DATA PROTECTION POLICY

This Data protection policy describes how our organization FIT Global handles the Data we collect and Process, and what measures have been taken to protect this Data. We will carefully handle the Data provided to us and collected by us and comply with applicable laws and regulations, including the General Data Protection Regulation (GDPR). Depending on the (sensitivity of the) Data collected, appropriate measures will be taken to prevent infringements.

Index

0. Introduction: The Data protection policy

The right to Data protection is part of the right to the protection of privacy. For our organization, protecting the privacy of our customers, our staff and all other stakeholders is of great importance. We are committed to protecting Personal Data from being misused, getting into the wrong hands as a result of poor security or being shared carelessly, or being inaccurate, as we are aware that people can be upset or harmed if any of these things happen. This policy sets out the measures we are committed to taking as an organization and, what each of us will do to ensure we comply with the relevant legislation. In particular, we will make sure that all Personal Data is:

- Processed lawfully, fairly and in a transparent manner;
- Processed for specified, explicit and legitimate purposes and not in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary for the purposes for which it is being Processed;
- accurate and, where necessary, up to date;
- not kept much longer than necessary for the purposes for which it is being Processed;
- Processed in a secure manner, by using appropriate technical and organisational means.

With this Data protection policy we want to explain how we collect and Process Personal Data, how we try to protect the Data as much as possible and how we implement the rights of the Data Subjects. This policy applies to all Personal Data Processed by our organization and to all Processing goals. This does not only contain the Data of our customers, but also the Data of, for example, our employees, contractors or trainees. This policy text is written for, and therefore applicable to, anyone who Processes Personal Data on behalf of our organization. So this policy is both for the management and for the employees, but also for every contractor or supplier. We ensure that this text is communicated through different channels in our organization.

Responsible for this policy:	Mr Maarten Klein Haneveld
Frequency of review:	annually

1. Definitions

In order to fully understand this Data protection policy, a number of definitions will be explained first. The complete definitions can also be found in the text of the GDPR.

Data Subject:	The natural person whose Personal Data is Processed or to whom the Personal Data relates.
Personal Data or Data:	Any information relating to an identified or identifiable natural person ("Data Subject"). 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.
"Special Categories" of Personal Data:	Data that is extra sensitive in nature, for example Data on health, genetic data (DNA research), biometric data (fingerprint), political opinions and religious beliefs or Data about ethnic origin. For Special Categories of Personal Data higher security levels are required.
Processing:	Any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; ("Process", "Processes" and "Processed" shall have the same meaning).
Controller:	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data. Where the purposes and means of such Processing are determined by Union or Member State law, the Controller or the specific criteria for its nomination may be provided for by Union or Member State law.
Processor:	A natural or legal person, public authority, agency or other body, which Processes Personal Data on behalf of the Controller.

2.Processing of Personal Data

Our organization only Processes Personal Data if there is a legal basis for the Processing. This legal basis is not necessary if the Processing is for private purposes only and thus is not related to business activities, for example keeping an address file for sending invitations for a birthday. In addition, the GDPR only applies if the Processing takes place within the European Union (EU) or if it concerns Personal Data of citizens in the EU.

2.1 Bases for the Processing of Personal Data

There are six bases for the Processing of Personal Data, of which the following 5 bases are important for our organization:

1. Consent of the Data Subject

   Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the Data Subject's agreement to the Processing of Personal Data relating to him or her. The following keywords are of great importance:

   - *Freely given* – this means that the Data Subject must have a genuine choice over whether or not to consent. Consent will not be free in cases where there is any element of compulsion, pressure or inability to exercise free will. Please note: consent is never freely given if the consent is "hidden" in the general conditions or in pre-ticketed boxes.
   - *Specific* – the consent can only be obtained for a specified, determined and legitimate purpose. The Personal Data can thus only be Processed for these specific purposes. If our organization got consent for a specific purpose and want to Process the Personal Data for a new purpose consent needs to be asked again as the explicitly given consent no longer applies.
   - *Informed* – the Data Subject must understand what he/she is consenting to. Our organization must make sure that we clearly and prominently explain exactly what the Data Subject is agreeing to, if this is not obvious. Including information in a dense privacy policy or hidden in "small print" which is hard to find, difficult to understand, or rarely read will not be enough to establish informed consent. The information should include the name of our organization and any third party that Processes the Personal Data, the purposes of the Processing, which Personal Data are Processed and the rights of the Data Subject. This can be done orally or in writing.
   - *Unambiguous indication of the Data Subject's agreement* – consent must be a positive expression of choice. It does not necessarily have to be a proactive declaration of consent. For example, consent might sometimes be given by submitting an online form, if there was a clear and prominent statement that this would be taken as agreement and there was the option to opt out. But we cannot assume consent from a failure to opt out unless this is part of a positive step such as signing up to a service or completing a transaction. However, we cannot assume consent from non-response to an email, as this would not be a positive indication of agreement. Proactive declarations of consent are for example: written or oral statements, including by electronic means, like ticking a box when visiting an internet website, choosing technical settings for information society services or any another statement or conduct which clearly indicates in this context the Data Subject's acceptance of the proposed Processing of his or her Personal Data.

