to ensure that the internal communication process runs smoothly.[15]

However, there are a number of exceptions to the fundamental prohibition on processing sensitive personal data.[16]

1) The data subject has given explicit consent for the processing. (Belgium can however decide when such individual consent cannot be called upon.)
2) The processing is necessary for the purposes of fulfilling obligations and exercising your rights as employer-controller or the data subject with regard to employment law and social security.
3) The processing concerns personal data which have clearly been made public by the data subject.
4) The processing is necessary for a legal claim (establishment, exercise or defence).
5) The processing is necessary for the purposes of preventive or occupational medicine.

Member States may also introduce conditions and restrictions with regard to the processing of genetic, biometric or health data.

D. PERSONAL DATA RELATING TO CRIMINAL CONVICTIONS AND OFFENCES

Personal data relating to criminal convictions and offences is subject to special conditions. Even with the consent of the applicant or employee, you can only process it if legislation allows this processing.[17] Thus you may process an 'extract from the criminal record' (replaces the 'certificate of good character') for functions when this is required by law or a regulator, such as for company auditors, accounting and tax professions, and the education of minors. This 'extract from the criminal record extract' does not include all convictions, but only those which are relevant for the function.[18]

May you ask for an 'extract from the criminal record' during the application procedure? The GDPR prohibits the processing of personal data relating to criminal convictions and offences. But 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 personal data relating to criminal convictions and offences in this way.[19]

E. FORMALITIES

You have identified which personal data you keep, analysed which data processing takes place within your enterprise and identified the legal basis for each processing operation. You need to go through these steps in order to finally determine which formalities you must fulfil.

EXAMPLE 1

You have identified that you are processing employee identification data in the personnel and payroll administration. You also share this information with your social secretariat. You do this in order to make possible the performance of the employment contract and to comply with the legal obligations within the context of the employment relationship.

EXAMPLE 2

You monitor closely who has access to the R&D department within your enterprise. Employees have access to the workplace after biometric authentication, e.g. through a fingerprint. This is sensitive personal data. You need the consent of each individual employee.

Depending on the specific situation, you need to fulfil various formalities within the context of the employment relationship:

1) The preparation of a register of the processing activities;
2) The formulation of a privacy policy;
3) The adjustment of the employment regulations is not compulsory and rarely recommended, but the conclusion of an annexe to the employment contract can be a solution.

Each of these documents is explained in more detail below.

1) The register of the processing activities

Before 25 May 2018, you had to report all fully or partially automated processing of personal data to the former privacy commission. The register of processing activities replaces this notification requirement.[20]

a. An obligation for employers

As an employer-controller, the register of processing activities needs to be prepared and kept up to date.[21] This register documents all processing activities that take place under your responsibility.

Not every controller is obliged to prepare a register of the processing operations. This obligation does not apply to enterprises which employ fewer than 250 people.[22] This exception is theoretical. In practice, an employer with fewer than 250 employees has to prepare a register. Even a small enterprise with fewer than 250 employees is required to prepare a register if the processing is non-incidental. Personnel management is never really incidental.[23]

You must keep the register in written and electronic form.[24] You must not make it public, present it to the employees (representatives) or send it to the GBA (Belgian Data Protection Authority).[25]

The Registry is a monitoring tool. The GBA may request you to submit the register and then you must immediately submit it to this supervisory authority.

It is a dynamic document. You must always modify it to take account of the actual processing of personal data within your enterprise.

You must prepare and maintain the register for all processing of personal data. Not only for the processing operations within the context of the employment relationship. Do you also process the personal data of, for example, customers? In that case, you must also include these processing operations in the register of processing activities.

b. What information must the register contain?

The register of processing activities must contain the following information:[26]

- the name and contact details of the (collective) controller(s), the controller's representative and the data protection officer (where applicable)
- the purposes of the processing;
- a description of the categories of data subjects and of the categories of personal data;
- the categories of the recipients to whom the personal data has or will be disclosed;[27]
- transfer of personal data to a third country or an international organisation (if applicable);
- if possible, the envisaged time scales within which the different categories of data must be deleted;
- where possible, a general description of the technical and organisational security measures.

