Lantik / BFA DFB Bizkaiko Foru Aldundia / Diputación Foral de Bizkaia	NCS-1/6

Security standard: LOPD clauses with access to data of which Lantik is the data controller

Prepared and updated by: Security Department	**Review: 00**
	Effective date: **17/07/2013**

1. PURPOSE	2. SCOPE
Compliance of Article 12 of the Spanish Protection of Personal Data Act 15/1999, of 13 December, and Article 21 of Royal Decree 1720/2007 (LOPD).	All projects and services rendered by third parties that have access to personal data of which Lantik is the Data Controller. In other words, when a third party contracted by Lantik is going to access data not belonging to Lantik but which it manages however in its systems (for example, Bizkaia Provincial Council data).

3. DEVELOPMENT

I. LANTIK S.A.is entrusted with processing the personal data belonging to multiple entities (File Manager) pursuant to the Spanish Personal Data Protection Act 15/1999, of 13 December, (hereinafter the LOPD).

II. Each of the entities with whom LANTIK S.A. collaborates has duly declared those files with the General Registry of the Data Protection Agencies.

Everything stipulated below is limited to the personal data contents that the successful bidder may be required to process in order to provide the contracted service.

III. The successful bidder, as part of this contract and on entering into it, shall become the data controller pursuant to Article 12 of the LOPD and Article 21c of Royal Decree (RD) 1720/2007). For the purposes of notifying the Data Protection Agency, the successful bidder shall agree to appear as the data controller of as many files as covered by this contract.

IV. The successful bidder may not use the aforesaid data for any other purpose other than the one indicated in the agreement adopted herein.

V. The successful bidder hereby undertakes to process the data pursuant to the instructions issued by the File Manager.

VI. Under no circumstances may the successful bidder communicate, reveal, assign or disclose the data, not even for their safekeeping, to third parties outside the contractual relationship established herein, except when specifically ordered by a Court.

VII. Subcontracting all or part of the contracted service to third parties is expressly forbidden, except in the case of the following requirements:

a. That said processing has been specified in the contract signed by LANTIK S.A. and the successful bidder.

b. That the personal data processing complies with the instructions of the File Manager.

c. That the successful bidder and the third party enter into a contract in the terms envisaged in Article 12.2 of Act 15/1999, of 13 December.

In those cases, the third party shall likewise hold the status of data controller.

VIII. The successful bidder hereby undertakes to abide by the applicable current legislation regarding data protection. Thus, any information to which its employees have access, as the result of this contract, shall be treated with the greatest confidentiality and it may not be disclosed to third parties or for its own use. The successful bidder shall be liable for any losses that may arise for the File Manager, LANTIK S.A. and for the parties affected.

IX. ***(Assess whether necessary)*** The successful bidder hereby certifies that its employees have signed a confidentiality clause where they undertake not to disclose the information to which they come into contact as part of their job or work during the fulfilment of the contract and subsequent to its term. . Should the successful bidder have been authorised to keep any data from the contract, it hereby undertakes to return it to LANTIK S.A. once the contractual obligations

have been fulfilled. In the case of legislation covering the keeping of the data, access to the data shall be duly blocked while legal liabilities may be sought.,

X. The successful bidder shall be subject to the liability established by data protection legislation and shall be personally liable should it use the data for a purpose other than the one stipulated herein, disclose the data to third parties or use them in any way that is in breach of the clauses of the contract.

XI. The successful bidder shall implement the necessary technical and organisational security measures established to current data protection legislation, according to the protection level of the personal data to which it has access during the provision of the services. The compulsory minimum security measures for this contract are set out in Annex I.

XII. Should the successful bidder provide its services at its own premises, outside those of the process manager, that circumstance shall be reflected in its own security document, indicating the file or process and its manager, along with the security measures to be implemented in relation to said processing.

XIII. The File Manager or LANTIK S.A, may, should they deem convenient, request the data protection audit report every two years. The report shall list the contracted services and the degree of compliance pursuant to the Spanish Personal Data Protection Act 15/1999 and its enactment regulations. The audit shall be conducted by independent expert, previously accepted by LANTIK S.A. and the successful bidder.

XIV. The successful bidder shall undertake to implement applications and information systems so that periodic data protection audits can be conducted.

XV. The breach of the duty of secrecy by the successful bidder or its employees, along with non-compliance of the personal data protection legislation, shall be grounds to terminate this contract..

ANNEX 1 - SECURITY MEASURES

The successful bidder shall implement the following security measures:

- **BASIC** data measures: The measures in paragraphs 1 to 20 shall be applied.
- **MEDIUM** data measures: The measures in paragraphs 1 to 27 shall be applied.
- **HIGH** data measures: The measures in paragraphs 1 to 33 shall be applied.

