Internal privacy policy

The privacy policy clarifies how personal data is processed in the company.

PYRAMID NV

PYRAMID NV

Tel. +32 (0)9 324 70 80

Lambroekstraat 5A
1831 Diegem (Belgium)

Contents

I. Preamble

I.I Introduction

In this privacy policy, **PYRAMID NV** demonstrates how it deals with the processing of personal data.

Digital innovations, such as smartphones, computers, GPS, Internet of Things, etc., have made our current working environment more pleasant and ensured our company operates more efficiently. The use of new technologies also implies large-scale processing of personal data.

The General Data Protection Regulation (GDPR), which entered into force on 25 May 2018, has given companies a bigger role in the internal control of the lawful processing of personal data, because a company as ‘data controller’ deals with personal data of people on a daily basis.

PYRAMID NV sees this as an opportunity to process personal data carefully, thereby reinforcing confidence in the company.

This document contains the policy which defines the direction to be taken and provides a structure within which our company will indicate and further strengthen the legal and useful operational methods used to process personal data.

I.II Objective

PYRAMID NV strives to make sure that personal data is processed in the fairest manner. In other words, personal data is processed on the basis of legitimate grounds for a specified purpose, transparently and proportionally.

This means the following:

- managing and storing information from customers and candidates and data from PYRAMID NV and its subsidiaries in a securely protected environment with the utmost care;
- increasing general awareness about the importance of information security and processing personal data;
- ensuring business continuity;
- minimising possible risks of incidents and their impact.

I.III Scope

PYRAMID NV consists of the following companies/departments:

- Pauwels Consulting NV;
- Pauwels Consulting France SARL;
- PIT Advisor NV;
- Akros Solutions SPRL;
- Akros Europe SPRL;
- Mediconsult V.D. International BVBA.

I.IV Implementation

This document contains the policy on protecting personal data. The implementation is divided into four parts:

- making everybody at PYRAMID NV aware about the processing of personal data;
  - PYRAMID NV maintains a data register with all processing activities concerning personal data;
  - this policy is publicised in the company;

- taking preventive measures;
  - implementation of security measures in company operations;
  - identifying high-risk processing operations for which a data protection impact assessment is required and where the recommendations of the Belgian Privacy Commission are closely followed;
  - checking agreements with external processors and external agreements for compliance with the GDPR;

- scheduling evaluations;
- applying and evaluating restoration measures;
  - following the procedure described below in the event of personal data breaches;
  - the data protection officer writes a report every year regarding the implementation of the policy, possible adjustments and the number of procedures that have been applied.

Pauwels Management BVBA, managing director, represented by Bert Pauwels
25 May 2018

II. Laws and regulations

II.I European legislation: the General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) dates from 24 May 2016, but companies and organisations had until **25 May 2018** to adapt to the new requirements of the GDPR. The points are briefly summarised in this chapter, then policy regarding these points is elaborated in the following chapters.

The full regulation can be found under the following link: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679.

In addition to this regulation, there is also a new **ePrivacy Regulation** which mainly deals with electronic communication data.

The GDPR defines the following main parties:

- the **data subject**: the individual whose personal data is processed;
- the **controller**: the organisation that processes data and determines the purposes and means of the processing;
- the **processor**: the entity that processes data on behalf of the data controller;
- the **supervisory authority**: this is currently the 'Belgian Data Protection Authority', which recently replaced the 'Belgian Privacy Commission'. A complaint can be filed with the supervisory authority when data is processed incorrectly;

  The Belgian Data Protection Authority drew up guidelines on how a company can conform to the recently enforced regulation. The privacy policy has been drawn up in accordance with these guidelines and provides the necessary protection and risk analyses where necessary. In addition, the documents of the 'Article 29 Working Party' of the European Union are also followed up in order to protect

personal data as much as possible. These recommendations can be found at http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358.

The GDPR sets out the following principles concerning the processing of personal data:

- processing must be **lawful, fair and transparent**; any information or communication relating to the processing of data must be easily accessible and intelligible;

- it must be for **specified, explicit and legitimate purposes**; note: the GDPR justifies processing for purposes other than the initial ones if the processing is compatible with the purposes for which the data was initially collected; this compatibility must be assessed by the controller; compatibility is not required if there is a legal basis for processing and authorisation is provided by European or national law;

- data must be **precise and accurate** and, where necessary, kept up to date; data may be corrected;

- data processing is **limited to what is adequate**, relevant and limited to what is necessary in relation to the purposes for which it is processed;

- the **period for which the personal data is stored is limited** to that necessary to fulfil the purposes; the data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed;

- **integrity and confidentiality**; the processing must be properly secured through appropriate technical or organisational measures.

Which activities are covered by the regulation?

The regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of

personal data which form part of a filing system or are intended to form part of a filing system.

The material scope has not changed with regard to the old directive.

The processing consists of the following actions with personal data:

- collecting, recording and organisation;
- storage, adaptation, structuring or alteration;
- retrieval, consultation, use;
- disclosure by transmission;
- dissemination or otherwise making available;
- alignment, combination;
- restriction, erasure or destruction.

Territory?

1. The controller is based in the European Union, where the regulation is applicable.

2. The controller is based outside the European Union. When, in that case, the processing activities are related to the offering of goods or services to those people or to the monitoring of the behaviour of data subjects in the European Union, then the regulation applies.

The following chapters explain how personal data is processed in accordance with the GDPR.

II.II Belgian legislation

Before the GDPR came into force, the legislation set out in the Belgian Data Processing Act of 8 December 1992 and amended on 11 December 1998 was applicable. This amendment came after the first Data Protection Directive of 1995. The basic principles of the old directive and consequently Belgian law have been preserved, but strengthened and described in more detail in the GDPR.

You can consult the full law at this address:

https://www.privacycommission.be/sites/privacycommission/files/documents/privacy_nl_0.pdf

The 'Belgian Privacy Commission' was replaced by the 'Belgian Data Protection Authority' (DPA). The text was adopted by the Chamber of Representatives on 9 November 2017. The authority has been established and the other provisions of the law came into effect on 25 May 2018.

What is the Belgian Data Protection Authority?

There are 6 bodies in the DPA:

1. an executive committee;
2. a general secretariat;
3. a front-line service centre;
4. a knowledge centre;
5. an inspectorate;
6. a dispute resolution body.

What can the DPA do?

- Provide information and advice to individuals, controllers (and their processors) and the government on complying with or enforcing data protection legislation.

- Supervise controllers (and their processors) on maximising the use of preventive instruments in the GDPR, such as certification, compliance with codes of conduct and indications for appointing a data protection officer.

- Verify compliance with the GDPR by the controllers (and their processors) with an inspectorate trained for the purpose.

- Issue sanctions, ranging from warnings to financial penalties for bad pupils. This is assessed on a case-by-case basis and a balanced and proportional treatment is proposed depending on the severity of the situation.

III. Processing of personal data in PYRAMID NV

III.I What personal data does PYRAMID NV retain?

1. General

'Personal data' is:

'any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.'

Any data which can be used to designate who a person is or which gives rise to designating an individual must be processed in a fair manner and in accordance with the GDPR.

PYRAMID NV maintains a data register with all processing of personal data. This register is evaluated and updated twice a year.

The categories of personal data are listed in the data register made available to the company and to the Belgian Data Protection Authority when requested. This is an internal document listing the processing activities carried out by PYRAMID NV.

For example, it contains an overview of the personal data processing that we perform and can identify. These are divided into different categories.

The first series of categories are normal personal data. These are drawn up with normal business operations in mind, but they are not exhaustive.

In addition, we have a number of special categories of personal data that are 'sensitive' in nature. The processing of this data is in principle prohibited, except in the exceptions provided for by law (see below).

2. Normal category of personal data;

- contact details (name, address, phone number, e-mail, title, gender, social media IDs, job, etc.);
- identification data, other than the national registration number issued by governmen ID no. passport, driving licence, pension number, vehicle registration number;
- electronic identification data and localisation (IP addresses, cookies, connection times, GPS, GSM);
- government information (national registration number);
- financial information (bank details, wages, loans, investments, group insurances, pensions, etc.);
- personal characteristics (age or date of birth, etc.);
- physical characteristics (height, weight, shoe size, eye colour, etc.);
- education and certificates;
- career data (CVs);
- hobbies and interests;
- consumption habits.

3. **Special category of personal data;**

- race or ethnic origin;
- political preference;
- religious or philosophical preference;
- memberships of associations, trade unions, etc.;
- genetic data;
- biometric data for identification purposes;
- data concerning health;
- data related to sexual behaviour or sexual orientation;

III.II Application of the personal data processing principles in line with the GDPR

1. Lawful, fair and transparent processing;

Any information or communication relating to the processing of data must be easily accessible and intelligible;

PYRAMID NV always uses one of the following legal grounds for the normal categories of personal data:

a) **Consent of the data subject:**
The consent of the data subject is given when the data subject agrees with the request to process the data subject's personal data.

