Towards the integration of the GDPR in the Unified Software Development Process: Proof of Concept

Elena Gómez-Martínez, Miguel Marroyo, Silvia T. Acuña
Departamento de Ingeniería Informática
Universidad Autónoma de Madrid
Madrid, Spain
{MariaElena.Gomez, Miguel.Marroyo, Silvia.Acunna}@uam.es

Abstract—**The General Data Protection Regulation (GDPR) is the core of digital privacy legislation across Europe (EU), and it applies to processing carried out by organisations operating within and outside the EU that offer goods or services to individuals in the EU, including software products. Nevertheless, software teams are generally unaware of the legal requirements for personal data protection and its application throughout the software life cycle. In this paper, we propose a comprehensive guidance to integrate compliance with GDPR requirements within the Unified Software Development Process (UP) across the entire lifetime.**

Keywords-data protection regulation; unified software development process; personal data; privacy requirements.

I. PROOF OF CONCEPT

Next, we aim at applying the proposed approach to the development of a real software product to check for compliance with the Spanish LOPDGDD, and consequently with the European GPDR. To validate that the application com- plies with the guidelines of the law, Regulatory Compliance List of the AEPD will be used [1].

We have considered a social network like Face- book, since it manages a huge amount of personal data. We have divided its development into the phases proposed in the UP.

A. Requirements and Analysis

The project will begin by delimiting the scope of personal data. Being a social network, it will have the Person class. The purpose of collecting these data will be to identify the user, in that way that other users can connect with her. In addition to the Person class, it will be necessary to consider the role of the person responsible for the data pro- cessing, whose identity will be stored, and a record of these activities, thus the Registry class will exist. The data con- troller will have the permission to block data. Finally, there will be the Administrator class, which will be responsible for managing the system and its users.

Since it is a social network in which users can express their opinions, the aspect of data processing on personality is covered, so it will be necessary to request acceptance from the user on this point. Users will be able to edit the content they have created, and if they decide to delete their profile, they will no longer appear in the search results within the application. Any content they create can be ex- ported outside of the application.

The business model will be based on the advertising within the application and the sale of the data to third par- ties, so that an information system can be created to store the information of those users who request not to receive this advertising. In addition, as it is a service on the Inter- net, it must be neutral, that is, any user will have the same service without distinguishing her condition. Sales of data to third parties will also occur, so data transfer processes between systems should be considered.

To guarantee digital security, the following is established: involvement of the data processing controller, high level of confidentiality for individuals' personal data, since information is stored that allows an individual to be identified, and registration of activities. The social network will only be accessible to people over eighteen years of age, so it will not be necessary to contemplate the aspects of the data processing of people under this age.

B. Design

Within the Person class, we will define as fields Full Name, Age and Sex. These data do not fall into any of the categories marked as special so explicit consent will not be necessary. The Registry class will have the fields mentioned in Section 3.3 and will be related to the person responsible for data processing Person. Each Person will have an N-to-N relationship between them. Each object will have a label that will indicate if the data is blocked or not. If so, no user will be shown in the application. In addition, the source of people's data will be store in the Registry, which in this case will be the user's own when they gave their consent when registering in the application.

C. Implementation and Testing

When registering, the user will be informed via a pop-up window that the application will store their personal data and the appearance of advertisements within the application. The user must click on a 'Confirm" button to be able to register in the application. As it is only available to per- sons over eighteen years of age, their age will be required as an essential requirement to register. Within the application, a section will appear where all the rights, summarized in Section 2.1, will be displayed. In addition, an area will be included with the legal notice, the established privacy policy, the identity of the person responsible for the data processing and a button where, when pressed will take the user to a request system to request access to the personal data that has been stored in the application.

D. Maintenance

Any user may request the withdrawal of personal data of a deceased person, for which the option of doing this with- out the need to register will be given. In addition, checks will be made of the accuracy and timeliness of the data. If any inaccurate or updated data is identified, the user will be informed with a message to complete or update it.