   It is also important that consent can be withdrawn at any time, after which the Personal Data may no longer be Processed.

Note: Persons under the age of 16 cannot give valid consent. In that case consent must be obtained from the legal representative.

2. Vital interests

   This means that the Processing of Personal Data is necessary to protect a vital interest (something essential for the life or health) of the Data Subject or a third party, but the Data Subject cannot be asked for consent. If the Data Subject is capable (both in law and in practice) of giving consent to the Processing, that justification should be preferred. Protecting someone's life is a legitimate basis for the Processing of Personal Data.

3. Legal obligation

   This legal basis covers Processing of the Personal Data that is necessary to fulfil a legal obligation to which our organization is subject. The obligation must be set out in Union or Member State law, must meet an objective of public interest and must be proportionate. Examples include obligations in the fields of employment and social security, including those that require Processing sensitive (now known as "Special Category") Personal Data or the provision of Data for tax purposes. The fact that the Processing of Personal Data is necessary to comply with the legal obligation does not, however, have to be explicitly stated in the law. After all, this depends on the interpretation of the law. It is then up to our organization to determine whether the Processing of the Personal Data is necessary for compliance with the legal obligation.

4. Agreement

   A fourth ground for the Processing of Personal Data concerns the execution of an agreement, for which the Processing of Personal Data is necessary (i.e. there is no less intrusive way to perform the agreement). This does not concern an agreement with the aim to Process Data, but an agreement that is concluded for another purpose. This can be either for an existing agreement to which the Data Subject is a party, or in preparation to enter into a agreement at the Data Subject's request and includes exporting Personal Data where that is a necessary part of the agreement. Note that in Dutch law "agreements" are not limited to those on paper, so this justification is also likely to cover less formal agreements between a Data Subject and a Controller.

   Please note: on this legal basis our organization may only Process Personal Data that are necessary for the execution of that agreement. To illustrate: if a person has purchased a service from us, then we need the address details of that person to be able to send an invoice for the services provided. This is part of the execution of the agreement. Please note that we may not use this Data for market research. In that case (separate!) valid consent must be obtained.

5. Legitimate interest

   This legal basis covers Processing that is necessary for a legitimate interest of the Controller or a third party, provided that interest is not overridden by the interests and rights of the individual. Therefore three conditions must be met:

   - FIT Global B.V. has a legitimate interest – such an interest must be lawful and clearly specified. This is the case if the Processing of the Personal Data is necessary for the performance of our business activities. A good example of this is conducting personnel administration.
   - The Processing of the Personal Data is necessary to represent this legitimate interest – for this second condition the Processing must be checked against the requirements of proportionality and subsidiarity. In short, this means that we must test whether the

purpose of the Data Processing is proportionate to the infringement that is made on the Data Subjects and whether it can be achieved in a less impactful manner;

- We have weighed our interests and those of the Data Subject - Processing is only permitted if our interests outweigh those of the Data Subject whose Data are Processed. It is also important that measures are taken to ensure that the rights and freedoms of the Data Subjects are guaranteed as far as reasonably possible. This means, among other things, that we may not store the Data for longer than is necessary for the purpose of the Processing.

Examples include Processing necessary to detect fraud or report criminal activity, to protect network and information security, for internal administration in a corporate group or not-for-profit organization.

Accountability is one of the Data protection principles. It makes our organization responsible for complying with the GDPR and expects us to be able to demonstrate our compliance. We as organization must demonstrate that we are compliant with the law. Such measures include: (i) adequate documentation on what Personal Data are Processed, how this Data is Processed, to what purpose and for how long; (ii) documented Processes and procedures aiming at tackling Data protection issues at an early state when building information systems or responding to a Data breach; (iii) the (possible) presence of a Data Protection Officer to be integrated in the organization planning and operations etc. This accountability applies as long as the Data Processing takes place. There is no prescribed way to comply with this obligation. The way in which this is recorded depends, of course, on our business operations and the nature of the Data Processing. The recording of Processing activities is an option (see paragraph 3 of this data protection policy).