This consent is:

- freely given;
- informed and specific;
- unambiguous;

Consent must always be given freely.

b) **Contractual reason:**
When data processing is necessary for the performance of a contract or the implementation of pre-contractual measures at the data subject's request;

c) **Legal obligation:**
Various laws and implementation decisions make the processing of personal data necessary for the company to comply with its obligations.

d) **Vital interest of the data subject or other data subject:**
The vital interest of the data subject means that processing data is of vital importance to help the person in question if the data subject is physically or legally incapable of giving consent. For example, if someone is found unconscious, an ambulance is called and the data of the data subject are forwarded.

e) **Public interest or exercise of official authority:**
It may be necessary to process personal data for the public interest.

f) **Legitimate interests pursued by the controller or by a third party, in line with the purpose of the processing:**
Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

Special categories of personal data may not be processed unless;

a) **explicit** consent is given;

b) the processing is necessary to carry out the obligations and exercise specific rights of the controller or of the data subject in the field of **employment and social security and social protection law** (as long as Union or Member State law or a collective agreement provides safeguards for the fundamental rights);

c) the **vital interests** of the data subject or other person prevail if the data subject is physically or legally incapable of giving consent;

d) it concerns a **foundation, association or any other not-for-profit body** with a **political, philosophical, religious or trade union aim**;

e) **it concerns public data**: data made public by the data subject;

f) **it concerns data for judicial reasons**: necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

g) **there is a substantial public interest**, on the basis of Union or Member State law which shall be proportionate to the aim pursued and provide for specific measures to safeguard the fundamental rights and the interests;

h) when processing is necessary for the purposes of **preventive or occupational medicine**;

i) when processing is necessary for reasons of public interest in the area of **public health**, such as protecting against serious cross-border health hazards, or ensuring standards for quality and safety of health care and of medicinal products or medical devices;

j) the processing is necessary for **archiving** purposes in the public interest, **scientific or historical research** purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law, which shall be proportionate to the aim pursued with specific measures.

2. For specified, explicit and legitimate purposes;

It must be clear to data subjects for which purpose their data is processed. These purposes must be defined as specifically as possible.

Note: the GDPR justifies processing for purposes other than the initial ones if the processing is compatible with the purposes for which the data was initially collected; this compatibility must be assessed by the controller, this is carried out by the company in consultation with the data protection officer.

Compatibility is not required if there is a legal basis for processing and authorisation is provided by European or national law;

The following purposes are determined in the data register (this is a non-exhaustive list):

- administration of staff and intermediaries;
- management of staff and intermediaries;
- work planning;
- checking the workplace;

- customer management;
- combating fraud and violations of customers;
- management of contestations;
- supplier management;
- collecting gifts;
- public relations;
- technical-commercial information;
- registration and administration of shareholders or partners;
- member administration;
- security;
- dispute management;
- protecting the society, the own sector or the organisation.

3. **Personal data must be processed precisely and accurately;**

Data must be processed precisely and accurately. The data subject is responsible for accurately communicating this data and informing the company in good time of any changes.

Data subjects can change their data by contacting the competent persons.

4. **Data processing and the period for which the personal data is stored are limited to what is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;**

The period for which the personal data is stored is limited to that necessary to fulfil the purposes;

The period for which the personal data is stored can be specifically determined, but where this is not feasible, data is stored as long as necessary. Obviously, this has to consider the rights of the data subject.

5. **Integrity and confidentiality;**

The processing must be properly secured through appropriate technical and/or organisational measures. Privacy by design principles are applied where possible to protect personal data, which means that where feasible default settings protect privacy as much as possible.

The organisational measures are further explained in this policy. Every employee, worker and part of the organisation must make the necessary efforts to implement this policy as much as possible.

III.III Is data provided to external parties?

PYRAMID NV will only provide personal data to processors or affiliated companies if this is necessary for the execution of the agreement with the data subject or to comply with a legal obligation or when the legitimate interest of the company requires it and this is compatible with the purpose of the processing and takes place in a proportional manner.

We conclude a data processing agreement with companies that process data on our behalf or the agreement between the parties provides sufficient safeguards to ensure the same level of security and confidentiality of your data. The GDPR states the following:

Data flows within the European Economic Area (EEA) is permitted. All European Member States are expected to ensure an adequate level of protection

Any data flow from the EEA to outside the EEA must consider the adequacy decision of the European Commission. If the country to which the data is sent does not have an adequacy decision, the company itself must give the safeguards, apply the corporate rules and implement a policy to provide the necessary safeguards and ensure appropriate protection. Model contracts can be found at http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm.

Appropriate safeguards are the following:

- binding corporate rules;

- standard clauses of the European Commission;
- contractual clauses authorised by the Belgian Privacy Commission;
- approved code of conduct or certification mechanism;
- explicit consent of the data subject;
- necessary for the performance of a contract.

III.IV Risk-based approach - method and PIA

The GDPR requires that a privacy impact assessment (PIA) is drawn up in certain cases.

Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a **high risk** to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out **an assessment of the impact** of the envisaged processing operations on the protection of personal data.