E. Results

Once the example is created, a compliance test is carried out following the requirements established in the Regulatory Compliance List by the AEPD [1]. The procedure carried out was as follows: for each requirement of the list, it is analysed whether in the adaptation of the regulations, either by the direct application of any of the articles or by derived requirements, it has been considered and if a development team who uses this adaptation can apply it directly. For example, for the requirement "Personal data are collected for specific purposes", in section 1 of Art. 4 it is indicated that '. . . it is essential that the scope of use and the purpose of said data be defined. . .", thereby, the adaptation has been considered.

From 267 requirements, the 78% are fulfilled, 30% are not applicable and the rest, not satisfied the regulation. If we only consider the percentage of requirements applicable to the technological framework, that is, one hundred and eighty-eight eliminating those that are not applicable, we would be obtaining approximately 68% of compliance. Despite being a high percentage, it is evident that approximately 30% of the GDPR requirements that involve a technical aspect or related to the UP would not be met only with the a priori measures that have been established.

F. GDPR compliance form

Below is the form with the list for GDPR compliance created by the Spanish Data Protection Agency. This form has been used for validating the proof of concept proposed, and indicates whether each characteristic in is fulfilled, is not fulfilled or is not relevant.

PRINCIPLES RELATING TO TREATMENT	Adaptation (Yes/No/NA)
Personal data is collected for explicit purposes	Yes
Personal data is collected for legitimate purposes	Yes
They are further treated in a manner incompatible with other purposes	No
Personal data remains accurate	Yes
They stay up to date	Yes
Inaccurate personal data are rectified with respect to the purpose	Yes
Inaccurate personal data regarding the purpose of the purpose is deleted	Yes
They are maintained for longer than necessary with respect to the purpose	Yes
They are treated for file purposes in the public interest	No
They are treated for scientific research purposes	No
They are treated for historical purposes	No
Personal data is processed for statistical purposes	No
Security measures have been put in place to protect the integrity and confidentiality of data	Yes
Security measures have been put in place against the unauthorized or unlawful processing of data	Yes
Security measures have been put in place to prevent accidental loss, destruction or damage	Yes
Traceability of treatment purposes is maintained	Yes

TREATMENT LAWFULNESS	Adaptation (Yes/No/NA)
Consent is given for each purpose of the processing	Yes
Processing is necessary to execute a contract or pre-contract	Not applicable
There is a legal obligation	Yes
Treatment is needed to protect vital interests	Not applicable
Treatment is necessary for public interest compliance	Not applicable
Treatment is necessary to satisfy legitimate interests	Not applicable

CONDITIONS FOR CONSENT	Adaptation (Yes/No/NA)
It can be shown that the affected person consented to the treatment	Yes
It can be shown that the processing is carried out as a result of compliance with a legal obligation	Yes
Consent is sought clearly and independently of the other matters	Yes
Consent is requested in an intelligible and easily accessible manner	Yes
Requested using clear and simple language	Yes
It is informed prior to obtaining consent	Yes
It can withdraw consent as easily as it is collected	Yes
Means are offered to withdraw consent at any time	Yes
Free consent is sought	Yes
To provide a service, only the necessary data is requested	Yes
Only the necessary data is requested to execute a contract	Not applicable

CHILDREN'S CONSENT IN RELATION TO INFORMATION SOCIETY SERVICES	Adaptation (Yes/No/NA)
The consent of children under the age of 14 is sought from the holder of the parental authority or guardianship over the child	Yes
It is verified that the consent was given by the holder of the parental authority or guardianship over the child	Yes

TREATMENT OF SPECIAL DATA CATEGORIES	Adaptation (Yes/No/NA)
Data is processed only when there are rules that exempt it	Yes
Data is processed with explicit consent and there are no rules of law that expressly prohibit its processing	Yes

