GUIDE TO THE GENERAL DATA PROTECTION REGULATION

GDPR

December 4, 2018

Table of Contents

1 Introduction

This document describes the model adopted by STANDARD PROFIL for the management of personal data protection regulations and the actions that are necessary for the maintenance of said model over time.

This model is established in STANDARD PROFIL in order to implement a true culture of compliance in the organization, and reaffirm compliance with the Law and the European Data Protection Regulation (hereinafter, GDPR).

2 Data Protection Model

Below are the components of the RGPD and the activities to be carried out to ensure its correct maintenance and updating.

2.1 Data processing and Records of Processing Activities

A **data treatment** is defined as: "*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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*".

When there is a substantial change in a treatment or a new treatment is identified, it will be necessary to update or create the Record of Processing Activities. This record contains the basics of each treatment and whose content is regulated in art. 30 of the GDPR. The information will be stored in the GlobalSUITE application in the inventory option → properties of each of the treatments.

It will be necessary to complete all the fields of the record.

It may generate a report for each of the treatments for displaying the information of the record completely, because the information of the record of activities, risk assessment and risk analysis combined. To do so, select the option Treatments → select Download button → RAT report.

2.1.1 Principles relating to treatment

If there has been any change in treatment or a new treatment has begun, it is necessary to analyze or update the following aspects:

- Data that make treatment are the necessary for its realization and there is no data that does not contribute and that may be excessive.
- For what purposes are the data to be used. Among others we can name the following:
    - Personnel management [recruitment, payroll, risk prevention, internal promotion, presence, etc.]

- Accounting management [billing, tax settlement, accounting, etc.]
- Customer management [billing services, payment of taxes, fraud management, advertising, communication, etc.]
- Video surveillance
- Geolocation [location of vehicle fleets, location of employees, location of patients, etc.]
- Health History [health history, appointments]
- Educational management [file of the students, additional services provided in the entity, etc.]

- The legal provisions that apply, which require a minimum period of conservation, will be taken into account:

Law	Documents	Retention period
Article 21 of Royal Legislative Decree 5/2000, of August 4, approving the revised text of the Law on Infractions and Sanctions in the Social Order	LABOR DOCUMENTATION OR RELATED TO SOCIAL SECURITY Documentation, records or computer media in which the data have been transmitted to prove compliance with the obligations regarding affiliation, registrations, cancellations or variations that may take place in relation to said matters, as well as the contribution documents and the receipts justifying the payment of salaries and the delegated payment of benefits. Add all contractual documentation.	4 years
Art. 30 Commercial Code	ACCOUNTING AND FISCAL DOCUMENTATION For mercantile purposes: Books, correspondence, documentation and supporting documents concerning your business, duly ordered from the last entry made in the books, except for what is established by general or special provisions. This mercantile obligation extends to both the mandatory books (income, expenses, investment goods and provisions) and the documentation and supporting documents recorded in the books (invoices issued and received, tickets, corrective invoices, bank	6 years

Law	Documents	Retention period
	documents , etc.).	
Articles 66 to 70 General Tax Law	ACCOUNTING AND FISCAL DOCUMENTATION For tax purposes: The accounting books and other mandatory books according to the applicable tax regulations (IRPF, VAT, IS, etc.), as well as the documentary supports that justify the entries recorded in the books (including computer programs and files and any other proof that has fiscal significance), must be kept, at least, during the period in which the Administration has the right to check and investigate and, consequently, to settle tax debt.	4 years
Article 17.1 of Law 41/2002 of November 14, on patient autonomy and rights and obligations regarding information and clinical documentation	MEDICAL HISTORY The health centers have the obligation to preserve the clinical documentation under conditions that guarantee their correct maintenance and safety, although not necessarily in the original support, for the proper assistance to the patient during the appropriate time in each case and, at least, five years counted from the date of discharge of each healthcare process.	5 years

- The legality of the treatment, based on the assumptions authorized by the data processing law, must be adjusted to any of the following legal bases:
    - **Contractual relationship,** existence of a contract or the intention to conclude a contract between the parties.
    - **Vital interests of the interested party or of other persons.** Protection of a vital interest for the life of the interested party. It corresponds normally with public or health interests, such as in the case of emergencies, epidemics, etc.
    - **Legal obligation for the Data Controller.** There is an applicable legal standard that authorizes the treatment. The same standard can serve as a basis for several related treatments.