A single assessment may address a set of similar processing operations that present similar high risks. In this respect, the data protection officer is asked for advice.

The data protection officer can use a combination of supervisors' guidelines and known risk lists and methods to carry out an appropriate risk assessment, considering the controller's processing.

The supervisors' guidelines take into account the various provisions in the GDPR that involve a risk-based approach.

The method of the PIA and the PIA model that has to be used for processing activities involving a high risk can be found in a separate attachment.

III.V Rights of data subjects

The General Data Protection Regulation aims to ensure transparent and clear communication with data subjects.

The General Data Protection Regulation stipulates that the data subjects have a number of rights. These rights are not absolute. PYRAMID NV undertakes to guarantee these rights as much as possible and with a balance of interests. It concerns the following rights:

1) Information and access to personal data;

The data subject can obtain information about the following:

- the purposes of the processing;
- the categories of personal data;
- the recipients or categories of recipients to whom the personal data has been or will be disclosed, in particular recipients established abroad or international organisations;
- the period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- the right to lodge a complaint with a supervisory authority;
- the source of the data in the event of indirect collection;
- the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

This request is free of charge. An administrative fee may be charged for additional copies. If this request is made electronically, the data subject will receive the information electronically.

Procedure concerning the right of information, access and rectification

1. Receiving a request from the data subject

The external privacy statement describes how the data subject can submit an access and/or rectification request. This is done at PYRAMID NV by e-mailing a request to a specific address: gdpr@pauwelsconsulting.com.

2. Identification obligation

The organisation must first establish the identity of the data subject before responding to the data subject's request.

3. Period within which an answer must be given

PYRAMID NV reacts within 1 month and tries to respond properly within this month unless it concerns complex matters. If the request is complex, for example involving a large amount of personal data, this period can be extended.

4. Refusal of a request?

In certain and exceptional cases, PYRAMID NV may refuse to respond to a request. This may be the case, for example, in the event of a manifestly unfounded or excessive request or when the legitimate interests of the company outweigh the interests of the data subject.

5. Answer to the request?

PYRAMID NV strives as much as possible to respond appropriately to the request of the data subject, unless this proves impossible or requires a disproportionate amount of effort.

2) Rectification and erasure of data;

Data subjects may request erasure of their data. PYRAMID NV responds to this request to the extent possible. The data subject may request this when:

- the personal data is no longer necessary in relation to the purposes;
- the data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing;
- the data subject objects to the processing of his or her data and there are no overriding legitimate grounds for the processing;
- the data has been unlawfully processed;

- the data has to be erased for compliance with a legal obligation.

Procedure concerning the right to erasure

1. Submitting a request

The external privacy statement describes how the data subject can submit an erasure request. This is done at PYRAMID NV by e-mailing a request to a specific address: gdpr@pauwelsconsulting.com.

2. Decision about the request

Due to technological advances, it is highly probable that a right to be forgotten is impractical since the data may well have been transferred to other processors. All reasonable measures will be taken to inform the other controllers who process your data that you have requested that all links to your personal data or any copies or reproductions of it are erased. This is therefore a best efforts obligation, rather than an obligation to achieve results.

The request for erasure of data will be refused where this can be justified, for example:

- for exercising the right of freedom of expression and information;
- for compliance with a law for which the processing of the data is necessary or for the performance of a task carried out in the public interest or in the exercise of official authority;
- if the processing is necessary for reasons of public interest in the area of public health;
- if the processing is necessary for scientific or historical research purposes or statistical purposes in so far as the right to data erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing;

- if the legitimate interests outweigh the interests of the data subject;
- for the establishment, exercise or defence of legal claims.

3. Answer

The answer and possible erasure will occur without undue delay.

3) Restriction of processing;

The data subject has the right to restrict the processing of his or her personal data in a number of cases:

- when the data subject questions the accuracy of the personal data;
- when the data subject considers that the processing is unlawful and opposes the erasure of the data and requests the restriction of processing;
- when the organisation no longer needs the data but it is required by the data subject for the establishment, exercise or defence of legal claims;
- when the data subject objects to processing, pending the outcome of the decision.

Procedure concerning the right to restriction

1. Information obligation and receiving a request

The external privacy statement describes how the data subject can submit a restriction request. This is done at PYRAMID NV by e-mailing a request with ID to a specific address: gdpr@pauwelsconsulting.com.

2. Investigation of the request

During the investigation into the restriction of the processing, the processing of this personal data will be limited as much as possible.

3. Decision about the request

If it is decided that the data subject's request for restriction is justified, the personal data concerned may no longer be processed.

The controller may only carry out further processing of the personal data in the following circumstances:

- the data subject gives consent again;
- with a view to legal claims or to protect the rights of others;
- it is required for urgent reasons of public interest for the Union or a Member State.