TREATMENT OF SPECIAL DATA CATEGORIES	Adaptation (Yes/No/NA)
It is necessary for the fulfilment of obligations and the exercise of specific rights in the field of labour law and security and protection to the extent that it is established by the rules of law	Not applicable
It is necessary to protect a person's vital interests and the data subject is not qualified, physically or legally, to give consent	Not applicable
It is carried out in the field of legitimate activities and with due guarantees and refers exclusively to current or former members or persons who have regular contacts in relation to the purpose (political, philosophical, religious or trade union)	Yes
It is carried out in the field of legitimate activities and with due guarantees and are not communicated to third parties without the consent of the interested parties	Yes
It deals with data that the data subject has made manifestly public	Yes
It is necessary for the formulation, exercise or defence of claims	No
It is necessary for preventive or work medicine purposes, evaluation of the worker's work capacity, medical diagnosis, provision of health or social assistance or treatment, or management of health and social care systems and services	No
It is necessary for reasons of public interest in the field of public health based on rules of law establishing appropriate and specific measures to protect the rights and freedoms of the person concerned, professional secrecy	No
It is necessary for purposes of public interest, scientific or historical research purposes or statistical purposes based on rules of law	No
It is carried out in compliance with the conditions regarding the processing of genetic data, biometric data or health data established by national regulations	No

TREATMENTS RELATING TO CRIMINAL CONVICTIONS AND INFRINGEMENTS	Adaptation (Yes/No/NA)
Data is processed under the supervision of public authorities	No

TREATMENTS RELATING TO CRIMINAL CONVICTIONS AND INFRINGEMENTS	Adaptation (Yes/No/NA)
Data is processed under the authorization of rules of law	No
Full criminal convictions are recorded under the control of public authorities	No

TREATMENTS THAT DO NOT REQUIRE IDENTIFICATION	Adaptation (Yes/No/NA)
Additional information is maintained with a view to identifying the data subject when the purposes do not require such identification	No
Additional information is obtained and/or treated with a view to identifying the data subject when the purposes do not require such identification	No
It can be shown that anonymised data do not identify stakeholders	No
The data subject is informed, and consent is obtained when his/her identification is reached	No
Data is cancelled when the data subject is identified	No

RIGHTS OF THE INTERESTED PARTY. TRANSPARENCY OF INFORMATION	Adaptation (Yes/No/NA)
Measures are taken to provide the data subject with all the information related to the treatment	Yes
The information is provided in a concise, transparent and intelligible way	Yes
Information is provided in clear and simple language	Yes
It is provided in writing or by other means, including electronic	Yes
It is provided verbally, upon accreditation of your identity	Not applicable
It makes it easier for the data subject to exercise their rights	Yes
Requests for the exercise of rights are addressed even if the processing does not require identification unless the data subject cannot be identified	Yes
The data subject is informed within one month of receipt of his or her solitude	Yes
It is informed before the exercise of complex rights or to many applications within a maximum period of three months from receipt of the application	No
It is reported within one month of the three-month extension indicating the reason for the resignation	No

RIGHTS OF THE INTERESTED PARTY. TRANSPARENCY OF INFORMATION	Adaptation (Yes/No/NA)
Interested parties can exercise rights by electronic means	**Yes**
It is reported by electronic means when the request is received by such means unless it requests that it be made by another means	Yes
The reasons for non-action and the possibility of filing a complaint with a supervisory authority and bringing legal proceedings are reported within one month of receipt of the application when the application is not made	No
The exercise of rights is provided free of charge	Yes
Information is requested to prove the identity of the natural person exercising their rights	Yes
When the information provided uses standard icons, the electronic format is mechanically readable	Yes

RIGHTS OF THE INTERESTED PARTY. INFORMATION TO PROVIDED WHEN DATA IS OBTAINED FROM THE DATA SUBJECT	Adaptation (Yes/No/NA)
The identity and contact details of the controller and, where appropriate, the representative is provided when requesting data	Yes
Contact details of the data protection officer are provided	Yes
The purposes of the processing for which the personal data and the legal basis of the processing are used are provided	Yes
Information on legitimate interest is provided	Yes
Recipients or recipient categories are reported	Yes
The period of retention of personal data or the criteria used to determine it is reported	No
The existence of the right to request access, rectification or deletion, the limitation of processing, to object and the right to portability are reported	Yes
If the processing is based on consent it is informed of the existence of the right to withdraw it at any time	Yes
The right to lodge a complaint with a supervisory authority is reported	No
Assignments based on legal or contractual requirements are reported	No
Assignments are reported based on a requirement to enter a contract	No