You will certainly recognise a number of the items of data that you will also have to provide to employees within the context of your obligation to provide information. You must inform the employees, but you must not do so by means of the register. A privacy policy is an instrument that can help you with this. Do you ask the employees for their consent for the operation by means of an appendix to the employment contract? Then you can also inform them via that route.

c. An example.

The GDPR does not enforce a specific template. It is therefore up to you to decide what the register of processing activities looks like.

An example can be found below. We have filled it in with the two examples that were mentioned earlier:

1) The processing of identification data in the personnel and payroll administration;
2) Biometric access control to the R&D department.

Processing data - categories of data	Purposes	Data subjects	Legal basis	Recipients	Third country recipients	Retention period
A. Identification data						
identification details: name, title, address (private, work), previous addresses	personnel and payroll administration; personnel evaluation; work planning; access control; workplace control.	staff members employed by the employer; persons employed on behalf of the employer.	performance of the employment contract between employer and employee. Compliance with legal obligations within the context of an employment relationship. Necessary proper functioning of the enterprise.	employer and professional advisers of the employer. Staff of the employer responsible for personnel administration.	none	5 years after the termination of the employment contract.
B. Financial data						
Financial identification data: identification and bank account numbers.	personnel and payroll administration	staff members employed by the employer; persons employed on behalf of the employer	performance of the employment contract between employer and employee. Compliance with legal obligations within the context of an employment relationship	employer and professional advisers of the employer. Staff of the employer responsible for personnel administration	none	5 years after the termination of the employment contract.
C. Physical data						
physical data: distinguishing features;	biometric identification	staff members employed by the employer in the R&D department	individual consent of the data subject	employer; company specialising in access control; Staff of the employer responsible for personnel administration	none	12 months after the termination of the employment contract.

2) The formulation of a privacy policy

The GDPR obliges you to provide information when you process personal data that you have either obtained directly from the data subject or that you have obtained from a third party.[28] A privacy policy is a method of satisfying this obligation.

A lot of information from the register of processing activities will find its place in the privacy policy. In the privacy policy you provide an answer to the questions you have to answer in order to comply with the information obligation (see the first part of the May issue).

Who is the controller? What are the purposes of the processing? What is the legal basis of the processing? Who receives the personal data? Do you transfer your personal data outside of the European Union? What is the retention period for the personal data? Is the provision of personal data an obligation or a condition? What are the categories of personal data involved?

The GDPR also obliges you to inform the data subject about his or her rights. You also include this information in the privacy policy.

The right of access and copying, the right of rectification, the right of erasure of data, the right to limit the processing, the right to object and automated individual decision-making, the right to transferability, the right to submit a complaint to the GBA.

The privacy policy is a dynamic document, as is the register of processing activities. You must modify both documents to take account of the actual processing of personal data within your enterprise. Thus remind the reader of the privacy policy that you shall modify the document in the future. The GDPR does not lay down a specific procedure for this. Inform the concerned parties hereof.

3) The employment regulations and the appendix to the employment contract

In theory, you can inform the employees by means of the employment regulations. However there are two main drawbacks to this.

1) The employment regulations only apply to employees and, for example, those with 'work-linked training'. However, the impact of the GDPR is wider than just the employees, also within the context of the employment relationship. For example, when you process applicant data, you must inform them using a separate channel. A privacy policy guarantees a more global approach and is perhaps also more practical.

2) The employment regulations are not a dynamic instrument. You need to apply a strict procedure when you want to change them.[29] The term of this procedure means that in practice you do not always comply with the information obligation laid down by the GDPR.

You can inform the employees by means of the appendix to the employment contract.

1) This shall be useful if you need or wish to obtain the consent of the employee for the processing of the personal data. Everything in one document, that is easy to implement.

2) The appendix to the employment contract also lacks the dynamic character required by the GDPR. That will particularly affect you if the data flows within your enterprise can change quickly and significantly. To remedy this, you can of course combine the appendix to the employment contract with a privacy policy.

F. HOW LONG SHOULD PERSONAL DATA BE KEPT?

Belgian law requires you to keep the (special) personnel register[30], the individual account and any appendices (copies of pay slips, etc.) for a period of five years. These are very precise rules.