4. Notification

If the personal data in question has been passed on to a third party, PYRAMID NV will provide the recipients with information about the right to restriction requested by the data subject, unless this proves impossible or requires a disproportionate amount of effort.

The company replies within a reasonable period of up to 1 month. This period can be extended if it concerns more complex matters.

4) A data subject can object to processing;

A data subject has the right to object to the processing of his or her personal data, including profiling based on the processing.

Procedure concerning the data subject's right to object

1. Submitting the request

The external privacy statement describes how the data subject can submit a restriction request. This is done at PYRAMID NV by e-mailing a request with ID to a specific address: gdpr@pauwelsconsulting.com.

2. Decision about the request

If the data subject objects to the processing of his or her personal data for direct marketing purposes (including profiling), the controller must respond to this request.

If the data subject objects to the processing on the basis of the public interest and legitimate interest, the controller shall no longer process the personal data unless it:

- demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject;
- requires it for the establishment, exercise or defence of legal claims.

Reasons must therefore be given concerning the decision to stop or continue processing. Submitting an objection is free of charge.

3. The answer

The decision is taken within a reasonable period of 1 month, subject to extension, required by PYRAMID NV to investigate the objection.

5) Data portability;

A data subject may ask the employer to provide any personal data processed on the basis of explicit consent or performance of the employment contract in a structured, commonly used and machine-readable format.

The scope of this right is also limited, since the data subject will only receive the data provided personally.

The data subject cannot exercise this right in other cases, such as when the processing of the data is based on a law.

Procedure concerning the portability of the data

1. Submitting the request and decision

If requested by the data subject, the company is obliged to transfer this personal data (in a commonly used and machine-readable format) directly to another organisation.

Any refusal must be justified.

2. Period

Such a request from a data subject must be answered without undue delay, unless it concerns complex matters, which the data subject must be informed about.

III.VI Procedure concerning personal data breaches

1) Identification of a personal data breach

A personal data breach (or suspected personal data breach) can be identified in various ways: automatically by computer systems, by an employee within the company or by a notification from outside the company.

As soon as someone within the company is aware of a personal data breach, they must immediately notify it to the DPO or the competent person for privacy data within the company if no DPO has been appointed (for the sake of clarity, the term DPO is always used).

The notification contains information about the following, insofar as this can be ascertained immediately:

- the nature of the personal data breach:
  - loss or damage of data;
  - reduction or loss of accessibility;
  - breach of the confidentiality of data;
- the identification of data;
- the impact on the organisation;
- the suspected cause.

Personal data breaches must be notified immediately on discovery. Anyone who detects personal data breaches must be available to the DPO for further follow-up.

2) Analysis by the DPO

The DPO will carry out an initial analysis immediately after receiving a notification of a personal data breach.

1. If there is no personal data breach, no personal data is involved or the personal data breach does not involve risks to the rights and freedoms of the data subjects, the DPO reports this to the Management Team and then proceeds as described under Point 10.

2. If there is a personal data breach involving personal data that is thought to involve a risk to the rights and freedoms of one or more data subjects and the personal data breach is limited in scope and impact and does not correspond to one of the situations listed below, the DPO personally settles the incident, reports to the Management Team and then proceeds as described under Point 4.

3. If there is a personal data breach involving personal data that is thought to involve a risk to the rights and freedoms of one or more data subjects and it corresponds to one or more of the situations listed below:

- impact on the IT infrastructure is suspected;
- malicious intent is suspected;
- impact on sensitive data is suspected;
- impact on a large set of data is suspected;
- impact on data from a large number of data subjects is suspected;
- any other situation that is serious enough to involve the crisis team in the evaluation;

then the DPO convenes the crisis team without delay and proceeds as described under Point 3.

3) Convening the crisis team

If necessary, the DPO will convene the authorised persons.

If a person from within the organisation is called but is unable to attend, a substitute is indicated. As soon as the crisis team is convened, it immediately meets and analyses the incident. Each member of the crisis team contributes to the analysis of the incident on the basis of his or her job, knowledge and expertise.

If the crisis team notes that certain expertise is missing and external assistance is needed, it makes a notification and an external advisor is sought.

A report of each meeting is drawn up containing the following information:

- those present (physical presence is not compulsory);
- place and time of beginning and end;
- report of the employee who notified the personal data breach and the DPO (first meeting); this can also be anonymous;
- reports of action points from previous meetings;
- precise representation of what was discussed;
- decisions made;
- communication measures;
- frequency and number of meetings (first meeting);
- possibly, a step-by-step plan with action points and agenda for a follow-up meeting.

