

InterPARES Trust Project Report



Title and code:	EU06 Girona City Council in the Cloud: Analysis of e-Services between Public Administrations
Document type:	Final report
Status:	Public
Version:	1.0
Research domain:	Policy
Date submitted:	July 2020
Last reviewed:	
Author:	InterPARES Trust Project
Writer(s):	Lluís-Esteve CASELLAS, City Council of Girona
Research team:	Sònia OLIVERAS, City Council of Girona Maria REIXACH, City Council of Girona

Document Control

Version history			
Version	Date	By	Version notes
1.0	July 2020	Lluís-Esteve Casellas	

Contents

Abstract or Executive Summary	4
Research team	5
Background	6
Aims and Objectives/Goals	8
Methodology	9
Findings	12
Conclusions	14
Products	16
References	34
Appendixes	36

Abstract or Executive Summary

The digital transformation of Public Administrations implies relevant changes in their business systems but also in the relationship between themselves, with providers and citizens. The exchange of digital information and records is already a standard practice. However, the key issue is to verify if these technological solutions take into account organizational aspects as Records Management and the preservation of the authenticity of records in the Cloud.

The focus is on how electronic services provided by Public Administrations affect the users, independently if they are Public Administrations or citizens. The results show that sometimes the services' conditions offered by public sector are not very different to those offered by private sector. The aim is that the conclusions of the case study of the City Council of Girona could be useful to design better policies and electronic services provided by Public Administrations to other Public Administrations and also for the citizens.

Girona City Council in the Cloud: Analysis of e-Services between Public Administrations

Research team

Lluís-Esteve Casellas Serra
Sònia Oliveras Artau
Maria Reixach Urcola

Project was disseminated at:

- Casellas, L-E. "E-Services between Public Administrations and Records Management, from the Local Government viewpoint in Catalonia". *Archival Science Colloquium – IntraPARES Trust International Symposium*. Marburg: Archivchule Marburg (Germany), 8 June 2016.
- Casellas, L-E. "Electronic services between Public Administrations: some recommendations for design and policies based on the case study of Girona City Council." *7th International Symposium of InterPARES Trust: Working with Digital Records: Studies in Archival Theory and Practice*. Jerusalem (Israel), 19 June 2018.
- Casellas, L-E. "Trustful e-Services in the Government-to-Government Context", *Trusting Records in the Cloud - The InterPARES Trust Open Seminar*. Roma (Italy), 10 December 2018.
- Casellas, L-E. "Trustful e-Services in the Government-to-Government Context". *11th ACA@UBC Symposium Policy Matters*. Vancouver (Canada), 15 February 2019.
- Casellas, L-E. "Trustful e-Services in the G2G Context: the case study of the City Council of Girona". *Symposium of Digital Preservation of Authentic Records*. San José (Costa Rica), 18-19 February 2020.

Disclaimer:

The documentation analyzed to carry out the work was collected mainly between 2014 and 2017. Most of the services under study were analyzed between 2015 and 2017. However, the continuous digital transformation of the Public Administration in Catalonia and Spain, and also at the Girona City Council itself, forced the revision of some services that have evolved over time, especially in 2018 and 2019. Although the analysis of the services that have evolved has been updated, not always it has been possible to do the same with the documents that regulate them. In some cases, it was because it did not exist previously or because it had not been updated at the time of the study. However, it was also needed to limit the analysis in time by the research team. Thus, possible omissions were not intended.

Background

In recent years, the legal framework of e-Government has gradually been taking shape, especially since the Digital Signature Act (2003). Subsequently, e-Government and electronic services for citizens (2007), information systems security (2010) and interoperability between public administrations (2010-2016) have been specifically regulated,¹ among other regulations that also have effect on e-Government, such as data protection, reuse of public sector information or transparency and good governance.² Besides these, the corresponding Catalan laws must be also taken into account: administrative procedure (2010), use of electronic media (2010) and transparency and good governance (2014).³

The most recent regulation, adopted in October 2016, is the Spanish General Administrative Procedure of the Public Administrations.⁴ Among other provisions, this new law establishes the obligation for public administrations to manage fully digital case files from October 2016, and to provide, within two years (2018), a digital archive service. If at the end of two years this service is not provided, or it is assessed as inefficient, administrations will have to use the service provided by the State. This law also strengthens the obligation to exchange data between administrations so that citizens do not have to submit documents they have presented before or that administrations already own.

Consequently, it is safe to say that the current legal framework advances inexorably towards e-Government, although the way of achieving it may not be that clear. In other words, the legal framework and the policies that foster e-Government have a clear technological component, specifically directed to the rationalization and efficiency in the

-
- 1 - Law 59/2003, of December 19, on Digital Signature. (Spanish) <https://www.boe.es/diario_boe/txt.php?id=BOE-A-2003-23399> [31.10.2016]
 - Law 11/2007, of June 22, on Electronic Access of Citizens to Public Services (effective repeal from October 2, 2016). (Spanish) <https://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/pae_NORMATIVA_ESTATAL_Leyes/LAW_11-2007_22Jun2007_eGov_Spain_NIPO_000-10-075-0.pdf> [31.10.2016]
 - Royal Decree 3/2010, of January, on National Security Framework. (Spanish) <http://www.boe.es/aeboe/consultas/bases_datos/doc.php?id=BOE-A-2010-1330> [31.10.2016]
 - Royal Decree 4/2010, of January, on National Interoperability Framework. (English) <https://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Estrategias/pae_Interoperabilidad_Inicio/pae_Eschema_Nacional_de_Interoperabilidad/ENI_INTEROPERABILITY_ENGLISH_3.pdf> [31.10.2016] All Technical Interoperability Standards approved between 2011 and 2016 are available in English on <https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Interoperabilidad_Inicio/pae_Normas_tecnicas_de_interoperabilidad.html#WCisfnhCaE> [31.10.2016]
 - 2 - Organic Law 15/1999, of December 13, on the Protection of Personal Data. (Spanish) <<https://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf>> [31.10.2016]
 - Law 37/2007, of November 16, on Reuse of Public Sector Information. (Spanish) <<https://www.boe.es/boe/dias/2007/11/17/pdfs/A47160-47165.pdf>> [31.10.2016]
 - Law 19/2013, of December 9, on Transparency, Access to Public Information and Good Governance. (Spanish) <<https://www.boe.es/boe/dias/2013/12/10/pdfs/BOE-A-2013-12887.pdf>> [31.10.2016]
 - 3 - Law 26/2010, of August 3, on Legal Regime and General Procedure of the Public Administrations of Catalonia. (Catalan) <<http://portaldogc.gencat.cat/utillsEADOP/PDF/5686/1090627.pdf>> [31.10.2016]
 - Law 29/2010, of August 3, on the Use of Electronic Media in the Public Sector of Catalonia. (Catalan) <<http://portaldogc.gencat.cat/utillsEADOP/PDF/5687/1106073.pdf>> [31.10.2016]
 - Law 19/2014, of December 29, on Transparency, Access to Public Information and Good Governance. <<http://portaldogc.gencat.cat/utillsEADOP/PDF/6780/1395384.pdf>> [31.10.2016]
 - 4 - Law 39/2015, of October 1, on General Administrative Procedure of the Public Administrations. (Catalan) <http://boe.es/diario_boe/txt.php?id=BOE-A-2015-10565> [31.10.2016]

use of technology, although economic saving is undoubtedly the main objective.⁵ By contrast, organizational aspects (like records management) have been either underestimated or their application has been implicitly assumed. For instance, there is no state law that explicitly refers to records management and, in fact, the only regulation that obliges all public administrations to have a records management system is the Archives and Records Management Act of Catalonia (2001), although without resources to be truly effective.⁶

Thus, taking into account the 8.000 existing municipalities in Spain, the correct question is not how many of these will be able to comply with the law by the end of 2016 but rather why the majority will not be able to do so. In this sense, one of the key factors is the weakness of records management within the public administrations and e-Government policies.⁷

Regarding the particular case of Catalonia, one might think that the situation in this matter is slightly better, because of the Catalan Records Management Act, although it is important to note that 63% of the 947 existing municipalities do not exceed 2.000 inhabitants. How will these municipalities face the compliance of the Spanish Law and, consequently, the transformation to digital in the short term? The answer is not clear at all. In this context, the city of Girona (with almost 100.000 inhabitants and a little over 1.000 municipal employees) should be, in principle, better positioned to achieve this goal.

In spite of this scenario, or because of it, the Spanish Government has promoted, mostly during 2015 and 2016, a set of electronic services to be shared by all administrations. These services coexist with other services offered by regional public administrations, with a level of use in constant growth. The consequence is that, with or without records management policies (more specifically digital preservation policies), both Spanish public administrations and citizens have thrown themselves into creating and exchanging digital records amongst them. The question is what to do with these records, most of them orphaned of records management systems.

Therefore, the main issue is to identify what electronic services (e-services) are used, who offers them and how are they offered. In this sense, we define **e-service** as:

Any technological resource (infrastructure or application) that facilitate access to platforms of business management, information exchange, data interoperability or data validation and verification. In a more extended meaning, it also cover the provisions of any service to the citizens

All public administrations act as services providers, either to citizens or to subordinate administrations. In this context, municipalities receive services mainly from the State and

5 The Report of the Spanish Commission for Public Administration Reform (CORA) illustrates this perspective, mainly focused on the structural changes to reduce expenditures considered as unnecessary. In other words, savings becomes the aim, not the consequence of a better design of the services' processes. (English) <http://www.seap.minhap.es/dms/en/web/areas/reforma_aapp/CORA-INGLES--web-/CORA%20INGLES%20%28web%29.pdf> [31.10.2016]

6 The analysis of results of the Catalan Law regarding Records Management in Public Administration is available in Lluís-Esteve Casellas, "La Llei d'arxius i documents i la gestió de documents: cinquanta ombres de la llei" (The Archives and Documents Act and Records Management: fifty shades of the Law), in: Lligall. Revista d'Arxivística Catalana 36, 2013, p. 21-40. (Catalan) <<http://www.arxivers.com/index.php/documents/publicacions/revista-lligall-1/lligall-36-1/1339-03-la-llei-darxius-i-documents-i-la-gestio-de-documents-cinquanta-ombres-de-la-llei/file>> [31.10.2016]

7 María Mata Caravaca, Appendix 3. Spanish Legislation on Records Management and Digital Preservation, in: EU04 (2016) Policies for recordkeeping and digital preservation: Recommendations for analysis and assessment services. Final Report, Stefano Allegrezza, Gabriele Bezzi, Maria Guercio, Letizia Leo, Maria Mata Caravaca, Matteo Monte, Ilaria Pescini, Brizio Tommasi, 2016, p. 38-50. <https://interparestrust.org/assets/public/dissemination/EU04_20160811_FinalReport.pdf> [31.10.2016]

regional governments and, to a lesser extent, from provincial governments. While most of these services are in principle voluntary, some become mandatory, since they are the last link in the chain of public administration.

In the case of Catalonia, moreover, there is the Open Administration of Catalonia (AOC), a consortium of Catalan public administrations created 15 years ago to promote their digital transformation. AOC is in fact the major provider of electronic services in Catalonia because its function of intermediation between public administrations. AOC is also an exceptional and unique case in Spain because any other regional government has create a similar service with the collaboration of provincial and municipal administrations. Nevertheless, Catalan Government offers some electronic services outside of this consortium, as well as those from provincial governments.

Aims and Objectives/Goals

The aim of the present work is to analyze how the current implementation of electronic services in the Spanish public administrations affects or is likely to affect the records management in the City Council of Girona and, more specifically, the preservation of these records from the authenticity viewpoint.

Thus, our main goal is to improve the integration of these electronic services in the records management system of the municipal organization. Nevertheless, integration is not only treated from a technological perspective, but rather from an organizational one. That is why one of the final products of the study expect to be a set of guidelines for improving policies on the use of electronic services in the City Council.

Beyond this obvious objective for the City Council, this work also seeks to go one-step further: our intention is to foster the interest and the debate within the Catalan professional community in order to influence the policies of those public administrations that provide electronic services, particularly the Catalan public administration.