- For the (special) personnel register, the retention period begins on the seventh day after the date of termination of service of the last employee.
- For the individual account (and any appendices), the retention period begins as from the annual closure of the account. However if there is any dispute about a payment after the employee's departure, you must keep the document for five years as from the date on which the last notified amounts must be reported to the NSSO.

These periods are minimum periods. Belgian law does not lay down any maximum periods. Which rule should you then apply? You can only fall back on the general principle of the GDPR. You may not retain personal data for longer than is necessary for the purposes for which it was collected and used.

- In the register of processing activities we opted for five years. This means that you keep the identification data in the personnel and payroll administration for as long as the individual account itself.
- For the biometric access control, we opted for 12 months in the register of processing activities. This period is in line with the limitation period for legal claims arising from the employment contract.[31]

Thus always determine the retention period in accordance with the objective that you want to achieve within your enterprise with the retention of the personal data concerned.

G. TRANSFER TO COUNTRIES OUTSIDE THE EU[32]

Personal data can circulate freely within the European Union. For countries outside the EU you must ensure, as the controller, that appropriate protection is guaranteed. This means that the privacy legislation of the country concerned provides a level of protection comparable to the GDPR.

For some countries, you do not need to take any additional measures. This is the case, for example, with the United States, provided that the enterprise in question is affiliated to the EU-US Privacy Shield (formerly Safe Harbour).

Is the protection provided by the other country inadequate? Then you must ensure privacy protection through binding company regulations (within a group of enterprises) or by including standard data protection clauses in your contract with, for example, the subcontractors or service providers concerned.

H. THE DATA PROTECTION OFFICER IS NOT ALWAYS MANDATORY

The GDPR obliges some enterprises to designate a data protection officer (DPO). However, there is a good chance that you are not obliged to designate a DPO. This obligation only applies for:

- a public authority or body;
- an enterprise where the core activity is mainly concerned with processing operations which, by their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large-scale;
- an enterprise that is principally responsible for the processing on a large scale of sensitive personal data and personal data relating to criminal convictions and offences.[33]

I. TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

The GDPR lays down that a risk analysis or privacy impact assessment (PIA) must be performed. This impact assessment is required in particular for processing involving new technologies which, by their nature, size, context and purposes, are likely to present a high risk. Consider, for example, large-scale processing and the processing of biometric data.[34]

Based on the PIA, the controller and the processor need to have implemented appropriate technical and organisational measures to ensure a level of security commensurate with the risk. These include encryption of data, protection of confidentiality and regular testing and evaluation of security.[35]

The controller and the processor shall ensure that any employee who has access to personal data only processes such data on the instructions of the controller.[36] The employment contracts act lays down a general duty of confidentiality on employees.[37] The inclusion of a more explicit confidentiality clause in the employment contract and the provision of training for employees are sensible measures.

J. OBLIGATION TO REPORT

If the PIA indicates that there is a high risk, the controller and processor must consult the GBA. The GBA will provide written advice if the risk is not sufficiently recognised or mitigated.[38]

K. SANCTIONS

The GDPR strengthens the sanctions when compared with the previous Belgian privacy act. The previous privacy commission could not apply sanctions. In certain circumstances, the courts accepted evidence that had been obtained unlawfully, for example in the event of dismissal for misconduct.[39] In exceptional cases previously, judges awarded (limited) moral compensation to individual employees because their (former) employer had not respected the privacy laws.

As from 25 May 2018, the controller must be able to demonstrate compliance with the principles regarding the processing of personal data.[40] Thus, as employer-controller, you must be able to provide proof that the

processing of personal data takes place in accordance with the GDPR. An employee can initiate a complaints procedure with the GBA. This body can then impose an administrative fine on the employer-controller.[41]

EXAMPLE 1

For the incorrect maintenance of a register of processing activities, a fine not exceeding € 10,000,000 or (for an enterprise) up to 2% of the total worldwide annual turnover in the previous financial year (whichever is the higher).

EXAMPLE 2

The maximum fine for processing sensitive personal data without the data subject's consent (without any other exception being applicable) is €20,000,000 or (for an enterprise) up to 4% of the total worldwide annual turnover in the previous financial year (whichever is the higher).