4) Evaluation

Both the DPO individually and the crisis team proceed to analyse the personal data breach and investigate:

- the nature of the personal data breach;
- the categories and number of data subjects involved in the incident;
- the categories and amount of data involved in the incident;
- the impact on the company;
- an assessment of the impact on the rights and freedoms of the data subjects;
- possible consequences of the incident;
- measures to rectify the personal data breach and avoid or reduce the consequences of the personal data breach;
- measures that can avoid future incidents.

5) Notification to the privacy authorities

The notification obligation does not apply to any security incident (i.e. a 'personal data breach' (in the sense of an incident) as defined in Article 4.12 of the GDPR), only to those that present a risk to the rights and freedoms of natural persons (Article 33 of the GDPR).

A security incident is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

This concerns, for example, security incidents which impact the availability, integrity or confidentiality of personal data (Article 32 of the GDPR).

The DPO or the crisis team must notify the detection of a risk of violation of the rights and freedoms of the data subject to the privacy authorities.

This notification includes at least a statement of the information legally required pursuant to Article 33 of the GDPR:

- the nature of the personal data breach;
- if possible, the categories and number of data subjects involved in the incident;
- if possible, the categories and amount of data involved in the incident;
- the name and contact details of the DPO;
- possible consequences of the personal data breach; and
- measures to rectify the personal data breach and avoid or reduce the consequences of the personal data breach.

Efforts are always made to notify the privacy authorities within the statutory period of 72 hours following the discovery of the personal data breach.

If it is not possible to collect certain information within the period of 72 hours following the discovery of the personal data breach, it will be provided to the privacy authorities without delay.

If the privacy authorities are notified after the period of 72 hours, the notification must explain the reason.

If the detected risk remains low, the procedure continues as described under Point 8.

6) Notification to the data subjects

If the DPO or the crisis team detects a high risk of violation of the rights and freedoms of the data subject, the latter must be informed in clear and unambiguous language.

At least the following information must be provided:

- the name and contact details of the DPO;
- possible consequences of the personal data breach; and
- measures to rectify the personal data breach and avoid or reduce the consequences of the personal data breach.

It is not necessary to inform data subjects if:

- technical and organisational measures were taken, such as encryption, which made the data unreadable;
- measures were taken in response to the personal data breach that exclude any risk of privacy violation; or
- such notification is not possible and a public announcement is published as an alternative.

7) Disclosure

If notifying the data subject is legally required, but would require unreasonable efforts and costs, a public announcement must be made. The crisis team can also decide if a public announcement is desirable.

In any case, it must always be ensured that every public announcement:

- does not cause unnecessary fear or panic;
- is limited to facts which have been checked by the crisis team;
- indicates that the necessary measures are being taken;
- does not report personal data; and
- provides contact details where more information can be obtained.

Only the managing director is authorised to carry out these public announcements.

8) Reparation measures and implementation of the action plan

The DPO and the crisis team direct the right people and services within the organisation, and if necessary external service providers, to implement the proposed action plan and envisaged measures. The possible causes of the incident are contained, defects are repaired, possible infections are removed and systems are restored to their original state before the incident.

The DPO will ensure the correct implementation of the action plan and take care of further follow-up.

A detailed report is kept of the implementation of the action plan and the measures.

Every person involved in the implementation of the action plan and/or the measures reports to the DPO on a regular basis.

- Closing the incident

  The DPO can determine if the incident can be closed on the basis of the reports and the discussions at crisis team meetings.

  An incident can be closed if:

  - the situation is under control (or has been reduced to acceptable proportions);
  - the measures implemented achieve the desired effect;
  - there is no longer a risk of violation of the rights and freedoms of the data subject; and
  - legal obligations have been met on time.

  When the incident is closed, the crisis team is dissolved and a communication circulated inside the organisation that the incident has been closed.

  If the situation is under control due to temporary measures, but a definitive measure is necessary to close the incident, the DPO may decide to close the incident subject to implementation of the definitive measure.

- Reports

Every incident must be registered. If the risk is high, the DPO draws up a report on the personal data breach which includes all relevant documents, communications and reports and which explains the nature of the personal data breach, the way it was dealt with, the measures taken, the persons involved, a follow-up report and recommendations for the future.

- Supplementing the register

The DPO adds the details of personal data breaches in a register, stating at least:

- the nature of the personal data breach and the actual circumstances;
- the effects of the personal data breach on the organisation and the rights and freedoms of the data subjects;
- the measures taken; and
- possible recommendations for the future.

IV. Key players regarding the processing of personal data

The managing director

The managing director is ultimately responsible for the general management of the organisation.

The internal privacy policy is an important part of the general management of the organisation. The managing director determines the strategic guidelines, but delegates operational responsibility for physical security and information security to the data protection officer.