2.2 Bases for the Processing of "Special Categories" of Personal Data

Our organization does not intend to Process "Special Categories" of Personal Data. This is also not permitted, unless it is possible to invoke a statutory exception **and** one of the bases for the ordinary Data Processing as described in 2.1.

In case we start collecting and Processing "Special Categories" of Personal Data in the future, eight out of ten exceptions for Processing "Special Categories" of Personal Data can apply within our organization:

1. The Data Subject has given **explicit consent** to the Processing of those Personal Data for one or more specified purposes;
2. Processing is necessary for the purposes of **carrying out the obligations and exercising specific rights** of ours or of the Data Subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the Data Subject;
3. Processing is necessary **to protect the vital interests** of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent;
4. Processing relates to Personal Data which are **manifestly made public by the Data Subject**;
5. Processing is necessary for the **establishment, exercise or defence of legal claims** or whenever courts are acting in their judicial capacity;

6. Processing is necessary for **reasons of substantial public interest**, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to Data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject;
7. Processing is necessary for the purposes of **preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services** on the basis of Union or Member State law or pursuant to contract with a health professional;
8. 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, respect the essence of the right to Data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject.

2.3 Collected Data

If Personal Data is collected directly from the Data Subject, we will inform his/her about:

- Our identity/contact details;
- The reasons for Processing and the legal bases, explaining our legitimate interests, and explaining, where relevant, the consequences of not providing Data needed for a contract or statutory requirement;
- Who we will share the Data with;
- If we plan to send the Data outside of the European Union;
- How long the Data will be stored; and
- The Data Subject's rights.

This information is commonly referred to as a "Privacy Statement". This information will be given at the time when the Personal Data is collected.

If Data is collected from another source, rather than directly from the Data Subject, we will provide the Data Subject with the information described above as well as: the categories of the Data concerned; and the source of the Data. If we use the Data to communicate with the Data Subject, we will at the latest give him/her this information at the time of the first communication.

2.4 Agreements with Processors

A Data Processing Agreement will be concluded if FIT Global B.V. uses Processors for the Processing of Personal Data. In every Data Processing Agreement it is expressly provided that the Data Processor:

- only acts on the Controller's documented instructions, unless Union or Member State law to which the Processor is subject, determines otherwise;
- imposes confidentiality obligations on all personnel involved in Processing the relevant Data;
- must ensure the security of the Personal Data by implementing the measures (see last month's update);
- abides by the rules regarding the engagement of Sub-Processors (prior authorization needed of the Controller and Sub-Processors must be appointed on the same terms as are set out in the contract between the Controller and the Data Processor);

- assists the Controller, where possible, with implementing measures to comply with the rights of Data Subjects;
- at the Controller's request, either returns or destroys the Personal Data at the end of the agreement, except as otherwise required by Union or Member State law; and
- provides the Controller with all information necessary to demonstrate compliance with the GDPR.

3. Records of Processing activities

Article 30 of the GDPR requires the Controller – and to a lesser extent the Processor – to keep records of the Processing operations they carry out. There is one exception: companies and organizations employing less than 250 employees are exempt from the obligation to register, *unless* the Processing is risky, the Processing is not incidental, or the Processing concerns special categories of Personal Data or criminal Data.

Although on the basis of the foregoing our organization is not obliged to keep records of the Processing operations we carry out, we decided to do so. In our organization there is a non-recurring Processing of Personal Data, such as keeping payroll records, a customer Database, and even the use of e-mail. In other words, the exception has so many hooks and eyes that hardly anyone falls under it, and therefore we make sure we comply with this obligation. Furthermore, keeping clear records of our Processing activities enables us to show how we comply with the law and of the decisions we make concerning Personal Data (setting out our reasons for those decisions).

A model of the records is attached to this Data protection policy in **annex 1**. These records must contain all of the following information:

- The name and contact details of the Controller and where applicable, the Data Protection Officer;
- The purposes of the Processing and the legal bases;
- A description of the categories of Data Subjects and of the categories of Personal Data;
- The categories of recipients to whom the Personal Data have been or will be disclosed including recipients in third countries or international organizations;
- The transfers of Personal Data to a third country or an international organization, including the documentation of suitable safeguards;
- The envisaged time limits for erasure of the different categories of Data; and
- A general description of the applied technical and organisational security measures.

4. Privacy by design & Privacy by default

In the GDPR, Privacy by Design is an explicit requirement for the Processing of Personal Data (article 25 GDPR). Privacy by Design states that any action a company undertakes that involves Processing Personal Data must be done with Data protection and privacy in mind at every step (from the earliest design stages to the operation of the productive system). This includes internal projects, product development, software development, IT systems, and much more. In practice, this means that the IT department, or any department that Processes Personal Data, must ensure that privacy is built in to a system during the whole life cycle of the system or Process.

