FEDRUS
International

Internal Privacy Policy

Version 1.0
01/10/2019
By Mr Olivier Sustronck, LLM

FEDRUS INTERNATIONAL
"Naamloze Vennootschap" (limited liability company)
VAT No. BE0630.779.617
Schoonmansveld 48
2870 Puurs
www.fedrusinternational.be

FEDRUS
International

The General Data Protection Regulation (GDPR)

After years of lobbying, the General Data Protection Regulation (hereinafter GDPR) was adopted on 27 April 2016. The new regulation is more than welcome, as the Privacy Directive dates back to 1995 and was to a large extent superseded by new technologies.

The GDPR does not fundamentally change the well-known principles, but rather tightens and updates the original rules to the Internet environment and transposes into law the directives of the "Article 29 Working Party" as well as Court of Justice case law. In addition, the GDPR gives the data subject more control over their personal data and imposes additional obligations on the processor and controller.

Even though the basic principles of the legislation remain largely the same, the impact of the GDPR on the business world will be considerable. For example, the GDPR imposes an obligation on every company to handle personal data consciously. Every company must keep a record of how it stores personal data, what personal data it keeps, for what reason, for how long, how it secures that personal data and so on. In addition, data subjects will have much more control over the personal data that is processed about them. For example, the companies' obligation to provide information has been extended and the data subjects can request the amendment, deletion or transfer of personal data upon simple request. Furthermore, data subjects can object to direct marketing or profiling.

The problem of impunity with regard to the Privacy Act ensured that the law was often not or insufficiently applied. The increased attention to privacy awareness in our society and the possibilities for the supervisory authorities to impose sanctions, such as heavy fines, should benefit the stricter application of the GDPR. As a result, many companies that currently have no – or rather, limited –privacy policies will be obliged to make the necessary efforts.

The regulation will enter into force on 25 May 2018 and, given that it is a regulation, will no longer have to be transposed into the national legislation of the European Member States. It is automatically and directly applicable in all EU countries.

FEDRUS
International

A. Basic principles of the GDPR

A.1. Processing of personal data

Personal data exists as soon as a natural person can be identified or is identifiable. This should be interpreted very broadly. For example, contact and billing data are personal data, and also photos, location data, a social media account, an IP address, an online profile or usage data of a software package.

Personal data is processed as soon as it is collected, collated, consulted, stored, modified, transmitted, disseminated or deleted. In other words, whenever personal data is used for any action.

Each time personal data is processed, the person responsible for processing must comply with certain legal obligations.

A.2. Actors during processing

The **controller** is the person who determines the purpose and means of processing. In particular, he is the person who usually obtains the personal data from the data subject and decides what to do with it. As his name suggests, he is responsible for ensuring that the processing of personal data is carried out correctly. This applies both to his own processing (and that of his staff) and to the processing operations carried out by third parties on behalf of the controller (processors).

The **data subject** is the person whose personal data is processed. In a company, the data subjects will mainly be the customers and staff. The person concerned is always a natural person. A company cannot be a data subject. The contact person or the partners of a company are of course natural persons.

The **processor** is an external person who processes personal data for/on behalf of the controller. He cannot be a staff member of the controller. Staff members are the responsibility of the data controller itself. For example, the company social security department is a processor of personnel data; an external IT company that maintains the server, an external website manager, an external marketing company and the accountant are all examples of processors that occur in most companies.

The processor shall enter into an agreement with the controller in which the rights and obligations he has with regard to the personal data he processes are included. The processor may never have more rights with regard to the personal data than those to which the controller is bound. The data controller shall be obliged to impose his or her processing restrictions on the processors.

A.3. When may personal data be processed?

Personal data may only be processed if one of the following processing grounds applies:

- Unambiguous and free **consent** of the person concerned;
- Necessary for the implementation of an **agreement**;
- **Legal** imperative;
- **Vital interest** of the person concerned or fulfilment of **public interest**;
- **Justified interest**.

In the case of a legitimate interest, the company must consider that its interests outweigh the interests of the person concerned. For example, for camera surveillance, guaranteeing safety in the workplace can take precedence over the privacy of the employee. It is also possible to send a newsletter to existing customers (i.e. without prior permission). The person concerned may oppose the application of the justified interest.

Attention should be paid to the fact that, if the processing ground for consent is not used, no consent will be requested. The disadvantage of using the processing ground of consent is that consent must always be free and constitute an active action. The company must be able to provide proof thereof. Implied consent is not permitted. In addition, permission can be revoked at any time. This is certainly not the best processing ground and should only be used if necessary. This applies all the more to employee consent. The relationship of authority between an employer and an employee raises the question of whether permission can be freely requested. An exception applies to taking and using a photograph.

The controller must keep a processing register in which he indicates what data he keeps, why he keeps this data, how he keeps this data, how long he keeps the data, how he secures the data.