Furthermore, from the analysis and results of this work we should be able to assess the services that the City Council itself offers to citizens, which in turn should allow introducing the necessary improvements for the provision of these services with sufficient security guarantees and the citizens' trust.

In conclusion:

- How do e-Services affect RM and the preservation of authenticity.
- To get a strategy to manage services provided in the Cloud.
- To influence policies of Public Administrations as e-Services providers.

That would be materialized by checking the policies and procedures to formalize the adhesion to the digital services provided by public administrations with a specific test of verification. Thus, in products for public administrations similar to the existent for the private providers referred to bid specifications, checklist and statements of responsibility.

Methodology

To analyze the set of all these services we will establish the following phases:

1. Identification of the set of services used between public administrations.
2. Assessment of the general degree of trust of the services.
3. Identification of the services that could affect the Records Management System of the City Council of Girona.
4. Assessment of the preservation of the authenticity of records.

1. Identification of the set of services

This phase focused on the only two online catalogues available, which corresponded to the main providers of electronic services in Catalonia: the Spanish Government and the Open Administration Consortium of Catalonia. The comparison of these catalogues, however, were not aligned, as can be seen below:

- Spanish Government (59 e-services):
 - E-Government and services to citizens (47, grouped in 11 sections).
 - Internal management (7).
 - Infrastructures (5).
- AOC Consortium (30 e-services):
 - Relations with citizens (10).
 - Internal management (7).
 - Relations between Public Administrations (5).
 - Identity and electronic signature (8).

2. Assessment of the general degree of trust of the services

In parallel with the revision of the catalogues, it was done a search for identifying the regulation at general level of the services, mainly in terms of policies and procedures for formalizing accession to the service. The aim was to analyze the regulation of these services according to the criteria of the *NA14 Cloud Service Provider Contracts Checklist* case study (Bushey, 2016), adapted to the public sector.

The baseline requirements for service providers used to analyse the public services were structured in four main groups of clauses referred to the following issues:

- CONTRACT MANAGEMENT
 - Regulation on the provision of services.
 - Subcontracting.
 - Information portability.
- INFORMATION SECURITY
 - Data location.
 - Infrastructure security measures.
- CONFIDENTIALITY AND PERSONAL DATA PROTECTION
 - Confidentiality agreement.
 - Responsibility for personal data protection.
 - Data protection measures and audits.
 - Rights of access.

- Destruction of data.
- RECORDS MANAGEMENT
 - Corporate management.
 - Characteristics of records.

This checklist focused mainly on contract regulation, information security, data confidentiality and records control. For this reason, it was intended to complement the analysis with the general principles derived from “Digital Records Maintenance and Preservation Strategies”, defined in *Preserver Guidelines. Preserving Digital Records: Guidelines for Organizations* (Hackett, 2008, Requirements Set C; InterPARES 2).

The planned analysis aimed to assess the degree of trust based on the general policy of the provider or, failing that, the specific policy of the platform and / or the specific policy of the service. However, the result was quite negative given the non-existence of general policies really. When it existed, it was very usual the lack of specification or the generalities of the terms of service and the conditions of accession to the services. In addition, not always this information was published online.

3. Identification of the services that could affect the Records Management System

Among the set of 89 services identified in the catalogues, 31 were detected that directly or indirectly affected the Management System. The non-existence of policies and regulation of services required a more detailed analysis. For this reason, since the number of services and the availability of the research team, its study was limited to the comparative analysis of the purpose of each service. This comparison allows us to identify six functional types of services:

1. Creation of records, usually by means of a structured template.
2. Transmission of data and records, by submitting or entering to an external system.
3. Publication of data and records on public platforms, official registries or official journals.
4. Verification of data and records, which substitutes documents provided by citizens.
5. Software application for business management, temporary storage or preservation over time.
6. Identity and digital signature, as a means of access to e-services and records validation.

For the purpose of the case study, the specific services for managing business activities and those aimed at identity and digital signature were discarded, placing as critical factors the creation of documents, their transmission, publication and online verification.

In any case, 16 of the 31 services were selected to be analyzed in more detail in relation to:

- The impact on the records management of the Girona City Council.
- The preservation of authenticity and, as a whole,
- The degree of trust that these services offered.

4. Assessment of the preservation of the authenticity of records

The majority lack of policies and regulations of service provision forced a more detailed analysis of each selected service. The analysis focused on three lines of work:

1. The formalization of the accession to each service.
2. The attributes of the records and the actions that guarantee their authenticity.
3. Obtaining authentic copies or new records that guarantee to get evidence of the actions carried out.

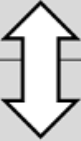
The review on the formalization of the accession to each service was oriented to identify the regulation of the service at low level and the control and the management of users of the City council of Girona who use them. The reference document used was the checklist for private providers (NA14).

As for the attributes to ensure authenticity and to obtain authentic copies, the requirements of Appendixes A and B of *Preserver Guidelines: Preserving Digital Records: Guidelines for Organizations* (Hackett, 2008; InterPARES 2) were adapted as checklists:

- *Benchmark Requirements for Supporting the Presumption of Authenticity of Electronic Records (Requirements Set A)*, for the creation of records or evidence of transactions carried out.
- *Baseline Requirements Supporting the Production of Authentic Copies of Electronic Records (Requirements Set B)*, for obtaining authentic copies of records when the e-service was for verification of records or data.

The impossibility to get indicators of some of the 16 selected services motivated that the final study was limited to eight services. However, the sample was considered enough solid since from a quantitative point of view it represented more than 25% of the services. From a qualitative point of view, the owners of the services were different administrations and were also offered from various platforms, own or intermediated.

Analysis Scheme

	PURPOSE	GUIDELINES	ANALYSIS OBJECT	SCOPE	TYPES OF ACTION
TRUST 	Services	Checklist NA14 InterPARES Set C Req.	General Policy Platform Policy Service Policy Terms and Conditions Accession Procedure	Institution Platform Services	Creation Transmission Publication Verification
				Records	Creation
AUTHENTICITY	Records	InterPARES Set A Req.	Records (A1 Req.) Systems (A2 to A8 Req.)	Evidence of action	Creation Transmission Publication Verification
				Copy of a record Copy of an evidence record	Creation Transmission Publication Verification

Findings

The main findings from the case study:

1. The analysis of public services requires the existence of an integrated catalogue of the set of services offered by the all levels of public administrations, or at least guidelines to stablish that the catalogues must be aligned.
2. The non-existence of an unique catalogue of services and the lack of regulation on them and, specifically, on the control of users prevent that the City Council of Girona is able to keep tools to control the use of external electronic services when the provider is a public administration. That is, for instance, the Catalogue of Applications, mainly for private cloud services providers, and the Register of Authorized Users of external e-Services.
3. Regarding the proposal to analyse (Requirements Set C of InterPARES) general policies, policies about the platforms and/or policies about the service of the public providers, general policies and policies on the service regulation are non-existent. For this reason, we have had to assess the general policy of e-Government Portal as the main regulation at the highest level. The AOC Consortium is the exception, since it accomplishes the tree levels.
4. Therefore, in the best case, it has been necessary to assess the general conditions under which the services are provided or, directly, the procedures and records to formalize the accession to them, when they exist. The AOC is the only one that offers a greater and better regulation of the conditions of provision of the services, also with

clear procedures for the accession to the services. In the case of the services of the Spanish Government, the information available and the regulation is quite unequal, while they are practically unusual in the services of the Catalan and Provincial Governments.

5. In any case, the information regarding the control of the records managed in these services, their conservation and the preservation of authenticity have not been taken into account in any of the documents analyzed. In this sense, essential requirements as the protection against the loss and corruption of the information or about preservation measures on media or technologies (Requirements Set A of InterPARES) are weak or not informed.
6. The preservation of authenticity in all the services analyzed is based on the digital signature. The traceability of actions by user administrations is almost never possible.
7. The traceability of actions is often conditioned by a lack of sufficient control in the management of users authorized to use these services. This information is generally not available from the Administrations using the service.
8. Very few services allow the obtaining of evidence about the action taken or obtain authentic copies of the records submitted technologies (Requirements Set B of InterPARES), especially when the service involves the creation of a record directly on the provider's platform. Most of the services that allow getting evidence are offered by the AOC.
9. Most services are not integrated with the management systems of user administrations. Therefore, any obtaining of evidence involves organizational measures. Thus, these guidelines on the organization of work always depend on the voluntariness and capacity of the staff.
10. In some cases a clear lack of control is detected over the records generated or transmitted, mainly in the services designed longer ago which, very often, are also the ones that offer a less strong control over the management of users.
11. Among all the services analyzed, the intermediation function of the AOC is valued in a particularly positive way. AOC is the only provider that offers the possibility of establishing some automated integrations with the management systems of the user administrations. This integration allows capturing traceability in an automatized way.
12. Regarding the service integration to the systems, there is an relevant lack about the critical requirements needed. Specifically, that is the requirement for the preservation of the authenticity (Requirements Set A of InterPARES) referred to the archival bond and the identification of the authoritative record.
13. Additionally, the intermediation function of AOC appears to be really useful because implies a normalizing effect on the administrations users and also acts as a multiplier of digital transformation to the public administrations. On the other hand, it is efficient since it facilitates an integration 1:n instead of n:m in relation with the all public providers.
14. The functional systematization of electronic services from the point of view of records management has facilitated the detection of common deficiencies related to the control of records, the traceability of actions and the preservation of authenticity. Therefore, also the identification of possible improvements to be

introduced that, nowadays, must be supplemented with organizational guidelines and operations to be performed manually.

15. Finally, one of the main improvements that would surely strengthen the control, traceability and integration of processes would be the replacement of information transmission services based on the sending of records by records exchange services in shared repositories between public administrations. In this way, each administration could be able to control what is deposited, who and when it does so and to regulate cooperatively how it is done. At the same time, this would allow a real simplification of communication between public administrations.

Conclusions

Firstly, we must admit that there has been a considerable legislative and technological effervescence during these last years, and positive results are to be expected at least in the medium term, but not before.

The legal framework is clearly focused on e-Government and it may be considered as appropriate. However, one of the main difficulties lies in the organizational aspects derived from the implementation of fundamentally technological solutions, which in most cases are carried out without additional resources. In this sense, the lack of clear and precise regulations on Records Management is actually a major weakness in the Spanish model and, in a certain way, it responds to a very traditional perception of archives.

Regarding the e-Services offered by Public Administrations, a remarkable effort has been made to design modular and interoperable solutions. AOC's intermediation service as provider of e-Services is particularly important, since it facilitates its use.

However, it should be noted that certain weaknesses shall condition the success of digital transformation:

- Despite the efforts made towards e-Government, the development of a records management system, even its very existence, is left entirely at the discretion of each organization. Therefore, there is no legal framework that determines that records management systems should be mandatory.
- The integration of e-Services to the business systems of user administrations is complex. The solutions offered, however good they are, are partial and do not solve management as a whole, hindering its implementation. In other words, if this integration with internal workflows is not possible, the result is totally the opposite of the efficiency goal of the e-Government.
- In general, the approach taken by Public Administrations as services providers is more collaborative than cooperative. The needs of other administrations as users of these e-Services haven't been taken into account, especially those services provided outside the intermediation service of the AOC. In these cases the aim of electronics services is often the benefit of the public administration that provides them.
- Except for AOC, there is a lack of general policies on the provision of electronic services by the administrations that offer them, and even on the specific regulation terms of each service. This usually has a clear impact on the formalisation of the

service and the internal regulation of user organizations; for example, users' authorizations, documentation control, etc.

- The tendency to base authenticity on the digital signature is clearly a very short term viewpoint of the task in hand and it should be corrected as soon as possible: what will happen with small organizations without record management systems when they have to transfer their records out from these services platforms? In this sense, the traceability of actions needs to be strengthened, as well as the identification of actions from which we have to obtain evidence.

Specifically for the City Council of Girona, the case study has allowed to identify deficiencies of the electronic services used and the establishing of guidelines to solve them addressed to the staff. Therefore, it has been mainly organizational measures since the changes on the services depend on the provider.