Privacy by Default means that once a product or service has been released to the public, the strictest privacy settings should apply by default, without any manual input from the end user. In addition, any Personal Data provided by the user to enable a product's optimal use should only be kept for the amount of time necessary to provide the product or service. In that regard, privacy by default is about the standard settings of our systems, processes, services and products. These settings should be in such way that the privacy of the Data Subject is protected as well as reasonably possible, without this being at the expense of the overall user-friendliness of our systems.

Measures to keep the Personal Data of the Data Subject secure:
We will use appropriate measures to keep Personal Data secure at all points of the Processing. Keeping Data secure includes protecting it from unauthorised or unlawful Processing, or from accidental loss, destruction or damage. We will implement security measures which provide a level of security which is appropriate to the risks involved in the Processing. Measures will include technical and organisational security measures. In assessing what measures are the most appropriate we will take into account the following, and anything else that is relevant:

- the quality of the security measure;
- the costs of implementation;
- the nature, scope, context and purpose of Processing;
- the risk (of varying likelihood and severity) to the rights and freedoms of Data Subjects;
- the risk which could result from a Data breach.

Measures may include:

- technical systems security;
- measures to restrict or minimise access to Data;
- measures to ensure our systems and Data remain available, or can be easily restored in the case of an incident;
- physical security of information and of our premises;
- organisational measures, including policies, procedures, training and audits;
- regular testing and evaluating of the effectiveness of security measures.

Examples

- **Data minimization.** Our organization is committed to Data minimization. Data minimization means that only those Personal Data will be collected that are necessary for the purpose of Data Processing. There should be no excessive Data collection.
- **Opt-in instead of opt-out.** The Data Subject is not approached for certain purposes, unless the Data Subject has explicitly indicated that he / she wishes to be approached.
- **Data Processing Agreements.** We conclude Processing agreements with third parties when third parties Process Personal Data on behalf of us.

Data retention
We will retain Personal Data for the period necessary to fulfill the purposes for which the Personal Data was collected in the first place and will not store this information for more than five (5) year after the Data is no longer necessary or those purposes, provided that no legal requirements exist to the contrary such as in the case of retention periods required by law.

Security measures have been implemented to the best knowledge of our organization or our partners at the time of drafting this policy or prior to this.

5. Data Protection Impact Assessments (DPIA)

In some cases, a risk analysis called "Data protection impact assessment" (DPIA) must be performed prior to a Processing activity that (might) contains a high risk for the Data Subject. The DPIA helps us to understand the privacy risks and enables us to take measures to reduce such risks. Organizations are not obliged to perform a DPIA for each Data Processing. A DPIA is only mandatory if Data Processing is likely to pose a high privacy risk for the Data Subjects. The decision whether a DPIA is necessary or not is up to our organization. When we are planning to carry out any Data Processing that is likely to result in a high risk we will carry out a DPIA. These include situations when we Process Data relating to vulnerable people, trawling of Data from public profiles, using new technology, and

transferring Data outside the EU. Any decision not to conduct a DPIA will be recorded. We may also conduct a DPIA in other cases when we consider it appropriate to do so. DPIAs will be conducted in accordance with the ICO's Code of Practice 'Conducting privacy impact assessments'. The Working Party Guidelines on Data Protection Impact Assessment (DPIA) and determining whether Processing is 'likely to result in a high risk' for the purposes of Regulation (EU) 2016/679, 4 April 2017, can help us in making that decision. The relevant Data Processing criteria are as follows:

1. **Evaluation or scoring**, including profiling and predicting, especially from "aspects concerning the Data Subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements". Examples of this could include a bank that screens its customers against a credit reference Database, or a company building behavioural or marketing profiles based on usage or navigation on its website.
2. **Systematic monitoring**: Processing used to observe, monitor or control Data Subjects, including Data collected through "a systematic monitoring of a publicly accessible area". This type of monitoring is a criterion because the Personal Data may be collected in circumstances where Data Subjects may not be aware of who is collecting their Data and how they will be used. Additionally, it may be impossible for individuals to avoid being subject to such Processing in frequent public (or publicly accessible) space(s).
3. **Data Processed on a large scale**: the GDPR does not define what constitutes large-scale, though the Working Group provides some guidance. In any event, the Working Group recommends that the following factors, in particular, be considered when determining whether the Processing is carried out on a large scale:
    - the number of Data Subjects concerned, either as a specific number or as a proportion of the relevant population;
    - the volume of Data and/or the range of different Data items being Processed;
    - the duration, or permanence, of the Data Processing activity;
    - the geographical extent of the Processing activity.
4. **Automated-decision making with legal or similar significant effect**. In this case the Processing aims at taking decisions on Data Subjects producing "legal effects concerning the natural person" or which "similarly significantly affects the natural person". For example, the Processing may lead to the exclusion or discrimination against individuals. Processing with little or no effect on individuals does not match this specific criterion.
5. **Sensitive Data**: this includes Special Categories of Data, as well as Personal Data relating to criminal convictions or offences. An example would be a general hospital keeping patients' medical records or a private investigator keeping offenders' details. This criterion also includes Data which may more generally be considered as increasing the possible risk to the rights and freedoms of individuals, such as electronic communication data, location data, financial data (that might be used for payment fraud). In this regard, whether the Data has already been made publicly available by the Data Subject or by third parties may be relevant. The fact that Personal Data is publicly available may be considered as a factor in the assessment if the Data was expected to be further used for certain purposes. This criterion may also include information Processed by a natural person in the course of purely personal or household activity, whose disclosure or Processing for any other purpose than household activities can be perceived as very intrusive.
6. **Datasets that have been matched or combined**. For example originating from two or more

Data Processing operations performed for different purposes and/or by different Controllers in a way that would exceed the reasonable expectations of the Data Subject.

7. **Data concerning vulnerable Data Subjects**: the Processing of this type of Data can require a DPIA because of the increased power imbalance between the Data Subject and the Controller, meaning the individual may be unable to consent to, or oppose, the Processing of his/her Data. For example, employees would often meet serious difficulties to oppose to the Processing performed by their employer, when it is linked to human resources management. This also concerns more vulnerable segment of the population requiring special protection, such as, for example, the mentally ill, asylum seekers, or the elderly, a patient, or in any case where an imbalance in the relationship between the position of the Data Subject and the Controller can be identified.
8. **Innovative use or applying technological or organisational solutions**, like combining use of finger print and face recognition for improved physical access control, etc. The GDPR makes it clear that the use of a new technology can trigger the need to carry out a DPIA. This is because the use of such technology can involve novel forms of Data collection and usage, possibly with a high risk to individuals' rights and freedoms. Indeed, the personal and social consequences of the deployment of a new technology may be unknown. A DPIA will help the Controller to understand and to treat such risks.
9. **Data transfer across borders outside the European Union**, taking into consideration, amongst others, the envisaged country or countries of destination, the possibility of further transfers or the likelihood of transfers based on derogations for specific situations set forth by the GDPR.
10. **When the Processing in itself prevents Data Subjects from exercising a right or using a service or a contract**. This includes Processings performed in a public area that people passing by cannot avoid, or Processings that aims at allowing, modifying or refusing Data Subjects' access to a service or entry into a contract. An example of this is where a bank screens its customers against a credit reference Database in order to decide whether to offer them a loan.

Does the Data Processing meet criteria mentioned in points 1, 2 or 3? Then we perform a DPIA. For the other criteria, we adhere to the general rule that a DPIA will be mandatory if the Data Processing meets two or more conditions. Nevertheless, it can happen that we decide not to execute a DPIA anyway. In that case we ensure that our decision can be substantiated and that this is recorded in writing.

It is of course also possible to carry out a DPIA on a voluntary basis. This promotes Data protection and encourages reflection on the impact of the Processing on the privacy of the Data Subjects and the possibility of choosing an (alternative) approach with a less drastic impact on privacy.

NOTE: the execution of a DPIA may also be mandatory for an existing Processing. This is the case if a change results in Data Processing (after the change) presenting a high privacy risk. For that reason, we ensure periodic testing whether the execution of a DPIA is compulsory.

6. Data Protection Officer (DPO)

In some cases, it is mandatory to appoint a Data protection officer (DPO). A DPO is an enterprise security leadership role required by the GDPR. DPO's are responsible for overseeing Data protection strategy and implementation to ensure compliance with GDPR requirements.

In the three situations below, we are obliged to appoint an DPO.

- If our organization conducts large-scale Processing of Special Categories of Personal Data, like health details or information about ethnicity or religious beliefs;
- If the core activities of our organization involve regular and systematic monitoring of Data Subjects on a large scale;
- For government agencies or public authorities (i.e. healthcare and educational institutions).

This is not the case for our organization; we therefore have **no** obligation to appoint an DPO. Therefore, no DPO has been appointed within our organization.