Sensitive and special personal data, such as financial data, profiling, data relating to race, religion, orientation and medical data should be kept with special care.

FEDRUS
International

B. Obligation to inform the employee

B.1. What personal data of employees is processed?

We collect and process various personal data of our employees. It may involve the following personal data:

- Identity and contact details such as surname, first name, date of birth and contact details;
- Data relating to your recruitment and qualifications: CV, motivation letter, notes made during the job interview, diplomas, training courses, evaluations, certificates, etc.;
- Administrative and financial information during execution of the employee contract: national register number, address, seniority, marital status, bank account number, family composition, wage data, employment contract, etc.;
- Organisation chart;
- Your wages and payslips;
- Insurance-related information;
- The name of an emergency contact person;
- Health data: Sickness certificates, attestation as a result of accidents at work, results of medical examinations and tests, maternity and parental leave, etc.
- Data relating to the performance of professional activities: Log-in data of work accounts and other applications to which the employee has access, logging, documents drawn up within the framework of the professional activity, communication (internal as well as external), leave request, etc.;
- If applicable: data relating to professional clothing, badges, the serial number of devices;
- If applicable: data relating to the company car and the corresponding leasing contract;
- If applicable: smartphones and laptops;
- If applicable: a detailed invoice of the telephone subscription;
- If applicable: biometric data (finger scan in Puurs)
- Pictures with explicit permission (e.g., on Facebook);

B.2. Why are these personal data processed?

The personal data relating to the CV, the motivation letter, and the notes of the job interview are processed in order to go through the application process on the one hand and to have an overview of who is coming to apply on the other hand. The legal basis for this is consent and justified interest. The applicant sends the data to the company and can also expect the company to keep them up to date to a certain extent. It is also important for the company to keep a record of job applicants and the reason for which they were rejected or hired.

The contact details of the person and the administrative and financial information, and payslips are kept both as a legal basis for the execution of an agreement as well as for a legal obligation.

Data relating to insurance, log-in data, company car, mobile devices, badge, working documents and correspondence for the company shall be kept on a legal basis for the performance of a contract, at least according to the legitimate interest. These data will not be systematically analysed or checked, but can be consulted in case of suspicion of misuse or absence, under the legitimate interest, to ensure the continuity and security of the company.

The name of an emergency contact person is processed based on the employee's vital interest.

With your permission, photos of you can be placed on the company's Facebook page, website, promotional material and on the social media channels. This permission is requested at the bottom of this document and can be revoked at any time after permission has been granted.

B.3. How long will this data be kept?

The data is kept for a period that is necessary in function of the purposes of the processing and in function of the contractual relationship between the employees and the company.

In any event, personal data relating to an employee shall be deleted from the systems after a period of one year after leaving employment, except in the case of personal data which must be retained for a longer period based on specific legislation.

In addition, a surname, first name, contact details and notes are kept in order to maintain an overview of the persons who have worked in the company.

B.4. What are your rights as an employee?

A. Right of access and inspection

The employee has the right at any time, free of charge, to inspect the personal data held about them, as well as the use that the company makes of those personal data.

B. Right of correction, removal and restriction

The employee is free to choose whether or not to communicate their personal data to the company. In addition, the employee always has the right to request the company to correct, supplement or delete the personal data.
However, the employee cannot object to the processing of personal data that is necessary to comply with legal obligations such as administrative tasks.
The employee may also ask to limit the processing of their personal data.

C. Right of opposition

The employee has a right to object to the processing of their personal data for serious and legitimate reasons.

D. Right of free transfer of data

The employee has the right to obtain their Personal Data provided by them to the company in a structured, common and machine-readable form and/or to transfer it to other responsible persons.

E. Right of withdrawal of consent

Insofar as the processing is based on the employee's prior consent, they have the right to revoke that consent at any time.

F. Automatic decisions and profiling

The processing of employees' personal data does not include profiling and will not be subject to automated decisions.

G. Exercise of rights

The employee may exercise their rights by writing to the contact person of the data controller, Mrs. Lynn Geulleaume, at the company postal address, at lynn.geulleaume@fedrusinternational.com or by telephone at +32 3 500 40 52.

H. Complaints

The employee has the right to file a complaint with the Belgian Data Protection Authority (DPA), Rue de la Presse 35, 1000 Brussels, Tel +32 (0)2 274 48 00, Fax +32 (0)2 274 48 35, email: contact@apd-gba.be.

This is without prejudice to a remedy before a civil court.
If the employee would suffer damage as a result of the processing of their personal data, the employee may bring a claim for damages.

B.5. Transfer of personal data to third parties

In the processing of certain personal data, the company is assisted by a number of processors. This includes, inter alia, the following data:

Administrative data, payment and payroll data is passed on to the company social security department for the purpose of carrying out payroll administration. These data are also shared with the competent government bodies within the framework of our legal obligations and can be provided within the framework of an insurance contract.