These measures has focused on the reinforcement of the procedures to authorize users to access the services and also its control. On the other hand, guidelines about getting evidence of action have been taken. Obtaining these evidence records and its integration to Records Management System, unfortunately, is always a manual process, thus training and making aware the staff have been a priority.

Finally, the influence to public providers is not easy to get, although some small changes have been obtained. Nevertheless, the most relevant have been the possibility to raise awareness the professional community by the introducing the results in several dissemination and training events in Catalonia and Spain.

Products

Product 1. Requirements for contracts with record and / or data management.

- Contract management.
- Security information.
- Confidentiality and protection of personal data.
- Records and data Management.

Product 2. Checklist of the requirements of cloud contracts.

Product 3. Recommendations for the planning and the design of electronic services between Public Administrations.

Product 1

Requirements for contracts with record and / or data management

1 Contract management

- 1.1 Regulation of the provision of the service
- 1.2 Subcontracting
- 1.3 Portability of information

2 Security of information

- 2.1 Data location
- 2.2 Security measures
- 2.3 User management

3 Confidentiality and protection of personal data

- 3.1 Commitment to confidentiality
- 3.2 Responsibility in matters of personal data
- 3.3 Security measures
- 3.4 Collection of data and rights of the people interested
- 3.5 Disposal of data

4 Records and data management

- 4.1 Regulation and transparency
- 4.2 Corporate management
- 4.3 Characteristics of records and data
- 4.4 Preservation of the authenticity

CONTRACT MANAGEMENT

Regulation of the provision of the service

1. Regulation of services provision municipal information management will be based on Law 9/2017, of November 8, on Contracts of the Public Sector, which transposes to the Spanish legal system the Directives of the European Parliament and of the Council 2014/23 / EU and 2014/24 / EU, of February 26, 2014.
2. by the contractor, and by the City Council will act as interlocutors to monitor this contract and to solve the incidents that may arise, in accordance with the provisions of Law 9 / 2017, art. 62

Subcontracting

3. In accordance with the provisions of Law 9/2017, additional provision 25:
 - The tenderer will provide the City Council with information regarding the identification of the subcontractors, as well as with the information to verify them.
 - The provision of services by subcontracted third parties will be carried out with the same security and treatment guarantees stipulated for the main provider.

Portability of information

4. The tenderer will guarantee at all times the portability of the data derived from the management of the contracted service, in accordance with the following requirements:
 - The delivery of the data and records will be made at the end of the contract in the format agreed in the contract.
 - The delivery time will be as short as possible and in no case will it prevent the continuity of the service if it has been awarded to another provider, which will facilitate the transfer of data.
 - The delivery of the data and records will be with the necessary requirements to guarantee their integrity and authenticity.
 - The portability of the data and records will not imply any expenses related to these actions in any case.
5. The portability of data may be requested in advance when reliable treatment of a subcontracted company has been detected in a reliable manner. It may also be required when unilateral changes are made by the provider of the conditions for the provision of the service.
6. The export made by the tenderer must be verified and validated by the City Council of Girona, the new tenderer who performs the order or a third party that the same City Council designates. The tenderer will facilitate this process as much as it can.

SECURITY OF INFORMATION

Data location

7. The tenderer will always prove the location of the servers where the data is managed and stored, as well as the location of the backup copies.
8. The location of the servers, own or of third parties, either for the data managed or backups, will always be within the European Economic Area (EEA: European Union, Iceland, Liechtenstein and Norway).
9. The tenderer must inform of international service transfers are foreseen in the service management, that is, outside of the EEA. In this case, they will only be made when there are sufficient legal guarantees and these transfers are authorized by the Spanish Data Protection Agency (AEPD) or the European Commission.
10. The transfers of data that may need to be carried out outside the accepted countries will always and previously require the agreement of the City Council of Girona and the mandatory authorization of the AEPD, in accordance with the international guarantees established at any time.
11. The tenderer is obligated to inform the City Council of Girona whether a competent authority of a third country can request and obtain information on personal data of the files that it manages on its servers, or those that it has contracted, and under what conditions.
12. The breach to comply with the clauses on the location of the servers will be the reason for the termination of the contract and the City Council of Girona declines any responsibility and compensation for this reason, as well as the denial of the authorization of international transfers by the AEPD.
13. The cancellation of the agreement between the European Union and the United States, as happened with the Save Harbor, to allow international transfers of data with American companies that are in the agreement will imply its new approval and regularization before the AEPD or acceptance in the following established agreement. The negative resolution of the agency will be cause for termination of the contract without any penalty or compensation in charge of the City Council of Girona.

Security measures

14. The tenderer and any possible subcontractor must have and prove that they have a contingency plan in regard to security.
15. The tenderer must have qualified professionals and with ideal levels of management and maturity in the services provided.
16. The tenderer and any possible subcontractor must provide a precise, documented and accredited reference that the security products, equipment, systems, applications or their components have previously been certified by the Certification Body of the National Assessment Scheme and Certification of Security of Information Technologies. In the case that this certification does not exist or that is in process, it will also include a precise, documented and accredited reference that is the most suitable, in accordance with the specific administrative clause of Annex V, of Royal Decree 3 / 2010, of January 8, which regulates the National Security Scheme in the field of Electronic Administration (ENS).

17. The technical description of the service that involves automatic processing of personal data must include the treatment of special categories of personal data, according to article 9 of Regulation (EU) 2016/679 of the European Parliament and the Council, of 27 d April 2016, regarding the protection of natural persons with regard to the processing of personal data and the free movement of these data and which repeals Directive 95/46 / EC (General Regulation on data protection).
18. The subcontractors will have to apply the levels of security of the information appropriate to the risks, in accordance with what establishes the RGPD in the article 32.
19. The necessary measures in the storage and transmission of data in surroundings considered insecure (portable, personal assistants, peripheral devices, etc.) will also be adopted, in accordance with article 21 of the ENS.
20. Measures to guarantee the confidentiality of the stored information and the transmissions may be by encryption or by fragmentation, or by their combination, as determined in each case.
21. The City Council of Girona will have to have the relevant information about the methods of data encryption by the bidder.
22. The tenderer will also have to inform the City Council of Girona of the possible security measures that it will have to take to avoid damaging their data.
23. The tenderer will assume the obligation to register the incidences that affect the data and the measures taken to solve them and to inform the City Council of Girona, in accordance with the provisions of the ENS.
24. The tenderer and its subcontractors will back up with guarantees of availability and integrity of the data and will have a continuity plan for the activity to deal with possible incidents that may affect their information systems.
25. The tenderer will submit to ordinary and extraordinary audits in accordance with the provisions of the ENS (art. 34), and will have to provide accurate information of who performs them and the standards based on.
26. The tenderer must also provide information on how the security measures will be taken internally and the City Council of Girona will always have the option of verifying them and accessing the records of access to the data, as well as the audits of internal and external security.

User management

27. As basic security requirements the system should have, if applicable:
 - It will provide the access to the information to personnel of the City Council of Girona to realize the functions of opportune management and control.
 - It will provide its own functionality to access controls, as well as having functions that allow customizing, for each user profile, its access and operation features. Profile management must be centralized in a figure (Profile Administrator) associated to one or more people within the City Council of Girona, who will be responsible for the assignation, modification and/or denial of access permissions to the users.
 - It will provide to define profiles for external users of the City Council of Girona, with the purpose of providing different functionalities to specific groups and duly identified taxpayers.

- The security module will offer, for each user, only the features associated with its profile. It will have a management tool for manage profiles by non-computer personnel, to customize the application environment under the premise initially required (user interface determined by its profile).
- The security module will have passphrase verification functions, which must be customizable, as well as passphrase format validation mechanisms (minimum length, symbols, rules ...), causing deactivation after a given number of failed access attempts in the authentication process.
- It will record all movements made by each user, at transaction level, including unfruitful access attempts that may occur. These audit trails will allow an exhaustive control and integrated with the operations that are carried out.
- It will have a historical file of movements, offering specific queries and reports that allow auditing the operations carried out based on multiple criteria, allowing to obtain status and characteristics chronologically and operating.
- It will allow the use of different digital certificates (at least those issued by the FNMT and CATCert) and the electronic DNI as part of the authentication process.
- It will incorporate mechanisms that allow the electronic signature of the records that are generated in the system itself.
- It will have audit tools that facilitate the diagnosis and treatment of incidents.

CONFIDENTIALITY AND PROTECTION OF PERSONAL DATA

Commitment to confidentiality

28. The data managed through the service will be exclusively for the use described in the contract and it is totally forbidden to make different use on the part of the successful tenderer or previously unauthorized third parties.
29. The tenderer will inform the City Council of Girona about the confidentiality instructions that his staff governs.
30. The confidentiality on the part of the tenderer and all its personnel will be maintained during the period of validity of the contract and also once this is extinguished.

Responsibility in matters of personal data

31. The applicable legislation is the Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, relative to the protection of the physical persons with respect to the treatment of personal data and to the free circulation of these data and repealing Directive 95/46 / EC (General Regulation on Data Protection - RGPD), Organic Law 3/2018, of December 5, on the Protection of Personal Information and Guarantee of Digital Rights (LOPDGDD) and , if applicable, their corresponding valid at all times.
32. The City Council of Girona is responsible for the file or files with personal data, as defined in the RGPD (article 4).
33. The access, management or integration of personal data into systems that are the property of the tendering party implies that the latter is in charge of processing the file,

as defined in the RGPD (article 4) and with the obligations established in Law 9/2017 (additional provision 25a). The City Council of Girona will continue to be the person in charge of the file with personal data, as defined in the RGPD (article 4), of the file itself and the results derived from the treatment and management of the service.

34. The subcontractors will be considered as responsible for the processing of the file, in accordance with Law 9/2017 (additional provision 25a), as stated in the contract, the data are managed in accordance with the instructions of the City Council of Girona and between the tenderer and the subcontractor there is written contract in the terms provided for in the RGPD (art. 28.3). There will always be prior authorization from the City Council of Girona that will allow the tenderer to appeal to another contractor, according to the RGPD (article 28.2), and inform in any case if there are changes.
35. If there is a subcontractor there will always be a contract or any other legal act that imposes the same data protection obligations as those of this contract, especially the appropriate technical and organizational measures.

Security measures

36. The tenderer will apply all the security measures established by law and, as responsible of the file, it will collaborate with the City Council of Girona to describe the treatment of data to include it in the Registry of the treatment activities of the City Council of Girona.
37. The applications contracted for the provision of the service must allow a correct management of users and accesses, as well as of traceability of actions if the level of sensitivity of the data requires it.
38. If the service is carried out in the premises and/or systems of the tenderer, it undertakes to implement the measures to guarantee the integrity and security of the data required by the responsible.
39. If the service is carried out in the premises and/or systems of the tenderer, it must indicate the postal address or specific reference so that the City Council of Girona can know the details.
40. It will be necessary to incorporate and comply with all the points indicated in the RGPD (section 3 of article 28).

Collection of data and rights of the people interested

41. In the data collection forms will be used the informative text approved by the City Council of Girona, with the information determined in the RGPD (Article 13) and express mention of the tenderer's responsibility as processor of data, if it applies.
42. The tenderer will guarantee cooperation and will provide tools for the exercise of rights of access, rectification, erasure, restriction of processing, object and portability of data by citizens.
43. The tenderer will provide detailed information on the procedure of exercising the rights of access, rectification, erasure, restriction of processing, object and portability of the data and who will assume the execution and response to the interested parties, within the deadlines established by law, and will inform to the City Council of Girona.
44. In the event that the rights are exercised directly with the processor of data and it can solve it, it will inform to the City Council of Girona.

Disposal of data

45. Upon finalizing the provision of the contracted service, the tenderer will commit to the destruction of the data in a secure manner, once returned to the City Council of Girona or transferred to the new person in charge of the treatment that the City Council of Girona could have designated and provided the export It has been verified and validated by the City Council of Girona. The data that for reasons of derived responsibilities should be kept for a while will be blocked in an appropriate manner.
46. The tenderer will formally certify the removal or blocking of data subject to the provision of the contracted service, as well as those derived from its management.
47. The tenderer will inform the City Council of Girona about the methods and mechanisms of removal and blocking of data that apply to the data managed.
48. The tenderer will offer at any time of the contract, upon completion or during the period of data blockage after the contract has ended the portability of the data at the request of the contracting party.