The data shall be classified according to Article 81 of RD 1720/2007, which can be summarised as follows:

- Basic level: All files or processing of personal data shall adopted the basic-level security measures.
- Medium level: The following files or processing of personal data shall also implement medium-level security measures, in addition to the basic-level security measures:
    - Those relating to criminal or administrative offences
    - Those relating to the provision of information services on asset solvency.
    - Those controlled by the tax administrations and relating to the exercise of the powers of taxation.
    - Those containing a set of personal data that provide a definition of the characteristics or identity of citizens and which permit the evaluation of specific aspects of their identity or behaviour.

- Other data controlled by financial institutions, Management Agencies and Common Services of the Social Security Institute, by the Mutual Funds for accidents at work and occupational illness associated with the Social Security and relating to the exercising of their powers.

- High Level: In addition to the basic- and medium-level measures, high-level measures will have to be applied when:
  - They refer to data on ideology, trade union membership, religion, beliefs, racial origin, health or sex life.
  - They contain or refer to data collected for security forces without the consent of the data subjects.
  - Those that contain data arising from acts of gender-based violence.

In case of any query, please contact the LANTIK S.A. Security Department.

BASIC-LEVEL MEASURES

- **Access through communication networks**

1. The successful bidder hereby undertakes that all the security measures required for access to personal data by means of communication networks shall guarantee an equivalent security level to the once for local mode accesses.

- **Work system outside the premises where the file is located**

2. The file manager expressly authorises the processing of personal data outside the premises where the file is located. The successful bidder hereby undertakes to guarantee the relevant security level for the type of file processed outside the premises. This authorisation covers all the process operations outside the premises where the file is located in the following cases:

    1. To host backup copies
    2. Data recovery
    3. Contingencies
    4. Contingency plan drills
    5. Equipment maintenance.

- **Temporary files**

3. The successful bidder hereby undertakes that the temporary files shall comply with the relevant security levels depending on the natural of the personal data stated by the File Manager.
4. The successful bidder hereby undertakes to delete any temporary file once it ceases to be necessary for the reasons for its creation.

- **Incident log**

5. The successful bidder shall have a procedure to notify and manage incidents, which must contain a log where the personal data file must be recorded, along with the type of incident, the time at which it occurred, the person who made the notification, to whom it was notified, the consequences and the corrective measures applied.

6. The successful bidder shall consider data recovery as a security incidence and shall, therefore, log them indicating the person who carried out the process, the restored data and, where applicable, which data needed to be manually recorded in the recovery process.

- **Identification and authentication**

7. The successful bidder shall establish a mechanism that allows any user who tries to access the information system to be identified unequivocally and on an individual basis and to verify that the user is authorised.

8. When the authentication mechanism is based on passwords, the successful bidder shall have an allocation, distribution and storage tool that guarantees their confidentiality and integrity.

9. The successful bidder hereby undertakes that the mechanisms that control the passwords shall require the user to change them at intervals not exceeding 1 year and while the passwords are in force, they shall be stored in an unintelligible form.

- **Access Control**

10. The users of the successful bidder shall only have authorised access to those applications with the profile required to carry out their duties, as established in description of the user administration service.

11. The successful bidder shall establish mechanisms to prevent a user from being able to access application with different rights other than the authorised ones.

12. Only authorised users may grant, alter or cancel authorised access to the applications.

- **Media management**

13. The successful bidder hereby undertakes to provide a catalogue with the inventory of the computer media that contain personal data, identifying the type of information that they contain, and to store them in a place with access restricted to authorised personnel.

14. The removal of the computer media containing personal data outside the premises where the file is located may only be authorised by the file manager.

15. The successful bidder hereby undertakes that when the medium is going to be discarded or reused, the necessary measures shall be adopted to prevent any subsequent recovery of the information stored in it.

16. The successful bidder hereby undertakes that when the media are going to leave the premises where the files are located, the necessary measures shall be adopted to prevent any improper recovery of the information stored in them.

- **Recovery and backup copies**

17. The successful bidder hereby undertakes that the procedures established to make backup copies and to recover data shall guarantee the restoration of the data in their state at the time of the loss or destruction, as indicated in the relevant operating manual.

18. The successful bidder hereby undertakes to make backup copies, at least once a week, unless the data has not been updated in that period.

- **Testing with real data**

19. The successful bidder hereby undertakes that the tests prior to the implementation or modification of the information systems that process personal data shall not be conducted using real data, except when the relevant security level for the type of file processed, by applying the security measures equivalent to those applied to the original file and making a backup copy beforehand.