L. YOU CAN NOW GET STARTED

The Belgian government has prepared draft legislation to spell out the GDPR in concrete terms for Belgium. That does not mean that you can still wait. The GDPR came into force on 25 May 2018 and all obligations already apply. It is however striking that the proposed legislation pays little attention to the protection of personal data in the context of the employment relationship.

Partena Professional is happy to assist you with the implementation of the GDPR within the context of the employment relationship within your enterprise. Contact us via legal.partners@partena.be.

Yves Stox, Senior Legal Counsel

1 The CBPL proposed a more comprehensive step-by-step plan: General Data Protection Regulation – Prepare yourself in 13 steps: https://gdpr-eu.be/wp-content/uploads/2016/12/STAPPENPLAN-NL-V2.pdf

2 Art. 6.1.a GDPR.

3 Art. 4.11 GDPR.

4 Art. 7.1 GDPR.

5 Consideration 155 GDPR.

6 Art. 7.3 GDPR.

7 Art. 27 Royal Decree of 13 February 2001 implementing the act of 8 December 1992 on the protection of privacy with regard to the processing of personal data.

8 Art. 7.2. GDPR.

9 Art. 6.1.b GDPR.

10 Art. 6.1.c GDPR.

11 Art. 6.1.f GDPR.

12 Consideration 47 GDPR.

13 Art. 9.1 GDPR.

14 Consideration 51 GDPR.

15 That is also the position of the GBA.

16 Art. 9.2 GDPR.

17 Art. 10 GDPR and art. 10 draft legislation of 11 June 2018 concerning the protection of natural persons with regard to the processing of personal data.

18 FOD Justice, Circular no. 204 (C - 2013/09204), Extracts from the criminal record.

19 Commission for the Protection of Privacy Opinion 08/2002, 11 February 2002, 3: "In the absence of an 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".

20 Art. 30.1 GDPR.

21 The processor of personal data, for example the social secretariat, must also prepare and keep up to date a register of processing activities (art. 30.2 GDPR).

22 Art. 30.5 GDPR.

23 The Commission for the Protection of Privacy, Recommendation 06/2017 regarding the Register of processing activities (CO-AR-2017-011), 6-7.

24 Art. 30.3 GDPR.

25 Art. 30.4 GDPR.

26 Art. 30.1 GDPR.

27 Thus, you do not need to identify the individual recipients.

28 Art. 13-14 GDPR.

29 Art. 11-13 of the employment regulations act.

30 The normal personnel register generally does not need to be kept by employers who fall within the scope of DIMONA (immediate declaration of employment in the social security system). If they do, all their data concerning starting and termination of service is forwarded electronically.

31 The legal claims arising from the employment contract lapse 1 year after the termination of this contract or 5 years after the event from which the claim arose, without this term being allowed to exceed 1 year after the termination of this contract (art. 15 employment contracts act).

32 Art. 44-50 GDPR.

33 Art. 37 GDPR.

34 Art. 35 GDPR; Consideration 91 GDPR.

35 Art. 32.1 GDPR. Also see art. 25 GDPR with regard to data protection by design and by default (privacy by design and privacy by default).

36 Art. 32.4 GDPR.

37 Art. 17, 3° Employment Contracts law. See also National Labour Council, Opinion no. 2.087, Draft legislation of law regarding the protection of business secrets.

38 Art. 36 GDPR.

39 The Court of Cassation ruled in the Antigoon jurisprudence that the judge assesses the admissibility of illegally obtained evidence, taking into account the elements of the case as a whole. The court must take into account the way in which the evidence was obtained and the circumstances in which the unlawfulness was committed. The judge cannot simply ignore the evidence. Unless when a form prescribed under penalty of nullity is disregarded, such evidence may only be refused if the taking of evidence is compromised by a defect which renders it unreliable or that is likely to prejudice the right to a fair trial (Cass. 10 March 2008, S.07.0073.N).

40 Art. 5.2 GDPR.

41 Art. 83 GDPR.

NEWS

STARTERS WAGES: DEFERRAL

Recruiting young people will become cheaper, but not as from 1 July 2018.

You can read more about this new measure in the April issue. The implementation of this measure has now been postponed. The amount of the net flat-rate allowance has still not been fixed. Perhaps a number of modalities will even be adjusted...

Even though the measure will formally enter into force on 1 July 2018, in practice, starters wages will remain a dead letter for the time being.