- **Public interest or exercise of public powers.** When a public or other body that carries out activities of public interest, perform the assigned functions that are defined in the applicable legislation.

- **Legitimate interest prevailing of the Data Controller or of third parties to whom the information is communicated**. When there is a relationship between the interested party and the Data Controller, and it is reasonably foreseen that further treatment will take place, either because the interested party's data have to be used to pursue a lawful purpose, such as prevention of fraud, because they will be used for direct marketing purposes, because they will be communicated to companies in a group, etc. It must always be borne in mind that a legitimate interest will not be considered to exist when the interest, rights or freedoms of the interested party prevail.

When during treatment additional purposes that are compatible with the purpose of initial collection are added, an additional legal basis to make lawful the treatment is not necessary. Therefore, when we detect that new uses of current treatments are being made, this point should be analyzed. If they were purposes incompatible with the original treatment, a new treatment must be registered.

2.1.2 Consent and information

It is defined as **consent**: "*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*"

The consent and the information to gather the data are very important and the following aspects have to be taken into account:

- You have to take into account how you are going to make the consent request:

  - Sensitive data, international transfers and automated decisions must have an express and unequivocal consent.

  - In the case of other data, it must be an informed consent and must not be done through tacit consent.

  - It is necessary to store the consent and have proof of the provision thereof. It will be necessary to differentiate, according to the medium of provision, the type of storage: database of the website where it is evidenced that the privacy policy is accepted, form completed and signed, recording of the telephone conversation, SMS, email, etc.

- Information, information clauses have to meet the following requirements:

  - The existence of the file or treatment, its purpose and recipients.

  - The mandatory nature or not of the response, as well as its consequences.

  - The possibility of exercising ARCO rights.

- The identity and contact details of the person responsible for the treatment.
- The contact details of the DPO, when the appointment is made.
- The term or criteria for the conservation of information.
- The existence of automated decisions or profiling.
- The forecast of transfers to Third Countries.
- The right to file a claim with the Control Authorities.

So, if it is a review, we must re-check the information clause and the form of consent request, to ensure that it is done according to the new situation.

We will be able to offer the necessary information in two layers, this means that in a first moment in the collection of the data we will inform the interested person succinctly and in a second moment in an extensive way. This can be done in the following way depending on the collection medium used, for example:

Data request form. We will have a table with the basic information that should be placed in the same field of vision as the place where there is to show compliance with the request (the signature, if it is on paper, or the "send" button, if it is a form electronic), forming part of the copy that is available to the interested party. The second layer can be presented by referring to a web page that can be accessed by the interested party, on the back of the form or through a link if we are in an electronic form.

Other display options of the second layer of information:

* Additional information on paper:
  - In the same completed form (for example, on the back).
  - As an annex that is given to the interested party and that can keep it.
  - As information exposed, clearly visible, on posters, panels, triptychs, etc., of which a copy may be requested to preserve.
* Additional electronic information:
  - On a specific web page, which is accessed through a hyperlink.
  - As a document available for download from a URL.
  - As information attached to an e-mail addressed to the interested party.
* Additional telephone information:
  - As a locution that is offered to the interested party, as a complement or alternative to an offer of availability of additional information electronically accessible or sent by postal or electronic mail.

In the GlobalSUITE “Document Manager” option, there are models for its use.

2.1.3 Data Processor

The Data Processor is defined as: *a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.*

In the case of changing a person in charge of processing or hiring a new one, a service provision contract must be signed. It must be ensured that the following considerations are included:

1. Purpose: describe the provision of the service and the type of treatment that is carried out (consultation, restructuring, etc.).

2. Duration: the duration of the provision of the service must be defined, especially if it is renewable or not.

3. Type of personal data and categories of interested parties: describe the type of data included in the file. Eg. Identification data, financial data, sensitive data, etc. In addition, it will describe which interested parties are affected. Eg. Clients, employees, suppliers, students, etc.

4. Obligation of the Data Processor of processing personal data only following the documented instructions of the Data Controller.

5. Conditions for the Data Controller to give prior, specific or general authorization to subcontracting.

6. Assistance to the Data Controller, whenever possible, in the attention to the exercise of rights of the interested parties.

It is also important to consider whether the provider has any certification related to information security such as ISO 27001 or ISO 20000.

With each Data Controller it is necessary to formalize a contract for the provision of services where the following aspects should be defined:

* If the Data Processor is allowed to subcontract or not.