RECORDS AND DATA MANAGEMENT

Regulation and transparency

49. The tenderer must prove that the creation, maintenance, management of records and data in their application or system comply with the basic requirements of the Records Management Systems, in accordance with the provisions of Law 10/2001, of July 13, of Archives and Records Management of Catalonia, in Law 39/2015, of October 1, of the Common Administrative Procedure of the Public Administrations, in the Royal Decree 4/2010, of January 8, by which the National Scheme is regulated of Interoperability in the field of Electronic Administration (ENI) and its technical standards.
50. The tenderer must demonstrate compliance with the legislation on transparency and right of access to information, including the active publicity of the information and the control and recovery of data necessary for the rendering of accounts in matters of transparency, auditing and control of the City Council and for the exercise of the right of access by citizens.

Corporate management

51. If the provision of the service affects transversal and corporate processes of the administrative management such as the processing of resolutions and agreements and the registers of incoming / outgoing records, the tenderers will have to adopt the measures set by the City Council to integrate these records and data to the corporate systems of the City Council, with the structure, form, format and periodicity established in the contract.
52. It will be valued especially that this integration is daily on the records and the data already properly validated.

53. The creation and management of records must guarantee the basic requirements of the corporate management, in accordance with Law 10/2001 and of the ENI, especially the application of:
- Business Classification Scheme.
 - The management and automated application of the Evaluation Tables in accordance with the Disposition Calendars of the City Council and the provisions of the National Commission for Access, Evaluation and Selection of Records of Catalonia.
 - The management and automated application of the Transfer Calendar in accordance with the Business Classification Scheme.
 - The management of the access system for records, with the exceptions of restriction and the terms of exclusion periods.
 - Obtaining recapitulative records based on the evaluation and selection of system data in the form of registration, formats and periodicity that are established.

Characteristics of records and data

54. The tenderer must prove that the records will be created with the guarantees of legal validity specified by Law 39/2015 (article 26.2), referring to the identification of the records, the date, the corresponding metadata and the signatures or sufficient means that have been established for their authenticity.
55. The applications that create and manage the records and data must comply with the requirements of the Interoperability Technical Standards and specifically those referred to:
- Interoperability in relation to the recovery and preservation of digital records throughout their life cycle, by incorporating the corresponding metadata (ENI, Chapter XI, especially Article 21).
 - Interoperability in the digital signature and certificates policy (ENI, Article 18).
 - The long-term preservation of digital records in the formats that are set, in accordance with the ENI (Article 23).
 - The guarantee of the electronic copies that must be issued (Law 39/2015, article 27.3).
 - The necessary metadata for the identification and management of the digital records and, if it is the case, its integration to the corresponding digital file.
 - Indexing, partial or definitive, of the file and its closure, as well as the exchange format with other Public Administrations.
 - The formats used for the creation, maintenance and export of records and digital data will always be accepted by the Catalogue of Standards, Resolution of October 3, 2012, of the State Secretariat of Public Administrations, which approves the Interoperability Technical Standard of the Catalogue of standards and, if applicable, those in force at any time.

Preservation of the authenticity

56. The administrative files will be created and managed in accordance with Law 39/2015

(art. 70) regarding the aggregation of records and their foliation, and with the specifications set by the ENI when it is necessary to transfer them to a public Administration or to the City Council itself.

57. Records and digital files shall at all times maintain compliance with the requirements necessary for long-term preservation by means of records management metadata that accompanies them, in accordance with the specifications of the ENI and those that may be set by the City Council in its record management and preservation policies.
58. The records will preserve the information referred to their digital signature regardless of the signature type. The records received from third parties signed by a qualified signature will be verified at the time of their capture and the signature verification information will be associated with the proces of the corresponding file.
59. The records shall be retained in accordance with the principle of a unique archive established by Law 39/2015 (article 17), with guarantees of integrity, authenticity, confidentiality, preservation, and traceability of actions according to which they have not been manipulated in no time.
60. The transfer of documentation to the management systems of the Municipal Archive will always include as a requirement the prior verification of the integrity of the transferred records, in accordance with the City Council's records management and preservation policies.
61. The City Council may require from the supplier the accreditation of monitoring systems to ensure the integrity of the records, as well as the identification of the algorithms and mechanisms that are applied.

Product 2

Checklist of the requirements of cloud contracts

Yes No Obs

CONTRACT MANAGEMENT

Regulation of the provision of the service

1. Has the service provision been regulated? In what format? (clause 1)
2. Is there a person responsible for the contract? Who? (clause 2)

Subcontracting

3. Is there subcontracting of work? (clause 3)
4. Are the data of subcontractors provided, if any? (clause 3)
5. Is the detail of the services provided by de subcontractors, if any, provided? (clause 3)
6. Is it mentioned that the subcontractors acted with the appropriate security measures? (clause 3)

Portability of information

7. Does the tenderer guarantee the portability of the data derived from the management of the outsourced service at all times? (clause 4)
8. Which data exchange format (s) will be used? (clause 4)
9. Are systems used to guarantee the integrity and authenticity of the information? (clause 4)
10. Is there a deadline for delivery by the tenderer? (clause 5)
11. Is there a validation period for the data delivered? (clause 6)

SECURITY OF INFORMATION

Location data

12. In which country are the servers, own or third parties, where the data and records derived from the management and their backup copies are managed and stored? (clause 7)
13. The location of the servers, own or third parties, where the data and records derived from the management and their backups are managed

and stored, will be within the European Economic Area? (clause 7)

14. Are international data transfers foreseen in the management of the service? (clause 9)
15. In the case of servers outside the European Economic Area, do you have the authorization of the Director of the AEPD? (clause 9)
16. Can a competent authority of a third country where the servers are settled, own or third parties, can request information about personal data? (clause 11)

Security measures

17. Does the tenderer and/or the subcontracted tenderer have a contingency plan in terms of security? (clause 14)
18. Is the contingency plan in terms of security attached? (clause 14)
19. Does the tenderer have qualified professionals with suitable levels of management and maturity in the services provided? (clause 15)
20. Does the tenderer and/or the subcontracted tenderer have the certification of the Certification Body of the National Scheme for the Evaluation and Certification of Information Technology Security or documentation in relation to the procedure? (according to Annex V, of the National Security Scheme (ENI))
21. Is it identified if there is treatment of special categories of personal data, according to article 9 of the General Data Protection Regulation (RGPD)?(clause 17)
22. Can subcontractors comply with the necessary measures in the storage and transmission of data in environments considered unsafe (laptops, personal assistants, peripheral devices, etc.)? (clause 18)
23. Will the necessary measures be met in the storage and transmission of data in environments considered unsafe (laptops, personal assistants, peripheral devices, etc.)? (clause 19)
24. Are there measures to guarantee the confidentiality of the information stored and in the transmissions? (encryption and / or fragmentation) (clause 20)
25. What methods of data encryption will be used? (clause 21)
26. Will the tenderer register the incidents, with the measures adopted and inform the City Council? (clause 22)
27. Does the tenderer and the subcontracted tenderer have a continuity plan for the activity? (clause 23)

- 28. Is the continuity plan for the activity of the tenderer and the subcontracted tenderers attached? (clause 24)
- 29. Will the tenderer submit to ordinary and extraordinary audits and inform who is doing them and based on what standards? (clause 29)
- 30. Will the Girona City Council have access to audits and access records of the data? (clause 26)

User management

- 31. Is there user management? If yes, continue. (clause 27)
- 32. Does the system have features that allow you to customize, for each user profile, its access and operational characteristics? (clause 27)
- 33. The functions of personalization of access, can it be managed by non-informatics personnel? (clause 27)
- 34. Will the system allow the definition of user profiles external to the Girona City Council, for specific purposes? (clause 27)
- 35. Does the system have password expiration systems? (clause 27)
- 36. Does the system have password format validation systems? (minimum length, symbols, rules) (clause 27)
- 37. Does the system deactivate a user before a certain number of failed access attempts in the authentication process? (clause 27)
- 38. Does the system have a history of movements, including unsuccessful access attempts that may have occurred? (clause 27)
- 39. Does the system allow the use of different digital certificates (at least those issued by the FNMT and AOC) and the electronic ID as part of the authentication process? (clause 27)
- 40. Does the system incorporate mechanisms that allow the electronic signature of the records generated in the same system? (clause 27)
- 41. Does the system have audit tools that facilitate the diagnosis and treatment of incidents? (clause 27)

CONFIDENTIALITY AND PROTECTION OF PERSONAL DATA

Commitment to confidentiality

- 42. Are you given information about the confidentiality instructions that govern your staff? (clause 29)

Responsibility in matters of personal data

43. Is it indicated that the Girona City Council is responsible for the file in the case it is? (clause 32)
44. Is it indicated that the tenderer is responsible for the file in the case it is? (clause 33)
45. Can subcontractors have the status of file manager and, if so, is it indicated? (clause 34)

Security measures

46. Does the tenderer inform that it complies with all the security measures established by law? (clause 36)
47. Is the service carried out in the tenant's premises and / or systems? clause 38)
48. If the service is carried out in the premises and / or systems of the tenderer, is the postal address or specific reference indicated so that the Town Hall can know all the details? (clause 39)

Collection of data and rights of of the people interested

49. Has it been specified that the informative text approved by the City of Girona will be used in the data collection forms? (clause 41)
50. Will the tenderer cooperate with the exercise of the rights of the persons concerned? (clause 42)
51. Will the tenderer correctly inform of the exercise of the rights of the persons concerned? (clause 43)
52. Will the tenderer manage the exercise of the rights of the interested persons? (clause 44)

Disposal of data

53. Will it be necessary to keep the data blocked once the service with the bidder is finished? (clause 45)
54. Is it reported that the bidder will have to certify the deletion of data? (clause 46)
55. Will the tenderer manage the exercise of the rights of the interested persons? (clause 47)

RECORDS AND DATA MANAGEMENT

Regulation and transparency

56. Does it comply with the basic requirements of record management systems, in accordance with Law 10/2001, Law 39/2015, the ENI and its

technical standards? (clause 48)

57. Does the tenderer prove compliance with the legislation on transparency and the right of access to information? (clause 49)

Corporate management

58. Does the service affect some of the transversal and corporate processes such as the processing of resolutions and agreements and the management of records of incoming and outgoing registry? If yes, continue (clause 50)

59. Has the structure, form, format and periodicity of integration been established? (clause 51)

60. Does the service allow to manage the corporate Business Classification Scheme? (clause 52)

61. Does the service allow the management and application of the Disposition Authority? (clause 52)

62. Does the service allow the management and application of the Transfer Schedule? (clause 52)

63. Does the service allow the management of the Access Regime of the records? (clause 52)

64. Does the service allow obtaining recapitulative records? (clause 52)

Characteristics of records and data

65. Does the tenderer prove that the records were created with the guarantees of legal validity specified by Law 39/2018? (clause 53)

66. Does the tenderer guarantee interoperability in relation to the recovery and preservation of digital records throughout their life cycle, through metadata? (clause 54)

67. Does the tenderer guarantee interoperability in the digital security policy and certificates? (clause 54)

68. Does the tenderer guarantee the long-term preservation of digital records in the formats that are set? (clause 54)

69. Can electronic copies be made? (clause 54)

70. Does the service offer partial or final indexation of the file and its closure, as well as the exchange format with the other Public Administrations? (clause 54)

71. Are the formats used for the creation and maintenance of digital records and data accepted in the ENI Standards Catalogue? (clause 54)

Preservation of the authenticity

72. Will the records preserve the information referred to your digital signature regardless of the type of signature? (clause 58)

73. Are the records received from third parties signed by qualified certified signature verified at the time of their capture and the signature verification information will be associated with the processing of the corresponding file? (clause 58)

74. Is there a verification system for signed records? (clause 58)

75. Will the records be kept in accordance with the single filing principle set by Law 39/2015, of the common administrative procedure (art. 17)? (clause 58)

76. Is there an integrity verification system before a transfer? (clause 59)

77. Is there a system for monitoring the integrity of records? (clause 60)

Product 3

Recommendations for the planning and the design of electronic services between Public Administrations

The purpose of these recommendations is to align the requirements of security and trust of e-services provided by public administrations with those required to external providers of similar services (Products 1 and 2). These recommendations are grouped into four sections:

- E-Service planning.
- Regulation of the e-service.
- Design and provision of the e-service.
- Presumption of the authenticity.