Yves Stox, Senior Legal Counsel

NEWS

COMPANY SMART PHONE AND SPLIT BILL: CLARIFICATION FROM THE TAX AUTHORITIES

Some time ago, the Minister of Finance decided that an employee pays no taxes on the benefit of the company smartphone in the event of a split billing system. In a recent circular, the FPS Finance explains this position.[1]

BASIC PRINCIPLE

If an employer uses a split billing system for the mobile telephone and Internet subscription, the private use of the mobile telephone (the device) does not give rise to a benefit of EUR 36/year. As announced, the FPS Finance is now providing additional clarification in a circular.

WHAT IS A SPLIT BILLING SYSTEM?

This system implies that the employee receives an invoice directly and separately from the provider for the private use of the mobile telephone and Internet subscription.

A system in which the employer directly receives an invoice for the professional and private use of the telephone and Internet subscription and the employee reimburses the costs of the private use to the employer (e.g. through deduction from the net wage) does not constitute a split billing system.

SPLIT BILLING SYSTEM IN ACCORDANCE WITH SERIOUS STANDARDS AND CRITERIA

Only to the extent that the split billing system is established in accordance with serious standards and criteria and thus corresponds to reality, there is no benefit for the mobile telephone.

1 Source: Circular 2018/C/63 on the benefits in kind for the personal use of a PC, tablet, Internet connection, mobile telephone or fixed or mobile telephone subscription.

Consequently, in the event of a split billing system with a threshold above which any use is deemed to be private use, the employer must provide proof that he set this threshold in accordance with serious standards and criteria.

EXAMPLE 1

An employer makes a smartphone with a mobile telephone and Internet subscription available to an employee. For both subscriptions, he sets thresholds above which any use is deemed to be private use. For the mobile telephone subscription, the threshold is set at EUR 10/month. The threshold for the mobile Internet subscription is set at 2 gigabyte/month. The employer set these thresholds in accordance with serious standards and criteria. The employee receives directly and separately an invoice from the provider for the private use. Such a system constitutes a split billing system. Therefore, making available the smartphone and the mobile telephone and Internet subscription does not give rise to any benefit in kind.

EXAMPLE 2

An employer makes a smartphone with a mobile telephone subscription available to an employee. If the employee wants to have a private conversation, he must first enter a specific number before entering the telephone number. In this way, professional conversations are distinguished from private conversations. The employee receives directly and separately an invoice from the provider for the private use. Such a system constitutes a split billing system. Therefore, making available the smartphone and the mobile telephone subscription does not give rise to any benefit in kind.

If the employer cannot provide proof that he set the threshold in accordance with serious standards and criteria, the private use of the mobile telephone and the mobile telephone and Internet subscription will eventually give rise to a taxable benefit in kind. The private use costs that the provider invoiced separately and directly to the employee in the split billing system may then be deducted from the benefit in kind as an own contribution.

SPLIT BILLING SYSTEM FOR BOTH THE TELEPHONE AND INTERNET SUBSCRIPTION

If the employer makes both a telephone and an Internet subscription available, the position is adopted on condition that the split billing system applies to both subscriptions.

If the split billing system only applies to one of the two subscriptions made available, the position is not adopted.

EXAMPLE 3

An employer makes a smartphone with a mobile telephone and Internet subscription available to an employee. The employee may use these subscriptions for private use. For the mobile telephone subscription, the employer sets a threshold of EUR 10/month above which any use is deemed to be private use. The employer set these thresholds in accordance with serious standards and criteria. He does not set a threshold for the mobile Internet subscription (i.e. there is no split billing system for this subscription). The employee receives directly and separately an invoice from the provider for the private use of the mobile telephone subscription. In this case however, a mobile Internet subscription is made available which consequently gives rise to a taxable benefit of EUR 60/year. There is also a taxable benefit of EUR 36/year for the private use of the smartphone. The position that there is no benefit for the smartphone only applies when there is a split billing system for both the telephone and the Internet subscription.

AND ON A SOCIAL SECURITY LEVEL?

It remains to be seen whether the NSSO will take the same position with regard to the company smartphone and the split billing system.

Peggy Criel, Legal Counsel


PART&NA
PROFESSIONAL