RIGHTS OF THE INTERESTED PARTY. INFORMATION TO PROVIDED WHEN DATA IS OBTAINED FROM THE DATA SUBJECT	Adaptation (Yes/No/NA)
It reports the existence of automated decisions, profiling, on the logic applied, the importance and expected consequences of the treatment	No
Before processing personal data for a purpose other than that collected, the data subject is informed, and the information covers that other purpose and any other relevant information	No

RIGHTS OF THE INTERESTED PARTY. INFORMATION TO PROVIDED WHEN THE DATA IS NOT OBTAINED FROM THE DATA SUBJECT	Adaptation (Yes/No/NA)
The identity and contact details of the controller and, where appropriate, his representative is informed	Yes
DPD contact details are reported	Yes
The purposes of treatment are reported	Yes
The legal basis for the processing is reported	Not applicable
The categories of personal data in question are reported	Yes
Recipients or categories of recipients of the data are reported	Yes
The period during which personal data will be kept is reported	Yes
The criteria used to determine this period of retention period are reported when it is not possible to report it	No
The specific legitimate interests on which the processing is based are reported	Yes
The right to request access to your own personal data is reported	Yes
The right to request rectification of your data is reported	Yes
The right to request suppression is reported	Yes
The right to restriction of treatment is reported	Yes
The right to object to treatment is reported	Yes
The right to data portability is reported	Yes
The existence of the right to withdraw consent is reported at any time	Yes

RIGHTS OF THE INTERESTED PARTY. INFORMATION TO PROVIDED WHEN THE DATA IS NOT OBTAINED FROM THE DATA SUBJECT	Adaptation (Yes/No/NA)
The right to lodge a complaint with a supervisory authority is reported	No
The source from which the personal data comes is reported	Yes
If they come from publicly accessible sources, this is reported	Yes
Information is provided within a month	Yes
If personal data is used for communication with the data subject, you are communicated the information to which you are entitled at the time of the first communication	Yes
If it is planned to communicate the personal data of the data subject to another recipient, the information is communicated to you no later than the time the personal data is communicated for the first time	Yes
The data subject is informed if treatments are carried out for purposes other than that which they were collected	Yes
It is not reported when the data subject already has the information	Yes
It is not reported when the communication of such information is impossible or involves a disproportionate effort	Not applicable
It is not reported because it may make it impossible or seriously impede the achievement of the objectives of the processing, but measures are taken to protect the legitimate rights, freedoms and interests of the data subject	Not applicable
It is not reported because the obtaining or communication is expressly established by applicable rules of law	Not applicable
It is not reported because personal data are confidential based on an obligation of professional secrecy governed by rules of law	Not applicable

RIGHTS OF THE INTERESTED PARTY. RIGHT OF ACCESS	Adaptation (Yes/No/NA)
Information is reported on the purposes of treatment	Yes
The categories of personal data being processed are reported	Yes
The recipients or categories of recipients to which the personal data were communicated or will be communicated are reported	Yes

RIGHTS OF THE INTERESTED PARTY. RIGHT OF ACCESS	Adaptation (Yes/No/NA)
The expected period of storage of personal data is reported	Yes
The criteria used to determine the retention period are reported	No
The right to request rectification or deletion of your data is reported	Yes
The right to request the limitation of data processing is reported	Yes
The right to seek opposition to treatment is reported	Yes
The right to lodge a complaint with a supervisory authority is reported	No
Information about the source of the data is provided when they do not collect from the data subject himself	Yes
A copy of the personal data being processed is provided when requested by the data subject	Yes
Information is provided in commonly used electronic format if requested by electronic means unless other means are provided	Yes

RIGHTS OF THE INTERESTED PARTY. RIGHT OF RECTIFICATION	Adaptation (Yes/No/NA)
Inaccurate personal data is rectified without undue delay	Yes
Incomplete personal data is completed considering the purposes of the processing	Yes