The managing director supports the commitment to keep personal data secure.

The management team

The management of each department is responsible for the fair processing of the personal data of their respective departments.

Managers

All managers are responsible for:

- ensuring that all workers and contractors are aware of, understand and comply with the privacy policy;
- collecting information about the effectiveness of security measures and reporting them to the data protection officer;
- informing the data protection officer of any actual and potential violation of the privacy policy with regard to the resources under their responsibility.

Information asset owners

Information asset owners are responsible for securing the company assets assigned to them. They can delegate tasks, but bear the final responsibility for:

- classifying the company assets;
- setting up specific control resources;
- granting access to the company assets, in accordance with the classification;
- participating in or organising security risk assessments to ensure that security requirements are correctly defined and company assets are sufficiently protected.

An information asset owner may ask the data protection officer for a temporary exemption from the security requirements or mitigating circumstances for a company asset. The data protection officer will assess the temporary exemption and accept or reject it depending on the risk. However, the information asset owner is responsible for drawing up an action plan so that the security requirements can nevertheless be met after a period of time.

The data protection officer

Lawyer Jents Debruyne is appointed as data protection officer of PYRAMID NV.

The **data protection officer** is responsible for monitoring and complying with the General Data Protection Regulation. The DPO can be seen as the prime prevention advisor for processing personal data. The DPO's tasks are the following:

- the DPO monitors the new legislation and its obligations; this includes maintaining a register on the processing of personal data; the DPO is also expected to give sufficient information and advice on this theme to the various stakeholders;

- the DPO manages the personal data processing policy and draws up a plan for its implementation and follow-up; in addition, agreements (such as contracts with third parties) are supplemented and the necessary documents drawn up; if a policy plan already exists, the existing system will be supplemented so that the obligations of the General Data Protection Regulation are met;
- the DPO monitors internal controls concerning the processing of personal data and assesses the risks of a violation of the rights of individuals; if a high risk is involved, a privacy impact assessment (PIA) is drawn up; based on this assessment, the DPO advises improvement actions and monitors their status;

- the DPO follows the specific procedures concerning personal data breaches;
- the DPO contributes to the awareness of workers on this subject;
- the DPO monitors changes in legislation concerning the rights of data subjects; in consultation with the IT services involved, the possibilities of integrating these rights into IT systems are studied;

- the DPO is a contact point for the supervisory authority; this used to be the ‘Belgian Privacy Commission’, before it was transformed by law into the ‘Belgian Data Protection Authority’.

The DPO must be independent, meaning the DPO may not determine the means and the purposes of the processing of personal data on which he or she gives advice. Someone from the management team cannot, therefore, act as DPO.

Workers, self-employed services, interim agreements

Workers and contractors are responsible for:

- complying with the security requirements and procedures relevant to their duties and ensuring that this policy and the additional regulations are monitored, in particular the 'safe personnel' policy;
- securing the information entrusted to them.

V. Protection measures

The following chapter discusses the security measures in the internal privacy policy. These ensure that personal data, and in particular the so-called special categories of personal data, is secured as much as possible in an appropriate manner.

The internal privacy policy is supported by the following procedures:

- policy documents: safe personnel, personnel data policy, privacy impact assessment;
- management of company assets and warehouses;
- technical security (cryptography);
- access security;
- physical security;
- security of business operations;
- communication security;
- procedure personal data breaches;
- e-mail policy;
- direct marketing policy, obtaining consent and storing data.

Policy documents

The policy documents and recommendations of the IT manager must be followed up to maximise technical security to the extent possible.

Audit on a regular basis by the data protection officer. Everything will be re-evaluated at least within 2 years;

Enough appropriate and technical measures will be taken;

Confidentiality or non-disclosure agreement
A non-disclosure clause will be added to the policy. A clause relating to the GDPR's safeguards concerning personal data is also being implemented with third parties. If the standard non-disclosure clause is not sufficient for the customer, a supplement can be made in mutual consultation.

Management of company assets

1. Network equipment

A change to network equipment is considered a significant change and must be tested sufficiently and extensively by the IT manager before it is implemented.

Network equipment must be managed using the supplier's management tools.

2. Mobile devices

See the attached mobile device policy.

3. Password policy

It is recommended that complex passwords are used. A strong password policy contains the following requirements:

- the password must not contain any part of the user's (first) name;
- the password must be at least 8 characters long;

- the password must contain 3 of the 4 following characters:
    - uppercase characters;
    - lowercase characters;
    - numbers (0 - 9);
    - special characters (for example: !, $, #, @,%).

Your device may not have a folder/document in which you store your password.
Passwords are changed every 6 months.

4. Technical aspects

The instructions of the IT manager on the technical aspects of security measures are closely followed.