- **Files on non-automated medium**

20. The successful bidder shall implement the specific measure to process files on non-automated medium that contain personal data:

    - It shall establish the criteria and procedures to file the media and documents in order to guarantee the correct safekeeping, location and consultation, and the exercising of the rights to challenge, access, rectify and cancel the data. In any event, the criteria established in the applicable sectoral standard shall be met.

    - The storage devices of the documents that contain personal data shall be fitted with mechanisms that hinder their opening and in any event, measures shall be adopted to prevent the access of non-authorised individuals.

    - Measures shall be implemented to prevent access of non-authorised individuals during the document processing and review processes.

MEDIUM-LEVEL MEASURES

- **Security Officer**

21. The successful bidder hereby undertakes to appoint one or more security officers who will be responsible for coordinating and controlling the effective application of the security measures applicable to the processing of personal data.

- **Audit**

22. The successful bidder hereby undertakes that an audit will be conducted of the data processing information systems and facilities to verify compliance of the regulations, of the current procedures and instructions regarding data security, at least, every two years. The information systems owned by the File Manager are excluded from the sphere of the audit.

23. The audit report shall establish the appropriateness of the measures and monitoring to **Title VII of Royal Decree 170/2007, which improves the Regulation enacting the Spanish Personal Data Protection Act 15/1999, of 13 December,** identify deficiencies and propose the complementary or corrective measures necessary. It shall also include the data, facts and observations on which the reports are based and proposed recommendations.

24. The audit reports shall be analysed by the competent security officer, who shall inform the data controller of the conclusions so he may take the adequate corrective measures and they shall be made available to the Spanish Data Protection Agency.

- **Identification and authentication**

25. The successful bidder shall limit the possibility of repeated attempts of unauthorised access to the information systems to a maximum of 5.

- **Media management**

26. The successful bidder shall establish a system to record the entry of media, , directly or indirectly, the type of document or support to be known, as well as the date and time, the issuer, the number of documents or supports included in the despatch, the type of information they contain, the method of despatch and the person responsible for receipt, who shall be duly authorised

27. The successful bidder shall establish a system to record the departure of media, , directly or indirectly, the type of document or support to be known, as well as the date and time, the issuer, the number of documents or supports included in the despatch, the type of information they contain, the method of despatch and the person responsible for receipt, who shall be duly authorised.

HIGH-LEVEL MEASURES

- **Media distribution**

28. The successful bidder hereby undertakes that the distribution of the media containing personal data shall be carried out by encoding such data or using any other mechanism that guarantees that such information is not accessible or manipulated during transport.

- **Accessing records**

29. The successful bidder shall have a mechanism that on each attempt to access the high-level data file:

- it shall store at least identification of the user, the date and time it was done, the filing system accessed, the type of access and whether it has been authorised or denied.
- Should access be authorised, it shall be necessary to store the information allowing the accessed record to be identified.
- The mechanisms that permit the logging accesses shall be under the direct control of the competent security officer and shall not permit their deactivation under any circumstances.
- The minimum period for storing the recorded data shall be two years.

- **Recovery and backup copies**

30. The successful bidder shall keep a backup coy and recovery procedures of the data in a different place to that housing the computer equipment that processes them which shall in any event comply with the security measures required.

- **Telecommunications**

31. The successful bidder hereby undertakes that the transfer of personal data through public or wireless electronic communications networks shall be done encoding such data or using any other mechanism that guarantees the information shall not be intelligible or manipulated by third parties.

- **Encoding**

32. The successful bidder shall ensure that the data that result in the file being classified as High Level shall remain encoded in the media and computer equipment that contain them.

- **Processing in non-automated processing**

33. The successful bidder shall implement the following procedures and media regarding the processing of high-level non-automated files:

  - The cupboards, filing cabinets or other elements for storing non-automated files with personal data shall be in areas to which access is protected by entrance doors with locks or another equivalent device. If that were not possible given the characteristics of the premises, the successful bidder shall adopt alternative measures that, duly justified, shall be included in the security document.

  - The generation of copies or the reproduction of the documents shall only be done under the control of the personnel authorised in the security document. Copies or reproductions to be discarded shall be destroyed to avoid access to the information contained therein or its later recovery.

  - Access to the documentation shall be exclusively limited to the authorised personnel and mechanisms shall be established to permit identification of access to documents that may be used by multiple users. he access of persons not included above shall be adequately recorded pursuant to the procedure established for this purpose in the security document.

  - Measures shall be adopted aimed at preventing access or manipulation of the information being physically transferred.

4 REVIEWING HISTORY

Review	Data	Change
00	17/07/2013	Standard approval