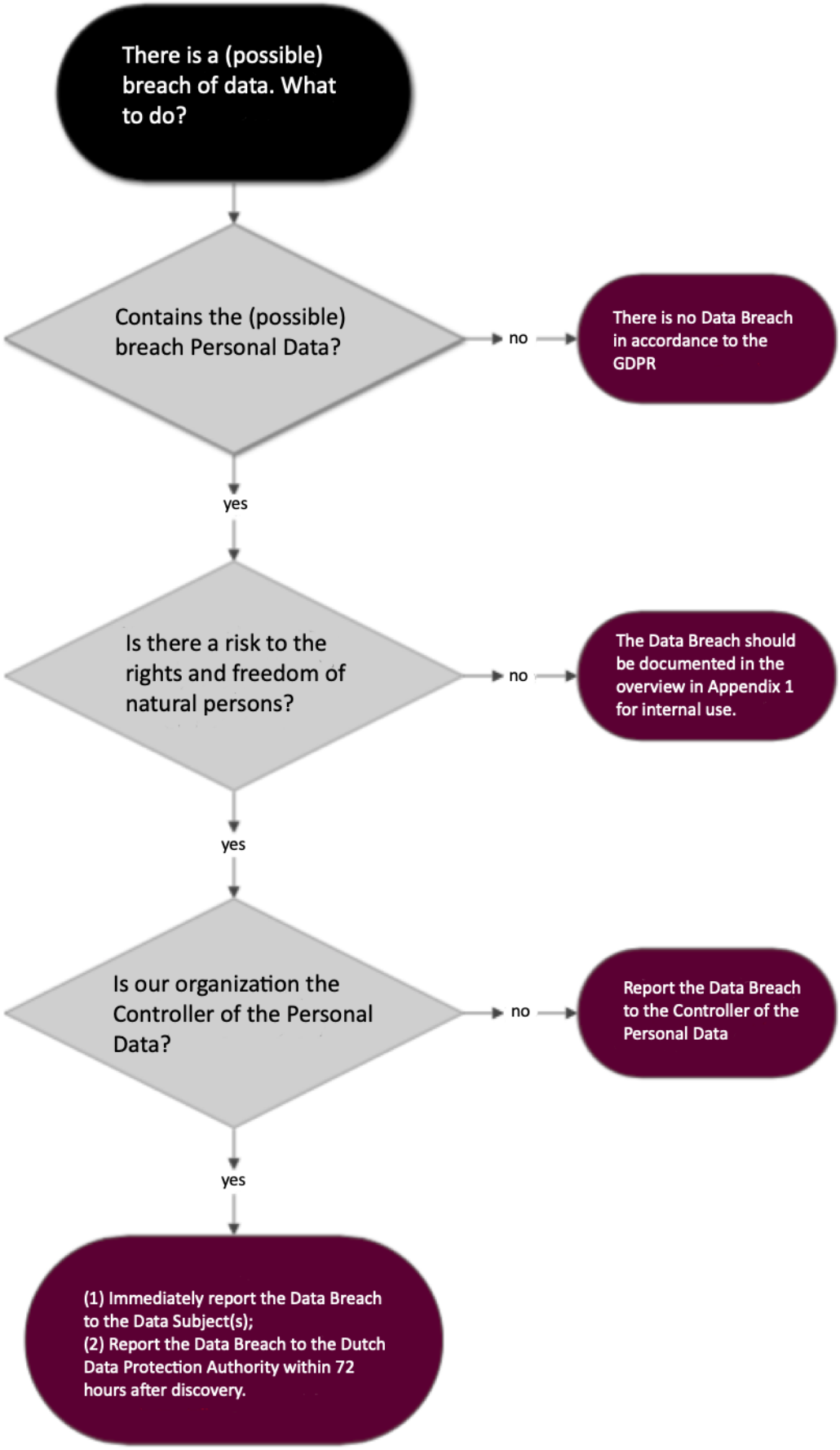
If at any time we decide to appoint a (then) mandatory or voluntary DPO, we will report the DPO to the Dutch Data Protection Authority (DPA). This can be done via the website of the DPA. As outlined in the GDPR Article 39, the DPO's responsibilities include, but are not limited to, the following:

- Educating the company and employees on important compliance requirements;
- Training staff involved in Data Processing;
- Conducting audits to ensure compliance and address potential issues proactively;
- Serving as the point of contact between the company and GDPR Supervisory Authorities;
- Monitoring performance and providing advice on the impact of Data protection efforts;
- Maintaining comprehensive records of all Data Processing activities conducted by the company, including the purpose of all Processing activities, which must be made public on request;
- Interfacing with Data Subjects to inform them about how their Data is being used, their rights to have their Personal Data erased, and what measures the company has put in place to protect their Personal Data.