E-Service planning

1. Otherness: Identifying the characteristics and the organizational and technological context of the administrations potentially users of the service and how they will operate with the platform that provides the e-service.
2. Intermediation function: To assess the usefulness and potential of an intermediation platform to interconnect all the e-services for the public administrations and to facilitate the integration with their own systems.
3. Holistic approach: The description of functions and basic requirements of the e-service into a single Inter-Administrative Catalogue of e-Service for all public administrations, in order to simplify the identification of the service, the provider and the operating conditions.

Regulation of the e-service

4. General policies: The key elements for trust such as the requirements of security, confidentiality, data protection and preservation of the authenticity should be included in the general policies.
5. Regulatory granularity: If a single policy does not cover the entire institution, the e-services platforms or each e-service, it is necessary to regulate each level to build a complete trusted environment, from general policies to operational policies.
6. Statements of responsibility: If certain information cannot be included into a policy because it could cause a breach in the security of the system, the institution should publish some statement of responsibility regarding its policy of information security.
7. Terms and conditions (SLA): The requirements and conditions of provision of each e-service and the management of possible incidents that may arise, including its cancellation, have to be defined clearly and available for the public administrations as users.

8. Regulation of procedures: The accession agreement of the public administrations to an e-service has to be defined by a specific procedure as well as the registering or deregistering of persons authorized to use it.

Design and provision of the e-service

9. File transfer orientation: The communication e-services between public administrations should be based on direct file transfer through shared repositories and not on the sending records as in a framework of paper documents.
10. User control: The access to an e-service must be specific for each person and the public administration, as user, should be able to supervise easily all the authorized persons to use it through a module of users' registry.
11. Levels of access: Although several persons of a public administration may have access to the same e-service, it is necessary to foresee the possibility of establishing different levels of access according to the degree of confidentiality of the data and the different roles of authorized persons.

Presumption of the authenticity

12. Records creation: The *Requirements for Supporting the Presumption of Authenticity of Electronic Records (Requirements Set A)*, of the InterPARES project, should be used to assess the point of creation and capture of digital records from the presumption of authenticity viewpoint in any e-service.
13. Authentic copies: The e-services of inter-administrative consultation of records or data, or their verification, have always to provide authentic copies or evidence of what has been consulted with enough guarantees of authenticity and trust.
14. Traceability: All actions carried out by users have to be properly registered as audit trails and these ones have to be available to authorized users of the user public administration.
15. Open integration: The integration of e-services into the management systems of public administrations facilitates control of their records, reinforces the automation to prevent manual incorporation of records from one system to another one. Thus, the e-services should be easily integrated by design.

References

- AOC Consortium, *Acord marc d'interoperabilitat amb l'AOC [Interoperability Framework Agreement with the AOC Consortium]*. Retrieved from <https://www.aoc.cat/wp-content/uploads/2015/11/CONVENI-MARC-INTEROPERABILITAT.pdf?x75273>
- AOC Consortium, *Catàleg de tràmits [Catalogue of procedures]*. Retrieved from <https://www.aoc.cat/serveis/>
- AOC Consortium, *Condicions específiques de prestació del servei EACAT [Specific conditions for providing the EACAT]*. Retrieved from <https://www.aoc.cat/wp-content/uploads/2017/03/eacat-condicions-especificques-dels-serveis-aoc-vdef-maig-2015.pdf?x75273>
- AOC Consortium, *Condicions generals de prestació dels serveis [General conditions for the provision of services]*. Retrieved from https://www.aoc.cat/wp-content/uploads/2015/11/Condicions_generals_Serveis_AOC_23_06_2015.pdf?x75273
- AOC Consortium, *Política de Seguretat de l'AOC [Security Policy of AOC Consortium]*. Retrieved from <https://www.seu-e.cat/documents/31307/0/Pol%C3%ADtica+de+seguretat/8d21a64d-1268-4805-8049-c1b4a89475e3>
- AOC Consortium, *Protocol de gestió i ús del Catàleg de dades i documents interoperables a Catalunya [Protocol for the management and use of the Catalogue of interoperable data and documents in Catalonia]*. Retrieved from <https://www.aoc.cat/wp-content/uploads/2015/11/ptotocolGestioUsDadesDocumentsInteroperables.pdf>
- Bushey, J., Demoulin, M., How, E., McLelland, R. (2016). *Cloud Service Provider Contracts. Checklist*. NA14, InterPARES Trust. Retrieved from https://interparestrust.org/assets/public/dissemination/NA14_20160226_CloudServiceProviderContracts_Checklist_Final.pdf
- Bushey, J., Demoulin, M., How, E., McLelland, R. (2018). *Cloud Service Provider Contracts*. NA14, InterPARES Trust. Retrieved from https://interparestrust.org/assets/public/dissemination/NA14_final_report_v5-1.pdf
- Casellas, L.E. (2017). E-Services between Public Administrations and Records Management, from the Local Government viewpoint in Catalonia. In Anderson, K., Becker, C., Duranti, L., Rogers, C. (Ed.), *Born Digital in the Cloud: Challenges and Solutions. Presentations at the 21th Archival Sciences Colloquium of the Marburg Archives School* (pp. 213-230). Marburg (Germany): Marburg Archives School Book, Series, nº 65.
- Colom Planas, J.L. (2012). *Cláusulas contractuales en entornos de cloud computing*. In Aspectos profesionales: Protección de Datos, Cloud Computing y Sistemas de Gestión. Retrieved from <http://www.aspectosprofesionales.info/2012/10/clausulas-contractuales-en-entornos-de.html>

Hackett, Y. (2008). Domain 3 Task Force. Appendix 21: Preserver Guidelines – Preserving Digital Records: Guidelines for Organizations. In Duranti, L. and Preston, R. (Eds.), *International Research on Permanent Authentic Records in Electronic Systems (InterPARES) 2: Experiential, Interactive and Dynamic Records*. Padova (Italy): Associazione Nazionale Archivistica Italiana. Retrieved from http://www.interpares.org/ip2/display_file.cfm?doc=ip2_book_appendix_21.pdf

Spanish Data Protection Agency (2018). *Guía para clientes que contraten servicios de cloud computing [Guide for clients who contract cloud computing services]*. Retrieved from <https://www.aepd.es/sites/default/files/2019-12/guia-cloud-clientes.pdf>

Spanish Government. General Secretariat of Digital Administration of the Ministry of Territorial Policy and Civil Service (2016). *Catálogo de servicios de administración digital [Digital administration services catalogue]*. Retrieved from <https://administracionelectronica.gob.es>

Appendixes

Appendix 1. Policies first analysis: Electronic Services and Records Management.

- Service, Owner and Provider.
- Electronic services: short description.

Appendix 2. Policies second analysis: Electronic Services and Records Management.

Appendix 3. Authenticity of records: third analysis.

Appendix 4. Requirements.

- Supporting the presumption of authenticity of electronic records (Requirements Set A).
- Supporting the production of authentic copies of electronic records (Requirements Set B).
- Digital records maintenance and preservation strategies (Requirements Set C).

Appendix 5. City Council of Girona: Guidelines

Appendix 1

Policies first analysis: Electronic Services and Records Management

Electronic services ordered by its owner.

OWNER	E-SERVICE NAME	PROVIDER
CATALAN GOVERNMENT (15)	DASC – Degree of Disability	AOC Consortium
	eTauler – Electronic Bulletin Board and Edicts	AOC Consortium
	Official Bulletin of Catalonia	AOC Consortium
	RUDEL – Unified Data Record of Local Entities	AOC Consortium
	SINI@ – Chilhood and Adolescence Information System	AOC Consortium
	ANICOM – Pet Register	Catalan Gov.
	ATENPRO – Protection to Victims of Gender Violence	Catalan Gov.
	Certificates of Habitability	Catalan Gov.
	HERMES – Electronic Register of Self-Protection Plans	Catalan Gov.
	PIRMI – Integration Minimum Income (Inactive)	Catalan Gov.
	City Planning Projects	Catalan Gov.
	RCP – Public Contract Register	Catalan Gov.
	RSHP – Register of Official Protection Housing Applicants	Catalan Gov.
	SIFECAT – European Funds Systems of Catalonia	Catalan Gov.
	XMLS – Mediation Network for Social Rental	Catalan Gov.
SPANISH GOVERNMENT (8)	AEAT – Personal Income Tax Data	AOC Consortium
	DGT – Data Checking with the Traffic Authority	AOC Consortium
	Official State Bulletin (BOE) – TEU – Single Notice Board	AOC Consortium
	Official State Bulletin (BOE) (Inactive)	AOC Consortium
	ARCHIVE	Spanish Gov.
	BDNS – Public Register of Grants	Spanish Gov.
	InSide	Spanish Gov.
	TESTRA – Edictal Traffic Sanctions Board (Inactive)	Spanish Gov.
AOC CONSORTIUM (5)	DESA'L – Document Manager	AOC Consortium
	EACAT – Processing Between Administrations (+ SIR)	AOC Consortium
	eFACT – Electronic Invoice for the Administration	AOC Consortium
	eNOTUM – Electronic Notification	AOC Consortium
	iARXIU – Single Electronic Archive	AOC Consortium
PROVINCIAL GOVERNMENT (2)	Official Bulletin of the Province (BOPG)	Provincial Gov.
	SIMSAP – Municipal Information System on Public Health	Provincial Gov.
EUROPEAN UNION	TED – Tenders Electronic Daily	European Union

Total: 31

Electronic services ordered by its provider

PROVIDER	E-SERVICE NAME	OWNER
AOC CONSORTIUM (14)	DESA'L – Document Manager	AOC Consortium
	EACAT – Processing Between Administrations (+ SIR)	AOC Consortium
	eFACT – Electronic Invoice for the Administration	AOC Consortium
	eNOTUM – Electronic Notification	AOC Consortium
	iARXIU – Single Electronic Archive	AOC Consortium
	DASC – Degree of Disability	Catalan Gov.
	eTauler – Electronic Bulletin Board and Edicts	Catalan Gov.
	Official Bulletin of Catalonia	Catalan Gov.
	RUDEL – Unified Data Record of Local Entities	Catalan Gov.
	SINI@ – Childhood and Adolescence Information System	Catalan Gov.
	AEAT – Personal Income Tax Data	Spanish Gov.
	DGT – Data Checking with the Traffic Authority	Spanish Gov.
	Official State Bulletin (BOE) – TEU – Single Notice Board	Spanish Gov.
	Official State Bulletin (BOE) (Inactive)	Spanish Gov.
CATALAN GOVERNMENT (10)	ANICOM – Pet Register	Catalan Gov.
	Certificates of Habitability	Catalan Gov.
	HERMES – Electronic Register of Self-Protection Plans	Catalan Gov.
	PIRMI – Integration Minimum Income (Inactive)	Catalan Gov.
	City Planning Projects	Catalan Gov.
	RCP – Public Contract Register	Catalan Gov.
	RSHPO – Register of Official Protection Housing Applicants	Catalan Gov.
	SIFECAT – European Funds Systems of Catalonia	Catalan Gov.
	XMLS – Mediation Network for Social Rental	Catalan Gov.
	ATENPRO – Protection to Victims of Gender Violence	Spanish Gov.
SPANISH GOVERNMENT (4)	ARCHIVE	Spanish Gov.
	BDNS – Public Register of Grants	Spanish Gov.
	InSide	Spanish Gov.
	TESTRA – Edictal Traffic Sanctions Board (Inactive)	Spanish Gov.
PROVINCIAL GOV. (2)	Official Bulletin of the Province (BOPG)	Provincial Gov.
	SIMSAP – Municipal Information System on Public Health	Provincial Gov.
EUROPEAN UNION (1)	TED – Tenders Electronic Daily	European Union