RIGHTS OF THE INTERESTED PARTY. RIGHT	Adaptation (Yes/No/NA)
Data is deleted when it is not necessary in relation to the purposes for which it was collected	Yes
Data is deleted when consent is withdrawn on which the processing is based	Yes
Data is deleted when you object to the processing	Yes
Data is deleted when it has been unlawfully processed	Yes
Data is deleted when required by a legal obligation	Yes
Data is deleted when obtained in connection with the information society's service offering	Yes
Processing is limited for a period to verify the accuracy of the data, when the data subject challenges its accuracy	No

Processing is limited when it is unlawful, and the data subject objects to the deletion of his/her personal data and instead requests the limitation of its use	Yes
Treatment is limited when they are not necessary for the purposes, but the data subject needs them for the formulation, exercise or defence of claims	No
Processing is limited when the data subject objects to the processing while checking whether the legitimate reasons of the controller prevail over those of the data subject	No
The data subject is informed when the limitation of treatment is lifted	No

RIGHTS OF THE INTERESTED PARTY. RIGHT TO LIMITATION OF TREATMENT	**Adaptation (Yes/No/NA)**
Processing is limited for a period to verify the accuracy of the data, when the data subject challenges its accuracy	No
Processing is limited when it is unlawful, and the data subject objects to the deletion of his/her personal data and instead requests the limitation of its use	Yes
Treatment is limited when they are not necessary for the purposes, but the data subject needs them for the formulation, exercise or defence of claims	No
Processing is limited when the data subject objects to the processing while checking whether the legitimate reasons of the controller prevail over those of the data subject	No
The data subject is informed when the limitation of treatment is lifted	No

INFORMATION TO THE DATA SUBJECT BEFORE RECTIFICATION, DELETION OR LIMITATION IN TREATMENT	**Adaptation (Yes/No/NA)**
The data subject is no longer rectified, suppressed or limited in treatment	Yes

RIGHTS OF THE INTERESTED PARTY. RIGHT TO DATA PORTABILITY	**Adaptation (Yes/No/NA)**
Data is provided when requested by the data subject in a structured, commonly used and mechanically readable format	Yes
Such data is transmitted to another controller if the processing is based on consent or a contract	Not applicable
Such data is transmitted if the processing is carried out by automated means	No
The data is transmitted to the new controller that the data subject determines, if technically possible	No

RIGHTS OF THE INTERESTED PARTY. RIGHT TO DATA OPPOSITION	**Adaptation (Yes/No/NA)**
Opposition requests are addressed, and data no longer processed	Yes
Requests for opposition are addressed, but data are not no longer processed for legitimate reasons that prevail over interests, rights and freedoms or for the formulation, exercise or defence of claims	Not applicable
The necessary means are put in place so that you can exercise your right to object by automated means	Yes

RIGHTS OF THE INTERESTED PARTY. AUTOMATED INDIVIDUAL DECISIONS, INCLUDING PROFILING	**Adaptation (Yes/No/NA)**
No treatments are carried out that involve a decision based solely on automated processing and that produces legal effects	No
Treatments are carried out that involve deciding based solely on automated processing and that produce legal effects because it is necessary for the conclusion or execution of a contract	No
Treatments are carried out that involve deciding based solely on automated processing and that produce legal effects because they are authorized in law	No
Treatments are carried out that involve deciding based solely on automated processing and that produce legal effects because explicit consent is available	No

RIGHTS OF THE INTERESTED PARTY. AUTOMATED INDIVIDUAL DECISIONS, INCLUDING PROFILING	Adaptation (Yes/No/NA)
If treatments are carried out that involve the decision based solely on automated processing and that produce legal effects, appropriate measures are taken to safeguard legitimate rights and freedoms and interests	No
If treatments are carried out that involve a decision based solely on automated processing and that produce legal effects, appropriate measures are taken to safeguard the right to obtain human intervention by the controller	No
If treatments are carried out that involve the decision based solely on automated processing and that produce legal effects, appropriate measures are taken to give the interested party the opportunity to express his or her point of view and challenge the decision	No
Automated individual decisions, including profiling, are made based on special categories of personal data because the data subject's consent is available	No
Automated individual decisions, including profiling, are made based on special categories of personal data because legal qualification is available	No
Stakeholders are informed about these automated individual decisions and their legal enabling	No
Automated individual decisions, including profiling, are made based on special categories of personal data because appropriate measures have been taken to safeguard the rights and legitimate interests of the data subject	No