* If the Data Processor is in charge of resolving and attending to the rights of those affected or has only the obligation to inform the Data Controller.

* If the Data Processor has the obligation to provide the right to information at the time of data collection or corresponds to the Data Controller.

* If the Data Processor is responsible for communicating to the Data Protection Authority or to the interested parties the existence of a security breach that has affected the data.

* Whether the Data Processor has to carry out an impact evaluation or not and what safety measures he has to implement, or whether there is a standard, certification, seal, etc.

* At the end of the contract, define whether the Data Processor should return the data to the Data Controller, to another Data Processor or destroy the data.

In the GlobalSUITE application in the "Document Manager" option → Are the custom clause models for the contract.

2.1.4 Transferencias internacionales de datos

International data transfer is a data processing that involves the transmission of data outside the territory of the European Economic Area, whether it is a transfer or a data communication (to a Data Processor). In the international transfer two figures intervene:

1. The data exporter is the individual or legal entity, public or private, or administrative body located in Spanish territory that makes a transfer of personal data to a third country.

2. The data importer is the natural or legal person, public or private, or administrative body receiving the data, in case of international transfer of the data to a third country, whether Data Controller, Data Processor or third party.

If the treatment has to be modified because there is an international transfer of data, it is necessary to analyze the place of destination and taking into account that only transfers can be made:

- When prior authorization has been given by the Director of the Agency. However, administrative authorization only applies in truly exceptional cases. In this sense, there are a series of assumptions of international transfers, which includes Article 43 of the Draft Organic Law on Data Protection, and which, as an exception to the general rule, must be previously authorized by the AEPD to be made at no have neither the adaptation decision approved by the European Commission, nor be covered by the contractual clauses or binding corporate rules that will be mentioned below:

    - Cuando la transferencia pretenda fundamentarse en la aportación de cláusulas contractuales que no correspondan a las cláusulas tipo previstas en el artículo 46.2 (letras c y d) del RGPD.

    - When the transfer is carried out by any of the Data Controller or Processor or those referred to in article 77.1 of the Preliminary Draft and is based on provisions incorporated into non-normative international agreements with other authorities or public bodies of third states, in particular, memoranda of understanding provided that they include effective and enforceable rights for those affected.

- A specific countries, territories or sectors (the RGPD also includes international organizations) on which the Commission has adopted a decision recognizing that they offer an adequate level of protection, are the following:

    - Switzerland.

    - Canada.

    - Argentina.

    - Guernsey.

    - Isle of Man.

    - Jersey.

- Faroe Islands.
- Andorra.
- Israel.
- Uruguay.
- New Zealand.
- United States. Applicable to entities certified under the EU-US Privacy Shield. In the website of the Privacy Shield you can access the list of certified entities: https://www.privacyshield.gov/list

- When adequate guarantees have been offered about the protection that the data will receive at its destination.
  - That the group of companies has adopted the binding corporate rules.
  - Standard clauses adopted by the Commission
  - Standard clauses adopted by a Control Authority and approved by the Commission.
  - Adoption of a Code of Conduct or certification, together with binding and enforceable commitments of the third party controller or processor in the third country to apply adequate guarantees, including those related to the rights of the interested parties.

- When any of the exceptions that allow the transfer of data without guarantees of adequate protection are applied, for reasons of necessity linked to the self-interest of the owner of the data or to general interests.
  - the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards (it will be made in the information clause).
  - the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request (the interested parties will be informed in the information clause, it is not necessary to obtain the consent, this case would be the transfer of employee data in a multinational, when the employee management policy is carried out globally).
  - the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person (the interested parties will be informed of the transfer made in the information clause, it is not necessary to obtain the consent. This would be the case of a transfer to a Data Processor).
  - the transfer is necessary for important reasons of public interest.

- the transfer is necessary for the establishment, exercise or defence of legal claims, (the interested parties will be informed of the realization of the transfer, but it will be done without the need to obtain their consent).

- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

- the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest.

STANDARD PROFIL in the Register of Treatment Activities will register international transfers and analyze the assumption that allows their realization.

The DPO, after its appointment, will be in charge of ensuring that international transfers are carried out in compliance with the necessary guarantees and will store the information that justifies the legality of the transfer in the Document Manager.

2.2 Treatment evaluation and risk analysis

At least annually, or when changes occur in the organization that affect the treatments, a review of the:

* Evaluation of the treatments where it is determined if it is necessary to make or not a PIA.
* Impact assessments and risk analysis.