The concrete knowledge level that a DPO must have will depend on the Data Processing that our organization is then performing. It is also important that there should never be a conflict of interest; the DPO must be able to work independently at all times.

7. Data breach

We have drawn up a protocol that must be followed in case of a (suspected) Data Breach.



7.1 Data has been leaked. When there is a Data Breach?

What is a Data Breach? A Data Breach means an "*infringement in connection with Personal Data*". This concerns a breach of security that results in the destruction, loss, modification, unauthorized disclosure or unauthorized access to transmitted, stored or otherwise Processed Personal Data. It does not matter whether the infringement occurred accidentally or deliberately. Some examples of Data Breaches: an unlatched computer while a third party is passing, a stolen hard disk or USB, a break-in to a Data system, an error-send email, several (unintended) addressees in the CC of an email, a hacked system.

There is only a Data Breach if a security incident has actually taken place and/or Personal Data have (or could have) come into the possession of third parties. Please note: a vulnerability in security, the so-called "security breach", is not a Data Breach. The security incident must have actually occurred, whereby the preventive measures taken have not been sufficient to prevent this.

7.2 What is Personal Data?

Personal Data is "*all information about an identified or identifiable natural person; an identifiable natural person who can be identified directly or indirectly, in particular by means of an identifier such as a name, an identification number, location data, an online identifier or one or more elements characteristic of the physical, physiological, genetic, psychological, economic, cultural or social identity of that natural person*".

In short, it concerns information that directly says something about a person or can be traced back to a person in a certain way. So, it is Data with which we can designate a specific person in a particular group. This goes beyond just the name and address details of a person. Information like "*the man with blonde hair who had an appointment at our office in Oosterhout on May 15, 2018 at 11:00*" is Personal Data. The same applies to "online identifiers", such as IP addresses or tracking cookies. Based on this information, we know or are able to know who that person is. Only when it is reasonably no longer possible to identify a person with the available information and resources the information does not (longer) qualify as Personal Data.

Data of deceased persons, legal entities and anonymous data are not Personal Data. This does not mean, however, that this information can just be made public.

7.3 When is there a risk to the rights and freedom of natural persons?

No explicit rules are known for this. This is a consideration that we as an organization must make. A factor that plays a role in this is the nature of the breached Personal Data; if Personal Data of a sensitive nature is breached, there is generally a risk to the rights and freedoms of the natural person. Some examples of Personal Data of a sensitive nature are:

- **Special Categories of Personal Data.** This includes, but is not limited to, Data on a person's religion or belief, race, political health, criminal data.
- **Financial data.** This is Data on, amongst other things, but not exclusively, the debts of the Data Subject(s), salary and payment Data or other Data about the economic situation of the Data Subject(s).
- **Data on personal characteristics.** This includes profiling and making prognoses on the basis of characteristics.
- **(Other) data that may lead to stigmatization or exclusion of the Data Subject(s)**. For example: information about work performance.
- **User names, passwords and other log-in Data.** The possible consequences for Data Subject(s) depend on the Processing of Personal Data to which the log-in data give access.

- **Information that can be used for (identity) fraud.** For example, a copy of an identity card in combination with the BSN.

Also, other factors, such as the amount of Personal Data that has been leaked per person, may result in a high risk for the rights and freedoms of natural persons.

7.4 Reporting to the Dutch Data Protection Authority

In principle, the Controller must report any Data Breach to the Dutch Data Protection Authority within 72 hours. Such a report will be made by the management of our organization or by the person responsible for this policy, unless this is not reasonably possible. In that case, it will be determined in joint consultation who will make the report to the Dutch Data Protection Authority. The 72-hour period starts running as soon as we know as an organization that there is a Data Breach. Only in case it is unlikely that the Data Breach impose a high risk to the rights and freedoms of natural persons the reporting to the Dutch Data Protection Authority is not deemed to be necessary.

If it is not possible to make a report to the Dutch Data Protection Authority within 72 hours, we will have to do this as soon as possible and include a statement for the delay.

7.5 Reporting to the Data Subject(s)

If it is established that there is a Data Breach and that this Data Breach involves a high risk for the rights and freedoms of the Data Subject(s), we must immediately inform the Data Subject(s). Some time may be taken to investigate the Data Breach and, if necessary, measures may be taken first to prevent further damage. The report must be made as quickly as possible to the Data Subject(s), so that the Data Subject(s) will also be able to limit the damage (for example by changing a password). Such a report will be made by the management of our organization or by the person responsible for this policy, unless this is reasonably not possible. In that case, it will be decided in joint consultation who will make the report to the Data Subject(s).