RESPONSIBILITY OF THE CONTROLLER	Adaptation (Yes/No/NA)
The nature, scope, context and purposes of the processing are considering in order to ensure and demonstrate that the processing is GDPR compliant	Yes
Risks of various probability and severity to the rights and freedoms of natural persons are considering	Yes

RESPONSIBILITY OF THE CONTROLLER	Adaptation (Yes/No/NA)
Appropriate technical and organizational measures are applied	Yes
Measures are reviewed and updated when necessary	Yes
Data protection policies have been developed	Yes
Data protection policies apply	Yes

DATA PROTECTION FROM DESIGN AND BY DEFAULT	Adaptation (Yes/No/NA)
Appropriate technical and organisational measures are analysed before determining the means of treatment	Yes
Appropriate technical and organisational measures to comply with the GDPR are considered during the design of the processing	Yes
During treatment, measures that have been determined are applied	Yes
During treatment, the effectiveness of the measures applied is checked	Yes
Appropriate technical and organisational measures are applied to ensure that, by default, only data necessary for each of the purposes is processed	Yes
Technical and organisational measures are applied considering the amount of personal data collected, the extent of the processing, the retention period and accessibility	Yes
The measures ensure that, by default, data are not accessible to an undetermined number of natural persons, without the intervention of staff	Yes

TREATMENT CO-RESPONSIBILITIES	Adaptation (Yes/No/NA)
The respective responsibilities of co-responsible in fulfilling the obligations imposed by the GDPR have been determined in a transparent manner, and by mutual agreement.	No
The agreement sets out the respective obligations to provide information to the data subject	No

TREATMENT CO-RESPONSIBILITIES	Adaptation (Yes/No/NA)
The agreement between controllers reflects the respective roles and relationships of both in relation to the data subjects	No
The essential aspects of the agreement are available to the data subject	No

TREATMENT MANAGER	Adaptation (Yes/No/NA)
Those who provide sufficient guarantees in accordance with the requirements of the GDPR and ensuring the protection of the rights of the data subject are chosen	Not applicable
The processor does not use another processor without prior written permission	Not applicable
The processing by the processor is governed by a contract or other binding legal act in accordance with the rules of law	Not applicable
The contract establishes the object, duration, nature and purpose of the processing, the type of personal data and categories of data subjects as well as the obligations and rights of the controller	Not applicable
The contract states that personal data is processed only following documented instructions from the controller	Not applicable
The contract ensures that persons authorized to process personal data have undertaken to respect confidentiality or are subject to a statutory confidentiality obligation	Not applicable
The contract states that the necessary security measures will be taken	Not applicable
The contract states that the conditions indicated for recourse to another processor will be respected	Not applicable
The contract provides that the processor shall assist in responding to requests for the exercise of the rights of the interested parties	Not applicable
The contract states that personal data will be deleted or returned after the provision of the services is completed, and will delete existing copies unless the retention of personal data is required	Not applicable

TREATMENT MANAGER	Adaptation (Yes/No/NA)
The contract provides that it will make available all the information necessary to demonstrate compliance with the obligations established, as well as to allow and contribute to the conduct of audits and inspections, by the controller or another auditor authorized by the controller	Not applicable
The contract provides that if the processor relies on another processor to carry out certain processing activities on processing on processing without the controller, the same data protection obligations as those stipulated in the contract, by contract or other legal act established under the law	Not applicable
The contract consists in writing	Not applicable
Data is only accessed by following instructions from the controller	Not applicable