The evaluation of treatments and the analysis of risks are in the GlobalSUITE application, and the actions to be carried out are:

* Review of the treatments analyzed and inclusion of those that have been identified as new in the organization.

* The evaluations given to each treatment will be reviewed with the persons in charge, in order to verify if it is still carried out in the same way, or any aspect that requires the performance of a risk analysis has changed.

- The result of the evaluation will be reviewed in case, as a consequence of the modification, it is necessary to make a PIA or review the one that was made at the time.

- Review of risk analysis. Update of the values given to determine the level of risk and the controls implemented.

The company will follow the risk analysis methodology document, which should be modified if it is considered necessary to make any changes in the methodology developed.

The result of the risk analysis will be presented to the Management, who must approve the acceptable level of risk.

2.2.1 Risk treatment plan

Once the risk analysis has been carried out, the actions necessary to mitigate the identified risks will be defined. To do this, within the GlobalSUITE application in the "Analysis" option → "Risk Management". The controls to be implemented for each will be defined and the following aspects will be defined in the risk treatment plan:

1. Name of the action to be implemented
2. Responsible for the implementation
3. Resources needed to carry it out (people, HW, SW, subcontracting, etc.)
4. Deadline for implementation
5. Cost associated with the necessary resources, both external and internal costs will be included.

This treatment plan must be communicated to each of those involved for approval.

The risk treatment plan must be periodically monitored to verify the status of the actions defined to mitigate the risk. Therefore, the actions defined will be reviewed to know the degree of achievement.

To do this, within the GlobalSUITE application in the "Risk Management" option → "Monitoring of the Treatment Plan", the degree of progress of said controls can be reviewed.

2.3 Notification of a personal data breach to the supervisory authority

It defines *«**personal data breach**»: 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.*

The Data Controller must document the security violations that have occurred. To do this, he will use the option of "Incidents and Problems" of GlobalSUITE, where the actions carried out, associated documentation, etc. will be described. In case of having to be communicated, it will be associated to the "Communications" option of GlobalSUITE where it will be recorded.

In the case of a security breach that affects the security of personal data, the Data Controller must notify to the Supervisory Authority within 72 hours, and, without delay, to the interested parties.

In addition, the Data Processor must notify the violation to the Data Controller without delay.

The models found in the GlobalSUITE "Document Manager" will be used.

If security measures have been adopted to ensure data breach, and especially those intended to make the data unintelligible, or when the Data Controller has taken further steps to ensure that there is no longer a likelihood of high risk taking place for the rights and freedoms of the interested party, or when it involves a disproportionate effort, the interested parties will not be notified. This decision must be justified in GlobalSUITE in the option of "Incidents".

2.4 Roles and responsibilities

The roles and responsibilities are defined in GlobalSUITE. In the option of "Roles and Responsibilities" of the start menu. The defined roles are:

- Senior Management
- Data Protection Officer
- Data Processor
- Risk Manager
- Owner of treatment
- Security Manager
- Data Controller

When there is a change in the organization, for example, the withdrawal of employees involved in the management of the system or modification of the assigned positions, it is necessary to update the application.

We will follow the following steps to modify a person:

* In the "Management" menu, we will select the employee option and proceed to register or dismiss the employees we need.

* Next, from the start menu, in the option of "Roles and Responsibilities", in the first tab we will assign/eliminate to each role the people appointed to perform these functions.

It is important to point out that when there is a modification in the appointment of the DPO, it will be the Management who must appoint the new manager formally and it must be communicated

to the rest of the company, and at the same time notified to the Control Authority (AEPD) when the company has a legal obligation to communicate.[1]

If it is necessary to modify the roles, it will be done from the start menu → "Roles and Responsibilities" → Button configure roles. It refers us to an administration configuration option.

In the "Roles and Responsibilities" option, we will have to check if the person named for a certain role complies with the competencies that are required. Otherwise, the Management must opt for one of the following options:

- Appoint a person who fulfills these competences.
- Review the competences, and consider if those competences that are not fulfilled are essential for the development of the position or not, and therefore modifiable or substitutable by other equivalent ones.
- Invest the necessary resources so that the person named can meet the requirements described (training, skills, etc.).

For each of the roles, the functions assigned to it in the management system will be defined. These functions, will vary in case of a modification of the applicable regulations, organizational modification (Eg. Assigning functions to other departments or areas), etc.