Data Subject(s) doesn't/don't need to be informed when:

- appropriate technical and organizational protection measures have been taken, for example encryption of the Data;
- measures have been taken afterwards to remove the identified risks for the Data Subject(s);
- the communication to the Data Subject(s) in question would cost a disproportionate amount of effort. In that case, a public announcement will be sufficient, for example: publishing information on the website.

Furthermore, a Data Breach does not have to be reported to the Data Subject(s) if the absence of such notification is necessary for:

- national security;
- national defense;
- public security;
- the prevention, investigation, detection and prosecution of criminal offenses, and the execution of criminal penalties;
- other important public interest objectives as determined by the European Union or a Member State;
- the protection of the independence of the judge and legal proceedings;
- the prevention, investigation, detection and prosecution of violations of professional codes for regulated professions;
- a task in the area of supervision, inspection or regulation relating to the exercise of an official authority;
- the protection of the Data Subject(s) or the protection of the rights and freedoms of others;

- the collection of civil claims.

7.6 What information should be given in the notification?

The following information must be provided in the notification to the Dutch Data Protection Authority:

- The nature and extent of the infringement (Data Breach);
- If possible, the categories of Data Subject(s), the Personal Data in question and - approximately - the number of Data Subjects and Personal Data registers concerned;
- The name and contact details of the person within our organization who can be contacted if more information is desired;
- The probable consequences of the Data Breach in relation to Personal Data;
- The measures that we have proposed or taken to address the Data Breach in relation to Personal Data, including, where appropriate, the measures to mitigate any adverse consequences.

For the notification to the Data Subject(s) it is important that this is drawn up in clear and simple language and that the following information is provided:

- A description of the nature of the infringement (Data Breach);
- The name and contact details of the person within our organization who can be contacted if more information is required;
- The likely consequences of the infringement (Data Breach) for the Data Subject(s);
- The measures we have proposed or taken to address the Data Breach, including the measures to limit the possible adverse consequences.

7.7 Registration of the Data Breach

It is mandatory to document or register all Data Breaches. This registration must in any case contain the facts about the infringement and its consequences. Furthermore, it is wise to register the measures taken. **Appendix 1** to this Data protection policy contains an example of how Data leaks can be documented.

Every employee, contractor, trainee or other person involved with our organization, who observes a Data Breach, is obliged to report this to the management or to the person responsible for this policy, by means of the form in the appendix, or in the absence of the management and the person responsible for this policy to the person who is then the next responsible within our organization. The management, the person in charge of this policy or the replacement in question, will then - if necessary - assess how to act on the basis of this protocol.

8. Data Subject Requests

The introduction of the GDPR has expanded the rights of the Data Subjects. It is important that employees within our organization are aware of those rights.

- *Access their Personal Data*
  Data Subjects have the right to access the Personal Data we collect and may obtain a copy of this Data by contacting us. Our aim is to provide the Data Subject with this information within 72 hours after receiving the written request.
- *Rectification*
  Data Subjects have the right to have Personal Data rectified if it is incomplete and/or erroneous and can make a request for rectification by contacting us. Our aim is to implement a rectification within 72 hours after receiving the written request.
- *Erasure*
  In some circumstances, Data Subjects have the right to the erasure of their Personal Data. Those circumstances include:
  - The Personal Data are no longer necessary in relation to the purposes for which they were collected and/or Processed;
  - The Data Subject withdraw the (explicit) consent he/she previously provided to Process the information;
  - The Data Subject object to the Processing of his/her Personal Data and has legitimate, compelling reasons which supersede our interests and reasons for Processing his/her Data;
  - The Data Subject object to his/her Personal Data being Processed for direct marketing purposes;
  - The Data Subject is below the age of 16 and our website has collected his/her Personal Data;
  - We are obligated to delete the Personal Data of the Data Subject after the time limits set by laws or other regulations;
  - There are (no longer) any legal grounds for Processing the Personal Data of the Data Subject.

  Our aim is to respond as quickly as possible to a request for removal of the Personal Data, but at least within 72 hours after receiving the written request.
- *Data minimization*
  Data Subjects reserve the right to minimize the Processing of their Personal Data. If we are informed that we are using incorrect Personal Data, we will not use this Data until it has been rectified. We will furthermore restrict Processing Data if the Processing is either unlawful or no longer necessary, or the Data Subject opposes the erasure of its Personal Data and instead request the restriction of their use.
- *Data portability*
  Data Subjects reserve the right to Data portability, i.e. to receive the Personal Data concerning the Data Subject that the Data Subject has provided to us. We will send this information to a Data Subject at a Data Subject's request. Our aim is to provide the Data Subject with this information within 72 hours after receiving the written request.

---------- end of document ----------