RECORDING TREATMENT ACTIVITIES	Adaptation (Yes/No/NA)
A record of treatment activities is keeps track	Yes
The registration includes the name and contact details of the controller and, where appropriate, the co-responsible, the representative of the controller, and the data protection officer	Yes
Registration includes the purposes of treatment	Yes
It contains a description of the categories of data subjects and the categories of personal data	Yes
Collects the categories of recipients to whom personal data was communicated or communicated, including recipients in third countries or international organizations	Yes
Collect transfers of personal data to a third country or international organization, including the identification of that third country or international organization	Yes
Includes the deadlines for the deletion of data categories	No

RECORDING TREATMENT ACTIVITIES	Adaptation (Yes/No/NA)
It includes an overview of the technical and organisational measures appropriate to the risk of treatments	Yes

TREATMENT SAFETY	Adaptation (Yes/No/NA)
To determine the measures to be applied, account is taken of prior art, implementation costs, and the nature, scope, context and purposes of the processing, as well as variable likelihood and seriousness risks to the rights and freedoms of natural persons	Yes
Appropriate technical and organisational measures are applied to ensure a level of security appropriate to the risk	Yes
Measures have been included to ensure the permanent confidentiality, integrity, availability and resilience of treatment systems and services	Yes
Measures to ensure the ability to restore availability and access to personal data quickly in the event of a physical or technical incident	Yes
There is a process of regular verification, evaluation and evaluation of the effectiveness of technical and organisational measures to ensure the security of treatment	Yes
The risks presented by the processing as a result of its accidental or unlawful destruction, loss or alteration that are transmitted, preserved or processed, or unauthorized communication or access to such data have been considered to assess the level of security applied	Yes
Steps have been taken to ensure that persons authorized to access data only process it by following instructions	Yes

NOTIFICATION OF PERSONAL DATA SECURITY BREACHES TO THE SUPERVISORY AUTHORITY	Adaptation (Yes/No/NA)
A procedure has been established to identify and manage security breaches	Yes
There is a procedure for processors to notify the controller of gaps at the time they become aware of them	No
There is a procedure for notifying the supervisory authority within 72 hours	No
There is a procedure for documenting the reasons why it cannot be reported within 72 hours	No
There is a procedure for providing information gradually when it is not possible to provide it simultaneously	No
Any personal data security breach is documented	Yes
The documentation includes the facts relating to it, its effects and the corrective measures taken	Yes
The notification procedure has been found to work	No

COMMUNICATION OF A GAP TO THE INTERESTED PARTY	Adaptation (Yes/No/NA)
There is a procedure for communicating the gap without undue delay when it is likely to pose a high risk to rights and freedoms	No
Communication to the data subject, carried out in clear and simple language, describes the nature of the gap	No

IMPACT ASSESSMENT RELATING TO DATA PROTECTION	Adaptation (Yes/No/NA)
DPD advice is sought	Not applicable
EIPD is performed before treatment when it is likely to pose a high risk to people's rights and freedoms	Not applicable
An EIPD is performed earlier in large-scale treatment of special categories of data or relating to convictions and criminal offences	Not applicable

IMPACT ASSESSMENT RELATING TO DATA PROTECTION	Adaptation (Yes/No/NA)
EIPD is performed before treatment that involves a large-scale systematic observation of a publicly accessible area	Not applicable
EIPD is performed in processing operations included in the list published by the supervisory authority	Not applicable
The EIPD includes a systematic description of the planned processing operations and the purposes of the processing, and where appropriate the legitimate interest pursued	Not applicable
It includes an assessment of the necessity and proportionality of processing operations with respect to their purpose	Not applicable
The EIPD includes a risk assessment for rights and freedoms	Not applicable
It includes measures envisaged to demonstrate compliance with the GDPR, considering the legitimate rights and interests of the interested parties and other persons concerned	Not applicable
Includes measures envisaged to address risks, guarantees and mechanisms to ensure data protection	Not applicable
EIDPs are re-examined whenever necessary and where there is a change in the risks associated with treatment operations	Not applicable
The supervisory authority is consulted before treatment when an EIPD shows that it would pose a high risk if no measures were taken to mitigate it	Not applicable
The respective responsibilities of those involved in the processing are reported in the consultation with the supervisory authority	Not applicable
The purposes and means of the treatment provided for in the consultation are reported	Not applicable
Measures and safeguards are reported to protect the rights and freedoms in the consultation	Not applicable
Contact details of the data protection officer are provided	Not applicable
Impact assessment is included	Not applicable
When consultation, any additional information requested by the supervisory authority is provided	Not applicable