Your surname, first name and contact details may be passed on to our IT providers for the purpose of managing your account. These data can also be placed online on the website or communicated to the company's customers in order to guarantee the smooth operation of the company. The IT provider may also gain access to the work data, albeit only if this is necessary when carrying out repairs, maintenance or when installing new products.

Cloud providers may have access to work data.
Accounting office may have access to financial data, such as pay slips and bank account number.

This list is not exhaustive.

In the event of a complete or partial reorganisation or transfer of activities of the company, whereby it reorganises, transfers, ceases or if the company goes bankrupt, this may mean that all personal data is transferred to new entities or third parties through which the business activities of the company are carried out in whole or in part.

The Company will use reasonable endeavours to notify you in advance that we will disclose your information to such third party, but you also acknowledge that this may not be technically or commercially feasible in all circumstances.

The Company will not sell, rent, distribute or otherwise make commercially available to third parties, an employee's personal information except as described above or with your prior consent.

In exceptional cases, the company may be required to disclose the personal information of one or more employees pursuant to a court order or in order to comply with other mandatory laws or regulations. The company will make every reasonable effort to inform the employees concerned, within the legal obligations to which the company is bound.

B.6. Security and confidentiality of personal data

The company shall take all appropriate security measures in order to prevent destruction, loss, falsification, misuse, alteration, lack of access, unauthorised access and data leakage. The company shall also make every effort to prevent any other unauthorised processing of these personal data.

C. Obligations of the employee

C.1. Data breach

Article 4, 12 GDPR defines a data breach as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, transmitted, stored or processed data. In concrete terms, this means that as soon as a person is granted access to personal data of which he was not entitled or did not intend to have access, there is a data breach.

Any security incident that may give rise to a data breach must be reported immediately! A security incident occurs as soon as personal data threatens to be unauthorisedly disclosed, lost, destroyed or altered. It is not necessary that data is actually used by a third party. The fact that an unauthorised person has access to the data, or the data ends up with the wrong person is sufficient.

There is also a security incident that must be reported as soon as personal data ends up with the wrong person. This person may be an external person from outside the company, but also a person within the company who normally does not have the authority to see certain data and yet has been given access to it.

Other examples of data breaches that should be reported include: When a computer is hacked that contains personal data, regardless of whether this data is copied or damaged. Nor is malicious intent a prerequisite in order to constitute a data breach. When a USB stick, smartphone or laptop is lost or an email is accidentally sent to the wrong address, a security incident occurs that needs to be reported. When the virus scanner detects an infection, there is a security incident that needs to be reported immediately.

As soon as a security incident is discovered, it must be reported immediately to the contact person of the data controller, Mrs. Lynn Geulleaume. She can be contacted by email at lynn.geulleaume@fedrusinternational.com or by telephone at +32 3 500 40 52.

C.2. Rights of the persons concerned

Each data subject may exercise their rights conferred on them by the GDPR. In doing so, that person may request information, request that data be amended or deleted and request that his or her data be transferred to a third party in a common machine-readable format.

A response to such a request must be given within one month. An additional period of two months may be granted within one month to provide a reasoned reply to the person concerned.

A request for information or a copy should be made free of charge. Only in case of abuse or repetitive question, an administrative fee can be charged. If the request is submitted digitally, it must also be (able to be) submitted digitally. A request for information is not absolute. Data created by the company itself about the person are not included. For example, user analyses of a customer of a software package will not fall under information law. Also personal notes about a person do not fall under the right to information (internal notes of customer or staff member).

In the event of a request for deletion of personal data, all personal data relating to that person must be deleted. However, this request is not absolute.

For example, personal data may be kept if they have to be kept in order to comply with a legal obligation. Personal data may also be kept after a request for erasure if they may be useful in the context of legal proceedings, until the expiry of the limitation period. It is important that within the period of one month (3 months) an open communication is always made to the data subject which data have been deleted and which data have not been deleted and for which reason.

As soon as a request is received from a data subject, it must be reported immediately to the controller, Mrs. Lynn Geulleaume. She can be contacted by email at lynn.geulleaume@fedrusinternational.com or by telephone at +32 3 500 40 52.

C.3 Data Confidentiality

During the performance of their job, the Employee has access to Confidential Information. The Employee is always required to keep this Confidential Information confidential and may only share it with colleagues who have been verified as authorised to access the Confidential Information in question.

The Employee undertakes not to share Confidential Information, knowingly or unknowingly, with unauthorised persons, including third parties.

In addition, the Employee undertakes never to use this Confidential Information to the Employer's detriment or for any purpose other than that for which it was commissioned.

The Employee declares to have read this agreement carefully and declares to fully agree with its contents.

□ I hereby expressly consent to the use of my photograph on Facebook, the website, for publications and promotional material of the company, including social media channels of the company.

(“Read and approved” & date of signature)

Employee’s Name & Signature