Total: 31

Electronic services: short description

EUROPEAN UNION	41
TED – Tenders Electronic Daily	41
SPANISH GOVERNMENT	41
ARCHIVE	41
BDNS – Public Register of Grants	41
InSide	41
TESTRA – Edictal Traffic Sanctions Board (Inactive)	42
ATENPRO – Telephone Service of Attention and Protection to the Victims of Gender Violence	42
Official State Bulletin (Inactive)	42
Official State Bulletin (BOE) – TEU – Single Notice Board	42
AEAT – Personal Income Tax Data	42
DGT – Data checking with the Traffic Authority	42
CATALAN GOVERNMENT	43
ANICOM – Pet Register	43
Certificates of Habitability	43
HERMES – Electronic Register of Self-Protection Plans	43
PIRMI – Integration minimum income (Inactive)	43
RCP – Public Contract Register	43
RSHPO – Register of Official Protection Housing Applicants	44
City Planning Projects	44
SIFECAT – European Funds Systems of Catalonia	44
XMLS – Mediation Network for Social Rental	44
AOC CONSORTIUM - OPEN ADMINISTRATION CONSORTIUM OF CATALONIA.....	44
Official Bulletin of Catalonia	44
eTauler - Electronic Bulletin Board and Edicts	45
RUDEL – Unified Data Record of Local Entities	45
SINI@ – Information and Management System in Childhood and Adolescence	45
DASC – Degree of disability	45
eFACT – Electronic Invoice of Administration	45
DESA'L – Document Manager	46
eNOTUM – Electronic Notification	46
iARXIU - Single Electronic Archive	46
EACAT – Processing between Administrations (+SIR)	46
PROVINCIAL GOVERNMENT OF GIRONA.....	46
Official Bulletin of the Province (BOPG)	46
SIMSAP – Municipal Information System on Public Health	46

Creation	51
CATALAN GOVERNMENT – Self-developed – SINI@.....	51
AOC Consortium – EACAT – Generic submission	52
Transmission.....	53
AOC Consortium – EACAT – e-NOTUM	53
SPANISH GOVERNMENT – MINHAFP – BDNS	54
AOC Consortium – Publication in the DOGC	55
PROVINCIAL GOVERNMENT – Publication in the BOPG	56
AOC Consortium - Via Oberta - DASC – Disability grade	57
AOC Consortium - Via Oberta - AEAT – IRPF data	58

EUROPEAN UNION

TED – Tenders Electronic Daily

Description: System for publishing the Supplement to the Official Journal of the European Union dedicated to European public procurement. It serves to publish the data online, at European level, corresponding to the contracts carried out by the public administrations of the member states of the EU, the European Economic Area (EEA) and other countries.

Provider: European Union.

Starting date: 2015

More information: <https://data.europa.eu/euodp/es/data/dataset/ted-1>

SPANISH GOVERNMENT

ARCHIVE

Description: Application to the SARA network cloud, of definitive file of files and documents, based on the OAIS model.

Provider: Spanish Government.

More information: <https://archive.redsara.es/archive>

BDNS – Public Register of Grants

(Base de Datos Nacional de Subvenciones)

Description: Portal that publishes the subsidies of the Public Administration to comply with the provisions in the regulations regarding the information on the calls and resolutions of subsidies. At the same time, it also serves to publish the extracts corresponding to the official state newspaper (BOE) for information, control and transparency purposes.

Provider: General Intervention Board of the State Administration (IGAE) – Ministry of Finance – Spanish Government.

Starting date: 2016

More information: <http://www.infosubvenciones.es/>

InSide

Description: System for the management of electronic documents and records that meets the requirements so that both can be stored and / or obtained according to the ENI, scheme that establishes the basic rules for the exchange and storage of documents and electronic files. It supposes the electronic documentary management of the documents of the alive management of the file, like previous step to the definitive archiving of the documentation in an interoperable and lasting format.

Provider: Spanish Government.

TESTRA – Edictal Traffic Sanctions Board (Inactive)

(Tablón Edictal de Sanciones de Tráfico)

Description: System to publish notifications of fines that have not been practiced at home, in the Electronic Road Administration or by other electronic means

Provider: National Department of Traffic (DGT) – Ministry of Home Affairs – Spanish Government.

Starting date: 2010

More information: Order INT / 3022/2010, of November 23, which regulates the Edictal Board of Traffic Sanctions - https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-18102.

ATENPRO – Telephone Service of Attention and Protection to the Victims of Gender Violence

(Servicio Telefónico de Atención y Protección a las víctimas de la violencia de género)

Description: Mobile teleassistance service for victims of gender violence in the area of the couple. The service provider is the Red Cross, but access to the service (affiliation, termination, etc.) is made at the request of the SIAD-EIVG.

Provider: Ministry of Health – Spanish Government.

Starting date: 2006 (Ajuntament de Girona)

Official State Bulletin (Inactive)

(BOE: Boletín Oficial del Estado)

Description: Process in EACAT platform to publish resolutions of public entities in the Official State Gazette (BOE in Spanish).

Provider: Open Administration Consortium of Catalonia.

Starting date: 2015

Official State Bulletin (BOE) – TEU – Single Notice Board

(Tablón Edictal Único)

Description: Process in the EACAT platform to publish resolutions of public entities on the Single Edictal Board of the Official State Gazette (BOE) that could not be notified in person.

Provider: Open Administration Consortium of Catalonia.

Starting date: 2015.

AEAT – Personal Income Tax Data

(Dades de l'IRPF)

Description: Verification and / or consultation service for tax information and fiscal address obtaining a document signed electronically with the data consulted.

Owner: State Tax Administration Agency (AEAT).

Provider: Open Administration Consortium of Catalonia

DGT – Data checking with the Traffic Authority

(Comprovació de dades amb la Direcció General de Trànsit)

Description: Service of verification and / or consultation of the history of a vehicle obtaining a document signed electronically with the data consulted.

Owner: National Department of Traffic (DGT).

Provider: Open Administration Consortium of Catalonia

Starting date: 2013

CATALAN GOVERNMENT

ANICOM – Pet Register

(Registre General d'Animals de Companyia)

Description: Application for all the municipalities in Catalonia to take census of pet animals resident in their municipality (dogs, cats and ferrets). It replaces the municipal census that each city council maintained, in case this one does not want to manage the own census of animals.

Provider: Ministry of Agriculture, Livestock, Fisheries and Food.

Starting date: 2011 (starting the service)

Certificates of Habitability

Description: Service for the processing of first and second occupancy certificate certificates.

Provider: Catalan Housing Agency.

Starting date: 2017 (electronic processing)

HERMES – Electronic Register of Self-Protection Plans

Description: Telematic processing system and homologation of the self-protection plans, which, at the same time, houses the electronic Register of self-protection plans in Catalonia.

Provider: Ministry of Home Affairs (Catalan).

Starting date: 2012

More information:

http://interior.gencat.cat/ca/arees_dactuacio/proteccio_civil/paus_hermes/registre_hermes/

PIRMI – Integration minimum income (Inactive)

(Renda mínima d'inserció)

Description: It is the portal's procedure for the PIRMI social assistance process, where social workers sent the reports to request this assistance. It is no longer used since 2017 because this assistance changed.

Provider: Catalan Government.

Final date: 2017

RCP – Public Contract Register

(Registre Públic de Contractes)

Description: It is the platform for the public registration of contracts of the Catalan public administrations and allows the consultation of citizens, for information, control and transparency.

Provider: Ministry of the Vice-presidency and of the Economy and Finance.

Starting date: 2013

RSHPO – Register of Official Protection Housing Applicants

(Registre Públic de Sol·licitants d'Habitatges de Protecció Oficial)

Description: Service to register applicants for official protection of housing, in order to be able to participate in processes for the award of official protection homes. The purpose of this registry is to provide information on the real needs and the territorial distribution of officially protected housing, as well as facilitating and streamlining the processes of allocation and transmission of protected housing, guaranteeing maximum transparency of all processes.

Provider: Catalan Housing Agency.

Starting date: 2007 (establish by Law 18/2007)

City Planning Projects

Description: Module for submitting urban projects to the Territorial Planning Commission for review and approval.

Provider: Department of Territory and Sustainability.

SIFECAT – European Funds Systems of Catalonia

(Sistema de Fons Europeus de Catalunya)

Description: Information management system and procedural procedures in the European funding files of the European Regional Development Funds (ERDF), including the selection phases, justification of the cost and control of projects.

Provider: Department of Economics and Knowledge.

Starting date: 2015

XMLS – Mediation Network for Social Rental

(Xarxa de Mediació per al Lloguer Social)

Description: Service that incorporates the data of the owner and the characteristics of the apartments that are incorporated into a stock exchange of social rental apartments. At the same time, it is also a record of the applicants of apartments at moderate prices.

Provider: Catalan Housing Agency.

Starting date: 2014 (established in Decree 75/2014)

AOC CONSORTIUM - OPEN ADMINISTRATION CONSORTIUM OF CATALONIA

Official Bulletin of Catalonia

(DOGC: Diari Oficial de la Generalitat de Catalunya)

Description: Process in EACAT platform to publish resolutions of public entities in the Official Journal of the Catalan Government (DOGC).

Provider: Open Administration Consortium of Catalonia – Ministry of the Presidency

eTauler - Electronic Bulletin Board and Edicts

Description: Publication service of edicts offered by the AOC Consortium of the Catalan Government to the town councils. The functionality is the publication with guarantees of the municipal agreements in an electronic board and the download of evidences of publication.

Provider: Open Administration Consortium of Catalonia.

Starting date: 2015

RUDEL – Unified Data Record of Local Entities

Description: Register of data of the municipal services regulated and financed by the Contract Program between the Catalan Government and the City Council. These are forms are completed once a year justifying the annual agreement. The agreement has different files according to the different services or programs and RUDEL is organised the same.

Owner: Department of Labor, Social Affairs and Families.

Provider: Open Administration Consortium of Catalonia.

SINI@ – Information and Management System in Childhood and Adolescence (Sistema d'Informació i Gestió en Infància i Adolescència)

Description: Centralized information system with all the relevant antecedents of child abuse detected by any service, department or administration.

Provider: Directorate General of Child and Adolescent Care (DGAIA).

Starting date: 2014

DASC – Degree of disability (Grau de discapacitat)

Description: Verification and/or consultation service about the degree of disability obtaining a document signed electronically with the data consulted.

Owner: Department of Labor, Social Affairs and Families.

Provider: Open Administration Consortium of Catalonia.

eFACT – Electronic Invoice of Administration

Description: Electronic invoice service for the receipt of electronic invoices by its suppliers, achieving the benefits linked to billing procedures (cost savings, streamlining and homogenization of processes) and contributing to the promotion and dissemination of the use of the electronic invoice in Catalonia

Provider: Open Administration Consortium of Catalonia.

Starting date: 2009 (City Council of Girona)

DESA'L – Document Manager

Description: Digital repository service that allows the management of electronic documents and files during the processing period of these, while they remain open and until their closure, when they must be transferred to the final digital file

Provider: Open Administration Consortium of Catalonia.

eNOTUM – Electronic Notification

Description: Telematics notification service that allows citizens and companies to be notified with full legal guarantee.

Provider: Open Administration Consortium of Catalonia.

Starting date: 2012 (City Council of Girona).

iARXIU - Single Electronic Archive

Description: Preservation and electronic archiving service that guarantees that records / documents generated or received by an organization in the exercise of their functions remain complete, reliable, authentic and accessible throughout their life cycle.

Provider: Open Administration Consortium of Catalonia.

EACAT – Processing between Administrations (+SIR)

(Registres entre administracions)

Description: Service offered by the Open Administration Consortium of Catalonia to exchange communications between Administrations, interconnecting the records of entry and exit of documentation.

Provider: Open Administration Consortium of Catalonia.

Starting date: 2009 (only registry) and 2016 (full integration).

PROVINCIAL GOVERNMENT OF GIRONA

Official Bulletin of the Province (BOPG)

(Publicació al Butlletí Oficial de la Província (BOPG))

Description: Publication service of the Official Gazette of the Province where publish the Provincial Government of Girona, the city councils and the Administration of Justice of the Province. The objective is to disseminate its management, by means of announcements, acts, agreements, announcements, edicts and other resolutions, making it more transparent and allowing citizen participation.