PYRAMID NV strives to maximise information security as much as possible, an area in which it is cooperating with high-quality suppliers;

The following IT security measures are regularly updated:

4 BESCHERMINGSMATRIX

Afhangend van uw type onderhoudscontract, zijn volgende punten voor u van toepassing:

Item	Maatregel	Geactiveerd in uw omgeving
2.1	Firewall	☒
2.2	Monitoring	☒
2.3	Updates	☒
2.4	Antivirus	☒
2.5	Managed Backup	☒srv-gt-dmn, srvsql, srvrdsnew, srv-bxl-dmn
2.5	Local Speedvault	☒
2.5	Backup van laptops	☐
2.6	Office 365	☒
2.6	Office Advanced Threat Protection	☒
3.1	Wachtwoordbeleid: complexiteit	☒
3.1	Wachtwoorden verlopen.	☒
3.2	Beveiliging externe toegang via VPN	☒
3.2	Beveiliging externe toegang remote desktop	☒
3.3	Encryptie Harde Schijven (Bitlocker)	☒
3.4	Werkposten vergrendelen	☒

In addition, PYRAMID NV strives to act as much as possible according to the privacy by design principles and to follow the instructions of the Business Support department.

5. Physical security; access security

The office is secured by doors and registration at the reception. Workers have a personal badge and key.

The server is placed in a separate room with sufficient cooling.

Access rights with respect to the network are sufficiently segmented. These are adjusted per department. Only a limited number of people have access to sensitive information.

6. Communication security

When communicating with external parties, it must always be verified whether the chosen means of communication is right for the type of information to be sent, taking into account the classification of the company asset. At the same time, personal data must always be protected as much as possible.

7. Mobile device policy

Objective

The objective of the mobile device and teleworking policy is to:

- determine what mobile devices may be used;
- describe how mobile devices should be handled;
- ensure the security of using mobile devices;
- describe what forms of teleworking are allowed;
- ensure the security of teleworking.

8. ICT equipment policy

PYRAMID NV gives its workers/contractors individual access to ICT equipment available so that they can carry out their jobs efficiently. This ICT material can consist of, among other things:

- portable computer with accessories (carrying case, power supplies, mouse, etc.);
- smartphone;
- tablet;
- hard drive;
- USB;
- authentication token to work remotely;
- etc.

Mobile devices which are owned by PYRAMID NV must be physically protected by workers and contractors. Mobile devices:

- must not be left unattended; if a device is left unattended for a short time, the device must be locked and password protected; the system will automatically lock a device after 10 minutes of inactivity at the most;
- must not be left unprotected on a desk at night, but stored in a locked locker or taken home;
- must be placed in the locked boot of the car;
- must not be left in a car at night, unless in a garage (even if the devices are in the boot);
- must not be used by third parties;
- may only be used for professional purposes;
- must not be used to store professional information which is not also available on PYRAMID NV's servers (the local hard drive of the mobile devices is not backed up);
- must be protected with a personal login name and password; the password is strictly personal and must not be shared with anyone inside or outside PYRAMID NV; the system requires the worker to make this password sufficiently strong and change it regularly.

The software, patches, security and antivirus software on these devices must be regularly updated. Installing additional software on a portable computer requires approval from the IT manager. Preferably, software required will be supplied.

Workers and contractors may use their own smartphone or tablet for professional tasks, provided they are secured with a PIN code or biometric data.

The user must maintain mobile devices with due care.

Each user is responsible for setting up, managing and securing the devices he or she uses. Users are liable for any use or misuse of this right of use. For security reasons, certain services and websites can be blocked. The user may not use the device in an unauthorised manner or employ it for unlawful purposes/illegal matters, such as harassing others, spreading libellous or discriminatory texts or violating copyrights.

The information stored on these mobile devices must be carefully archived and then deleted when the device is no longer used. If devices are re-used, they will be first examined by the IT manager to ensure they meet security and operational standards.

To conclude: when an employee or any other person suspects there is a security problem, he or she may inform the DPO/competent person.

VI. Monitoring

1. Internal publication

The privacy policy documents can be accessed on the intranet of Pyramid NV and Pauwels Consulting.

2. Evaluations

The following issues will be evaluated annually:

- Is the policy still accurate in terms of personal data?
- Are the security measures still up to date?
- What privacy impact assessments have been executed?
- What security incidents/personal data breaches have occurred?
- Are additional measures required?

A report is drawn up by the DPO at PYRAMID NV.

3. Contact

DPO/competent person: jents@advocaatdebruyne.be - +32 (0)479 50 46 35

Company contact details

PYRAMID NV

Lambroekstraat 5A
1831 Diegem (Belgium)

Tel. +32 (0)9 324 70 80

www.pauwelsconsulting.com