2.5 Rights

When requests for rights attention are received from those affected, they will be registered in the GlobalSUITE application in the "Management" option → "Rights". For each one of them a ticket will be opened and it will be completed with all the necessary data and documents.

For each of the rights we have to take into account the following:

[1] A DPO will be appointed when the company is obliged to make such appointment.

Derecho	Definición	Plazos	Contenido - especificaciones
Access	to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data.	One month since the request was received.	The communication addressed to the interested party will contain the following information: a) the purposes of and legal basis for the processing; b) the categories of personal data concerned; c) the recipients or categories of recipients to whom the personal data have been disclosed, in particular recipients in third countries or international organisations; d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; e) 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; f) the right to lodge a complaint with the supervisory authority and the contact details of the supervisory authority; g) communication of the personal data undergoing processing and of any available information as to their origi; h) the existence of automated decisions, including profiling, and the importance and the expected consequences of such treatment for the interested party.
Rectification	To obtain from the controller without undue delay the rectification of inaccurate personal data relating to him or her. Taking into account the purposes of the processing, Member States shall provide for the data subject to have the right to have incomplete personal data completed, including by means of providing a		Communication performing rectification.

Derecho	Definición	Plazos	Contenido - especificaciones
	supplementary statement.		
Erase – Right to be forgotten	To erase personal data without undue delay.		They will be erased by the Data Controller without delay, when the following circumstances existis: a) The data has expired. b) The consent has been withdrawn. c) The interested party has opposed the treatment. d) The data have been treated illicitly. e) There is a legal provision that obliges them to be deleted. Communication performing suppression.
Limitation	To obtain treatment limitation from the Data Controller.		The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies: a) The accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data; b) The processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; c) The controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; d) The data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject Communication performance of the limitation.

Derecho	Definición	Plazos	Contenido - especificaciones
Portability	The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.		This right may be realized when: * The processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and * The processing is carried out by automated means. Communication of the realization of data portability, in some cases directly to the new Data Controller.
Object	The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions.		The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.
Automated individual decision-making, including profiling	The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.		This right shall not apply if the decision: a) is necessary for entering into, or performance of, a contract between the data subject and a data controller; b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or c) is based on the data subject's explicit consent.

2.6 Review of the data protection model

2.6.1 Audit

At least once a year, an audit will be conducted, either by internal or external personnel, to verify that the system complies with the requirements of the GDPR.

The auditor must register in the tool, in the option “Plans” → “Audits” → “Planning”, the data that are requested in the audit.

Once the audit is done, the results of the audit will be documented in the tool in “Plans” → “Audits” → The audit report will be attached to the Document Manager. Non-conformities (NC) detected must be opened, so that they can be resolved by those responsible.

The auditor will present the result of the audit to the DPO to review the points detected in it. Once the audit report has been finalized, it will be submitted to the Management, who must approve the corrective actions to be applied.

2.6.2 Management of Non-Conformities

The NC management is carried out in the application from the Management → “Non-Conformities” option. It will record the actions to be implemented to be able to solve them and the monitoring that is carried out of them.

2.6.3 Review of the correct functioning of controls

Those responsible for compliance with the RGPD must perform internal reviews ex officio to ensure compliance with the requirements and maintenance of security controls implemented in the organization.

Written reviews of the revisions must be recorded, along with their results. The deviations found can be treated as Non-Conformities.

2.6.4 Measurement

In order to evaluate the effectiveness of the implemented security measures, indicators based on metrics can be defined.

The data must be completed in each one of the metrics and the results obtained should be reviewed, in the periodicity established for each one of them. In this way, it will be analyzed if there are deviations that can indicate a breach that should be treated.

You can define two types of metrics:

1. Metrics for the management system: training, audit, NC, etc.
2. Metrics for the controls to verify if they are efficient and that there are no deviations.

2.7 Training and awareness

It is necessary to carry out an analysis of the need for training and awareness and plan it annually. The Department of Human Resources and the DPO will participate in this planning. It will be recorded in the GlobalSUITE application in the option “Plans” → “Training”.

In order to check the effectiveness of the training, the participants in the courses will complete an evaluation test, which will be reviewed by the person responsible for the training. If this test is not passed, it will be necessary to repeat the training for said person, to ensure that he / she knows and understands the obligations regarding the processing of personal data.

3 Version control

ELABORATION	REVIEW	APPROVAL
Date:	Date:	Date:
Date:	Date:	Date:

aud[i]sec

seguridad de
la información