Provider: Provincial Government of Girona.

Starting date: 2009

SIMSAP – Municipal Information System on Public Health

(Sistema d'Informació Municipal de Salut Pública)

Description: Portal of visualization of the data referring to the actions carried out by the Public Health Agency of the Provincial Government of Girona, from the planning of the actions to the results obtained. It allows extracting statistics and conclusions. The City of Girona requests services in the field of health to apply in the city. It is also an electronic processor of subsidy files.

Provider: Public Health Agency of the Provincial Government of Girona.

Starting date: 2009

Appendix 2

Policies second analysis: Electronic Services and Records Management

ACTION	e-SERVICE NAME	OWNER	PLATFORM
Creation	<i>Specific Submission Process</i>	Consortium AOC	EACAT (AOC)
	(5) SIMSAP	Provincial Gov.	Specific
	SINI@	Catalan Gov.	Specific
	ANICOM	Catalan Gov.	Specific
	City Planning Projects	Catalan Gov.	Specific
Transmission	<i>Generic Submission Process</i>	Consortium AOC	EACAT (AOC)
	(3) e-NOTUM	Consortium AOC	EACAT (AOC)
	e.FACT	Consortium AOC	EACAT (AOC)
Publication	e-TAULER	Consortium AOC	EACAT (AOC)
	(6) DOGC (PRE – EADOP)	Consortium AOC	EACAT (AOC)
	BOE (Submission of notifications)	Consortium AOC	EACAT (AOC)
	DOUE	European Union	Specific
	BDNS	Spanish Gov.	Specific
	BOPG	Provincial Gov.	Own
Verification	Via Oberta - DASC – Disability grade	Consortium AOC	EACAT (AOC)
	(2) Via Oberta - AEAT – IRPF data	Consortium AOC	EACAT (AOC)

Total: 16

Where is the record, where is the evidence?

	e-SERVICE	CITY COUNCIL	INTERMEDIARY PROVIDER	ADDRESSEE / PROVIDER	ACTION'S EVIDENCE
CREATION	<i>SÍNI@(- DMS -)</i>	(0)	-	X	NO
	<i>SPECIFIC APPLICATIONS</i>	(x')	X	X'	YES
TRANSMISSION	<i>GENERIC APPLICATIONS</i>	X	X'	X'	YES
	<i>CITY PLANNING PROJECTS</i>	X	-	X'	NO
PUBLICATION	<i>E-NOTICEBOARD</i>	X	X'	X'	YES
	<i>GRANTS' PUBLIC REGISTER</i>	X'	-	X	(NO)
	<i>OFF. BULL. of CATALONIA</i>	X'	-	X	(NO)
VERIFICATION	<i>DISABILITY DEGREE</i>	z'	-	Z	YES
	<i>PERSONAL INCOME TAX</i>	z'	-	Z	YES
	<i>VEHICLE OFF. REPORTS</i>	(0)	-	Z	NO

0 = No information

X = original Record

X' = Authorized copy

x' = Simple copy

Z = Original source

z' = Simple copy from the source

Appendix. 3

Authenticity of records: third analysis

ACTION	e-SERVICE NAME	OWNER	PLATFORM
Creation	<i>Specific Submission Process</i>	AOC Consortium	EACAT (AOC)
	SINIA	Catalan Gov.	Specific
Transmission	<i>Generic Submission Process</i>	AOC Consortium	EACAT (AOC)
	e-NOTUM *	AOC Consortium	EACAT (AOC)
Publication	DOGC (PRE - EADOP – Publication)	AOC Consortium	EACAT (AOC)
	BDNS	Spanish Gov.	Specific
	BOPG	Provincial Gov.	Own
Verification	Via Oberta - DASC – Disability grade	AOC Consortium	EACAT (AOC)
	Via Oberta - AEAT – IRPF data	AOC Consortium	EACAT (AOC)

Total: 8

* Discarded because it is aimed to citizens.

All the services provided for the EACAT (AOC) platform have the terms and conditions of:

- Interoperability Framework Agreement:
<https://www.aoc.cat/wp-content/uploads/2015/11/CONVENI-MARC-INTEROPERABILITAT.pdf?x75273>
- General conditions for the provision of services:
https://www.aoc.cat/wp-content/uploads/2015/11/Condicions_generals_Serveis_AOC_23_06_2015.pdf?x75273
- Specific conditions for providing the EACAT:
<https://www.aoc.cat/wp-content/uploads/2017/03/eacat-condicions-especificues-dels-serveis-aoc-vdef-maig-2015.pdf?x75273>

Creation

CATALAN GOVERNMENT – Self-developed – SINI@

Policies assessment (Checklist + Requirements Set C of InterPARES)	
Use / Accession procedure	Unknown
Agreement internal reference	Unknown
Specific terms	-
URL service	https://ovt.gencat.cat/gsitfc/AppJava/inicial.do?set-locale=ca_ES
User management	https://dps.gencat.cat/mcl/inici.do?apl=SIN
Other reference documents	Unknown

Authenticity assessment (Requirements Set A of InterPARES)	
A.1: Expression of Record Attributes and Linkage to Record	-
A.1.a.i Names of the people	-
• Name of the author	Unknown
• Name of the writer	Unknown
• Name of the originator	Unknown
• Name of the recipient	Unknown
A.1.a.ii Name of action or matter	Unknown
A.1.a.iii Date(s)	Unknown
• Chronological date	Unknown
• Date of receipt	Unknown
• Date of archiving	Unknown
• Date of transmission	Unknown
A.1.a.iv Expression of archival bond	Unknown
A.1.a.v Indication of attachments	Unknown
A.2 Access Privileges	Unknown
A.3: Protective procedures: Loss and corruption of Records	Unknown
A.4: Protective Procedures: Media and Technology	Unknown
A.5: Establishment of Documentary Forms	Unknown
A.6: Authentication of Records	Unknown
A.7: Identification of Authoritative Record	Unknown
A.8: Removal and Transfer of Relevant Documentation	Unknown

Authentic copies or evidences assessment (Requirements Set B of InterPARES)	
Authentic copy / Evidence	No

AOC Consortium – EACAT – Generic submission

Policies assessment (Checklist + Requirements Set C of InterPARES)	
Use / Accession procedure	General accession to EACAT platform
Agreement internal reference	-
Specific terms	No
URL service	https://ovt.gencat.cat/gsitfc/AppJava/inicial.do?set-locale=ca_ES
User management	There is an entity manager in EACAT (password or digital certificate).
Other reference documents	-

Authenticity assessment (Requirements Set A of InterPARES)	
A.1: Expression of Record Attributes and Linkage to Record	-
A.1.a.i Names of the people	-
• Name of the author	Yes
• Name of the writer	No
• Name of the originator	Yes
• Name of the recipient	Yes
A.1.a.ii Name of action or matter	Yes
A.1.a.iii Date(s)	-
• Chronological date	Yes
• Date of receipt	No
• Date of archiving	No
• Date of transmission	Yes
A.1.a.iv Expression of archival bond	Yes
A.1.a.v Indication of attachments	Yes
A.2 Access Privileges	Users management
A.3: Protective procedures: Loss and corruption of Records	Yes
A.4: Protective Procedures: Media and Technology	Yes
A.5: Establishment of Documentary Forms	Yes
A.6: Authentication of Records	Yes
A.7: Identification of Authoritative Record	There are no copies
A.8: Removal and Transfer of Relevant Documentation	Yes

Authentic copies or evidences assessment (Requirements Set B of InterPARES)	
Authentic copy / Evidence	Reference to the authentic copy in the electronic receipt.

Transmission

AOC Consortium – EACAT – e-NOTUM

Policies assessment (Checklist + Requirements Set C of InterPARES)	
Use / Accession procedure	Standard form.
Agreement internal reference	2009014320
Specific terms	Specific conditions for the provision of this service
URL service	https://ovt.gencat.cat/gsitfc/AppJava/inicial.do?set-locale=ca_ES
User management	There is an entity manager.
Other reference documents	-

Authenticity assessment (Requirements Set A of InterPARES)	
A.1: Expression of Record Attributes and Linkage to Record	
A.1.a.i Names of the people	-
• Name of the author	Yes
• Name of the writer	No
• Name of the originator	No
• Name of the recipient	Yes
A.1.a.ii Name of action or matter	Yes
A.1.a.iii Date(s)	-
• Chronological date	Yes
• Date of receipt	Yes
• Date of archiving	No
• Date of transmission	Yes
A.1.a.iv Expression of archival bond	Yes, in the attachment
A.1.a.v Indication of attachments	Yes
A.2 Access Privileges	Users management
A.3: Protective procedures: Loss and corruption of Records	Yes
A.4: Protective Procedures: Media and Technology	Yes
A.5: Establishment of Documentary Forms	Yes
A.6: Authentication of Records	Yes
A.7: Identification of Authoritative Record	There are no copies
A.8: Removal and Transfer of Relevant Documentation	Yes

Authentic copies or evidences assessment (Requirements Set B of InterPARES)	
Authentic copy / Evidence	Evidence record available for 2 years

SPANISH GOVERNMENT – MINHAFP – BDNS

Policies assessment (Checklist + Requirements Set C of InterPARES)	
Use / Accession procedure	No
Agreement internal reference	-
Specific terms	No
URL service	http://www.oficinavirtual.pap.minhAFP.gob.es
User management	Unknown
Other reference documents	http://www.oficinavirtual.pap.minhAFP.gob.es/sitios/oficinavirtual/es-ES/CatalogoSistemasInformacion/TESEOnet/Documents/Especificaciones_WS_Publicacion_Convocatorias.pdf

Authenticity assessment (Requirements Set A of InterPARES)	
A.1: Expression of Record Attributes and Linkage to Record	
A.1.a.i Names of the people	-
• Name of the author	
• Name of the writer	
• Name of the originator	
• Name of the recipient	
A.1.a.ii Name of action or matter	-
A.1.a.iii Date(s)	-
• Chronological date	
• Date of receipt	
• Date of archiving	
• Date of transmission	
A.1.a.iv Expression of archival bond	No
A.1.a.v Indication of attachments	No
A.2 Access Privileges	Yes
A.3: Protective procedures: Loss and corruption of Records	No
A.4: Protective Procedures: Media and Technology	No
A.5: Establishment of Documentary Forms	No
A.6: Authentication of Records	?
A.7: Identification of Authoritative Record	No
A.8: Removal and Transfer of Relevant Documentation	No

Authentic copies or evidences assessment (Requirements Set B of InterPARES)	
Authentic copy / Evidence	No

Publication

AOC Consortium – Publication in the DOGC

Policies assessment (Checklist + Requirements Set C of InterPARES)	
Use / Accession procedure	No
Agreement internal reference	-
Specific terms	No
URL service	https://ovt.gencat.cat/gsitfc/AppJava/inicial.do?set-locale=ca_ES
User management	There is an entity manager.
Other reference documents	http://dogc.gencat.cat/ca/pdogc_serveis/pdogc_serveis_de_publicacio_al_dogc Handbook: http://dogc.gencat.cat/web/.content/continguts/serveis/serveis_de_publicacio/documents/manual_usuari_publicacions_dogc.pdf

Authenticity assessment (Requirements Set A of InterPARES)	
A.1: Expression of Record Attributes and Linkage to Record	
A.1.a.i Names of the people	-
• Name of the author	Yes
• Name of the writer	No
• Name of the originator	No
• Name of the recipient	No
A.1.a.ii Name of action or matter	Yes
A.1.a.iii Date(s)	-
• Chronological date	Yes
• Date of receipt	No
• Date of archiving	No
• Date of transmission	No
A.1.a.iv Expression of archival bond	No
A.1.a.v Indication of attachments	No
A.2 Access Privileges	Users management
A.3: Protective procedures: Loss and corruption of Records	Yes
A.4: Protective Procedures: Media and Technology	Yes
A.5: Establishment of Documentary Forms	Yes
A.6: Authentication of Records	Yes
A.7: Identification of Authoritative Record	There are no copies
A.8: Removal and Transfer of Relevant Documentation	Yes