DATA PROTECTION OFFICER	Adaptation (Yes/No/NA)
A Data controller officer has been designated by legal requirement	Not applicable
A Data controller officer has been designated considering its professionalism qualities, knowledge and competences in the field	Not applicable
Data controller officer contact details have been published and the supervisory authority has been informed	Not applicable
The Data controller officer is guaranteed to participate appropriately and in a timely manner in all matters relating to the protection of personal data	Not applicable
Its functions are supported in performance	Not applicable
You are provided with the necessary resources for the performance of your duties, access to personal data and processing operations	Not applicable
You are provided with the resources to maintain your knowledge	Not applicable
It is guaranteed that the Data controller officer does not receive any instruction regarding the performance of its functions	Not applicable
The DPD cannot be dismissed or punished for carrying out its functions	Not applicable
Data controller officer accounts directly at the highest hierarchical level	Not applicable
Data controller officer addresses stakeholder requests	Not applicable
The Data controller officer is obliged to maintain confidentiality in the performance of its functions	Not applicable
If the Data controller officer performs other functions, it is guaranteed that they do not give rise to conflict of interest	Not applicable

DATA PROTECTION OFFICER	Adaptation (Yes/No/NA)
The functions of the Data controller officer are to inform, advise and train staff of their obligations	Not applicable
The Data controller officer cooperates and acts as a point of contact with the supervisory authority	Not applicable

TRANSFERS TO THIRD COUNTRIES OR INTERNATIONAL ORGANIZATIONS	Adaptation (Yes/No/NA)
Transfers are made to countries, or sectors thereof, or international organizations declared to be of adequate level of protection by the European Commission	Yes
The validity of the European Commission's adequacy decisions is monitored	Not applicable
Transfers are made through appropriate guarantees that offer interested parties enforceable rights and the possibility of legal action.	Yes
There is a binding and enforceable legal instrument among public authorities or bodies	Not applicable
There are binding corporate rules	Not applicable
There are model data protection clauses adopted by the Commission	Not applicable
There are model data protection clauses adopted by a supervisory authority and approved by the Commission	Not applicable
There is a code of conduct together with binding and enforceable commitments in the third country that allows adequate guarantees to be applied	Not applicable
There is a certification mechanism together with binding and enforceable commitments in the third country to enable adequate guarantees to be applied	Yes
There are contractual clauses that require prior authorization from the supervisory authority	Not applicable
There are administrative agreements between public authorities and bodies incorporating provisions that include effective and enforceable rights for stakeholders	Not applicable

TRANSFERS TO THIRD COUNTRIES OR INTERNATIONAL ORGANIZATIONS	Adaptation (Yes/No/NA)
International transfers are made in the absence of a European Commission adequacy decision and adequate guarantees	Not applicable
The explicit consent of the data subject is available, and you have been informed of the possible risks	Yes
They are necessary for the performance of a contract with the data subject or for the enforcement of pre-contractual measures taken at the request of the data subject	Not applicable
They are necessary for the formulation, exercise or defence of claims	Not applicable
They are necessary for the protection of the vital interests of the data subject or others, when the data subject is unable to give consent	Not applicable
For imperious legitimate interests	Not applicable
It affects a limited number of stakeholders and is not repetitive	Not applicable
All concurrent circumstances have been assessed and appropriate safeguards have been offered	Not applicable
The supervisory authority has been informed	Not applicable

REFERENCES

[1] Agencia Española de Protección de Datos (AEDP). Regulatory Compliance List (In Spanish, Lista de cumplimiento normativo), November 2019. [Online]. https://www.aepd.es/sites/default/files/2019-11/guia-listado-de-cumplimiento-del-rgpd.pdf