Authentic copies or evidences assessment (Requirements Set B of InterPARES)	
Authentic copy / Evidence	No

PROVINCIAL GOVERNMENT – Publication in the BOPG

Policies assessment (Checklist + Requirements Set C of InterPARES)	
Use / Accession procedure	No
Agreement internal reference	-
Specific terms	No
URL service	e-Office of Diputació de Girona.
User management	The user registers himself.
Other reference documents	http://ssl3.ddgi.org/BopPublicar/

Authenticity assessment (Requirements Set A of InterPARES)	
A.1: Expression of Record Attributes and Linkage to Record	
A.1.a.i Names of the people	-
• Name of the author	Yes
• Name of the writer	No
• Name of the originator	No
• Name of the recipient	Yes
A.1.a.ii Name of action or matter	Yes
A.1.a.iii Date(s)	-
• Chronological date	Yes
• Date of receipt	No (there is a digital signature from the platform)
• Date of archiving	No
• Date of transmission	No (= digital signature date)
A.1.a.iv Expression of archival bond	No
A.1.a.v Indication of attachments	No
A.2 Access Privileges	Yes
A.3: Protective procedures: Loss and corruption of Records	No
A.4: Protective Procedures: Media and Technology	No
A.5: Establishment of Documentary Forms	No
A.6: Authentication of Records	No
A.7: Identification of Authoritative Record	No
A.8: Removal and Transfer of Relevant Documentation	No

Authentic copies or evidences assessment (Requirements Set B of InterPARES)	
Authentic copy / Evidence	<p>Signed record of evidence.</p> <p>We reported that the digital signature was not valid and they solved it.</p> <p>The evidence does not include the content submitted.</p> <p>The reception not provide any identifier.</p>

Verification

AOC Consortium - Via Oberta - DASC – Disability grade

Policies assessment (Checklist + Requirements Set C of InterPARES)	
Use / Accession procedure	No
Agreement internal reference	-
Specific terms	No
URL service	https://ovt.gencat.cat/gsitfc/AppJava/inicial.do?set-locale=ca_ES
User management	There is an entity manager.
Other reference documents	-

Authenticity assessment (Requirements Set A of InterPARES)	
A.1: Expression of Record Attributes and Linkage to Record	
A.1.a.i Names of the people	-
• Name of the author	Yes
• Name of the writer	No
• Name of the originator	Yes
• Name of the recipient	Yes
A.1.a.ii Name of action or matter	Yes
A.1.a.iii Date(s)	-
• Chronological date	Yes
• Date of receipt	Yes
• Date of archiving	No
• Date of transmission	Yes
A.1.a.iv Expression of archival bond	Yes
A.1.a.v Indication of attachments	Yes
A.2 Access Privileges	Users management
A.3: Protective procedures: Loss and corruption of Records	Yes
A.4: Protective Procedures: Media and Technology	Yes
A.5: Establishment of Documentary Forms	Yes
A.6: Authentication of Records	Yes
A.7: Identification of Authoritative Record	There are no copies
A.8: Removal and Transfer of Relevant Documentation	Yes

Authentic copies or evidences assessment (Requirements Set B of InterPARES)	
Authentic copy / Evidence	Signed record of evidence

AOC Consortium - Via Oberta - AEAT – IRPF data

Policies assessment (Checklist + Requirements Set C of InterPARES)	
Use / Accession procedure	No
Agreement internal reference	No
Specific terms	No
URL service	https://ovt.gencat.cat/gsitfc/AppJava/inicial.do?set-locale=ca_ES
User management	There is an entity manager.
Other reference documents	-

Authenticity assessment (Requirements Set A of InterPARES)	
A.1: Expression of Record Attributes and Linkage to Record	
A.1.a.i Names of the people	-
• Name of the author	Yes
• Name of the writer	No
• Name of the originator	Yes
• Name of the recipient	Yes
A.1.a.ii Name of action or matter	Yes
A.1.a.iii Date(s)	-
• Chronological date	Yes
• Date of receipt	Yes
• Date of archiving	No
• Date of transmission	?
A.1.a.iv Expression of archival bond	No (there are not file number)
A.1.a.v Indication of attachments	Yes
A.2 Access Privileges	Users management
A.3: Protective procedures: Loss and corruption of Records	Yes
A.4: Protective Procedures: Media and Technology	Yes
A.5: Establishment of Documentary Forms	Yes
A.6: Authentication of Records	Yes
A.7: Identification of Authoritative Record	There are no copies
A.8: Removal and Transfer of Relevant Documentation	Yes

Authentic copies or evidences assessment (Requirements Set B of InterPARES)	
Authentic copy / Evidence	Signed record of evidence

E-SERVICES

REQUIREMENTS	CREATION		TRANSMISSION	PUBLICATION			VERIFICATION	
	<u>SiNI@</u> DMS -)	(- SPECIFIC APPLICATIONS	GENERIC APPLICATIONS	PUBLIC REG. OF GRANTS	OFF. BULL. OF CATALONIA	PROVINCIAL OFF. BULLETIN	DISABILITY DEGREE	PERSONAL INCOME TAX
FORMAL AGREEMENT (terms of use)	NO	YES	YES	NO	NO	NO	- YES -	- YES -
USERS CONTROL	Provider	Provider	Provider	???	Provider	User	Provider	Provider
PRESUMPTION AUTHENTICITY								
A.1.a Name of persons	NO	YES	YES	YES	YES	YES	YES	YES
A.1.a.ii Name of action or matter	NO	NO	NO	YES	YES	YES	YES	YES
A.1.a.iii Data(s)	NO	YES	YES	YES	YES	YES	YES	YES
A.1.a.iv Archival bond	NO	- YES -	- YES -	NO	NO	NO	YES	NO
A.1.a.v Indication of attachments	NO	YES	YES	/	/	/	/	/
A.1.b Integrity	NO	/	/	/	/	/	/	/
A.2 Access Privileges	YES	YES	YES	YES	YES	YES	YES	YES
A.3 Protection: loss and corruption	NO	YES	YES	NO	YES	???	???	???
A.4 Protection: media and technology	NO	YES	YES	NO	YES	???	???	???
A.5 Documentary forms	NO	YES	YES	YES	YES	YES	NO	NO
A.6 Authentication of records	NO	YES	YES	???	YES	YES	NO	NO
A.7 Id. of authoritative record	NO	- YES -	- YES -	NO	NO	NO	NO	NO
A.8 Removal and transfer	NO	YES	YES	NO	YES	???	YES	YES
	Catalan Gov.	<u>AOC</u>	<u>AOC</u>	Spanish Gov.	Catalan Gov.	Provincial Gov.	Catalan Gov.	Spanish Gov.

Appendix. 4. Requirements *

Supporting the presumption of authenticity of electronic records

Requirements Set A	YES	NO
A.1: Expression of records attributes and connection to the document		
A.1.a IDENTITY OF THE RECORD:		
A.1.a.i Names of the persons concurring in the formation of the record, that is:		
• Name of author		
• Name of writer		
• Name of originator		
• Name of addressee		
A.1.a.ii Name of action or matter		
A.1.a.iii Date (or dates) of creation and transmission, that is:		
• Chronological date		
• Received date		
• Archival date		
• Transmission date (or dates)		
A.1.a.iv Expression of archival bond		
A.1.a.v Indication of attachments		
A.1.b INTEGRITY OF THE RECORD		
A.1.b.i Name of handling office		
A.1.b.ii Name of office of primary responsibility		
A.1.b.iii Indication of types of annotations added to the record		
A.1.b.iv Indication of technical modifications		
A.2: Access privileges		
A.3: Protective procedures: loss and corruption of records		
A.4: Protective procedures: media and technology		
A.5: Establishment of documentary forms		
A.6: Authentication of records		
A.7: Identification of authoritative record		
A.8: Removal and transfer of relevant documentation		

Supporting the production of authentic copies of electronic records

Requirements Set B	YES	NO
B.1: Controls over records transfer, maintenance, and reproduction		
B.1.a Unbroken custody of the records is maintained		
B.1.b Security and control procedures are implemented and monitored		
B.1.c No alteration of the content, annotations, and documentary form		
B.2: Documentation of reproduction process and its effects		
B.2.a Date of reproduction and name of the responsible person		
B.2.b Relationship between the records acquired from the creator and the copies produced by the preserver		
B.2.c The impact of the reproduction process on their form, content, accessibility and use		
B.2.d Accessible documents about possible alterations		
B.3: Archival description		

Digital records maintenance and preservation strategies

Requirements Set C

Preservation	YES	NO
A. MAINTENANCE STRATEGIES		
A1. Clear allocation of responsibilities		
A2. Provision of the appropriate technical infrastructure		
A3. System maintenance, support and replacement		
A4. Transfer of data to new storage media on a regular basis		
A5. Appropriate conditions for storage media		
A6. Redundancy and geographic location		
A7. System security		
A8. Disaster planning		
B. PRESERVATION STRATEGIES		
B1. Use of standards		
B1.1. Self-describing formats (persistent object preservation, tagging)		
B1.2. Encapsulation		
B1.3. Restricting the range of formats to be managed (normalisation)		
B1.4. Conversion		
B2. Technology dependence		
B2.1. Technology preservation		
B2.2. Reliance on backward compatibility		
B2.3. Software re-engineering		
B2.4. Viewers and conversion at the point of access		
B2.5. Emulation		
B3. Non-digital approaches		
B4. Data restoration (digital archaeology)		

* **Extracted from:** Authenticity Task Force, "Appendix 2: Requirements for Assessing and Maintaining the Authenticity of Electronic Records." In *The Long-term Preservation of Authentic Electronic Records: Findings of the InterPARES Project*, Luciana Duranti, ed. (San Miniato, Italy: Archilab, 2005), 204-219. Available at http://www.interpares.org/book/interpares_book_k_app02.pdf.

Set C Requirements: *Appendix C. Digital Records Maintenance and Preservation Strategies*: Adapted from: Kevin Glick, "Electronic Records Preservation Strategies," (unpublished report, 2006)

Appendix. 5

City Council of Girona: Guidelines

Guidelines to ensure the presumption of the authenticity of records created out of the Records Management System

The creation of records on third-party platforms has not imply loss of control over the validity of these records. Therefore, it is necessary:

1. Download the record from the platform once signed and sent.
2. Set-aside a "second original" of the record before submitting it if the creation and signature of the record is done out of the transmission platform.
3. Incorporate always the document obtained in the RMS manually.

Record creation	Actions to do			
Inside the platform	e-Signature	Transmission	Download	Capture into RMS
Outside the platform	e-Signature	Set –aside a 2 nd original	Transmission	Capture into RMS

Guidelines to ensure the evidence of actions in the use of electronic services

1. Evidence is understood to be the record that incorporates:
 - Information about the action taken
 - The references of identification and validity of the record on which the action has been carried out.
 - The content or reference of the content of the original record.
2. Evidence must be obtained of all the actions taken on any third-party platform carried out as part of the business activities.
3. The type of action performed on third-party platforms can be:
 - Creation actions of records (may be associated with the transmission).
 - Transmission actions of records.
 - Publication actions of records.
 - Actions of verification or consultation of records.
4. Actions to be performed depending on the context:

Is there evidence?	Is it signed?	Actions to do		
Yes	Yes	Download	Capture into RMS	
Yes	No	Download	Authentication	Capture into RMS
No	-	Print Screen	Authentication	Capture into RMS

5. Evidence reinforced indirectly by the context:

Reinforced evidence	Key point	
Transmission	Continuity of processing	<p>The creation of new records derived from the transmitted record ensures that it was actually received.</p> <p>The capture of these derivative records within the RMS is essential, both for business activities and for the presumption of authenticity.</p>
Publication	Published record	<p>The capture into the RMS of the record published in the digital official journal and its identification reference (permanent link) guarantees that the action was completed.</p>
Verification / Consultation	Mirror effect	<p>In this case, the reinforced evidence is based on the trust on the service provided by the third party and the measures that it takes to preserve the presumption of authenticity.</p>