Some Aspects of GDPR Implementation in NAR

Bogdan-Florin POPOVICI, Ph.D.
National Archives of Romania, Brașov County Division, Brașov, str. G. Bariţiu nr. 34, 500025, Brașov, România
e-mail: bogdanpopovici@arhivelenationale.ro

Some Aspects of GDPR Implementation in NAR

ABSTRACT

While the implementation of GDPR raised concerns for archivists in Europe mainly from the perspective of the quality of archives and archival processing challenges, this paper focuses on administrative implication of collecting personal data during the services to the public performed by National Archives of Romania. First, they are identified the main processes where the protection of personal data may be involved, then discuss the challenges and propose some possible solutions. The conclusion is that, if implemented in a smart way, GDPR gives an opportunity for modernization of workflow and reduce of red tape in organizations.

Key words: GDPR, National Archives of Romania, services for public, data protection

Alcuni aspetti dell'applicazione del Regolamento generale sulla protezione dei dati nell'Archivio nazionale della Romania

SINTESI

Mentre l'applicazione del Regolamento generale sulla protezione dei dati ha sollevato preoccupazioni per gli archivisti in Europa principalmente dal punto di vista della qualità degli archivi e delle sfide della gestione archivistica, il presente articolo si concentra sulle implicazioni amministrative della raccolta di dati personali durante i servizi al pubblico eseguito dall'Archivio nazionale della Romania. In primo luogo, vengono identificati i principali processi dove la protezione dei dati personali può venir interessata, quindi si discute delle sfide e si propongono alcune possibili soluzioni. La conclusione è che, se attuato in modo intelligente, il Regolamento generale sulla protezione dei dati dà un'opportunità di modernizzazione del flusso di lavoro e di riduzione della burocrazia nelle organizzazioni.

Parole chiave: Regolamento generale sulla protezione dei dati, Archivio nazionale della Romania, servizi al pubblico, protezione dei dati

Nekateri aspekti implementacije GDPR v NAR

IZVLEČEK

Medtem ko je implementacija Spolšne uredbe EU o varstvu podatkov povzročila skrbi arhivistom v Evropi predvsem z vidika kakovosti arhivov in izzivov arhiviranja, se ta prispevek osredotoča na upravne posledice zbiranja osebnih podatkov med storitvami javnosti, ki jih izvajajo nacionalni arhivi Romunije. Najprej so identificirani glavni procesi v katerih je lahko vključena zaščita osebnih podatkov, nato pa sledi razprava o izzivih in nekaterih možnh rešitvah. Ugotovljeno je, da če se GDPR izvaja na pameten način, le to daje priložnost za posodobitev delovnega procesa in zmanjšanje birokracije v organizacijah.

Ključne besede: GDPR, Državni arhiv Romunije, javne storitve, varstvo podatkov

Câteva aspecte ale implementării RGPD în Arhivele Naționale

REZUMAT

Prezentul articol face o serie de considerații asupra modului de implementare a RGPD în instituția Arhivelor Naționale. Spre deosebire de majoritatea abordărilor, care se referă la modul de prelucrare al arhivei și la integritatea documentelor cu valoare arhivistică ce cuprind date personale, în material ne referim la documentele administrative (actele) Arhivelor Naționale, primite sau create în relație cu utilizatorii serviciilor și măsurile care se impun

a fi luate pentru conformitatea instituțională cu GDPR. Analiza este structurată pe servicii (relația cu creatorii și deținătorii, relația cu operatorii prestatori, serviciile de rezolvare cereri și sală de studiu). Deși la momentul redactării încă nu sunt implementate semnificativ măsuri de conformare, iar probleme ridicate nu au încă răspuns, considerăm că analiza ar trebui să fie parte a discuției, fiind fluxul ideal de adoptare a măsurilor (analiză atribuții ANR, analiză proces, analiză termen de păstrare și nevoia de culegere a datelor, analiză termen de păstrare, analiză soluții tehnice). Concluzia studiului este că, deși o sarcină semnificativă, implementarea RGPD poate fi o oportunitate de analiză birocratică și de raționalizare a exigențelor de întocmire și păstrare documente (acte).

Cuvinte-cheie: RGPD, protecția datelor personale, Arhivele Naționale, servicii pentru public

Introduction

The enforcement of GPDR starting from May 25th, 2018, generated a lot of emotions, within European Union and beyond. Despite the fact a buffer period of 2 years existed, there were not many organizations really interested in Regulation effects and its implementation. In my opinion, part of this disinterest explains the high emotions around the official enforcement of GPDR.

As far as the National Archives are concerned, we noticed that the debates focused mainly on the quality of records that may be affected by the (in)famous "right to be forgotten" and about the privileges such institutions have in processing (that is, acquiring, storing, archival processing) and in delivering access[1]. While these topics are undoubtedly relevant, in this paper we shall focus on some "administrative" aspects, regarding the way GPDR may affect the way some functions of National Archives of Romania should be exercised. We shall list the main functions of the institution and then identify the personal data that are captured and stored by performing the activities associated with these functions. For each case, we shall challenge the ground for collecting those data, if they are really necessary or they are legacy of old practices, but also the current retention periods associated with personal data collected.

It must be emphasized that, at the time of writing this material, no definitive answers were given to the issues presented further on, so the text should be considered as the author's interpretations and opinions and not the official position of National Archives of Romania. In the same time, we emphasize that so far, there is no article in Romanian professional literature concerning this topic.

Setting the framework

National Archives of Romania is, according to the law[2], the institution enabled with the administration, monitoring and special protection of National Archival Heritage of Romania. These broad goals are to be attained by controlling the whole lifecycle of records. In this regard, National Archives

- approve classification schemes and retention schedules for creators,
- confirm the records disposition of creating bodies,
- approve the appointment of records managers in the organizations,
- authorize the private recordkeeping operators,
- acquire, store, process of permanent records,
- deliver access to the records, either for readers or by releasing certified copies at the request of entitled persons.

In performing all these functions, records are generated and personal data are present, either as subject of processing or as part of procedures of various authorization. And, as I mentioned above, if the integrity of records and conditions for access of archival records were central to many debates, the other sets of data - collected as living organization - are often out of sight, despite it may pose more difficult questions than the personal data contained in historical archives.

1. See, for instance the draft of *EAG Guidelines on the enforcement of the EU General Data Protection Regulation 2016/679 in the archive sector*.

2. LAN, art. 5.

Supervising preservation and elimination of records

One spread trend among practitioners in creating bodies is to overestimate the need of certain categories of records. Mostly if one asks the "authors", they would like to keep everything forever, "just in case" (noting that *forever* here means 'as long as they are in charged with a specific matter'). GDPR though asks that personal data should be kept no longer than is necessary for the purposes for which they are processed[3]. This would of course contradict the practitioners interests and the exception of GDPR concerning the "archiving purposes in the public interest"[4] may fit very well with their interest. Therefore, it can be envisaged that assignation the permanent value[5] to some "very important" categories may occur. Since retention schedule are not just information records, but impose certain obligation further on, for creators and National Archives, I consider this as a risk to be mitigate and National Archives should pay special attention to this possible trend when aproving retention schedules.

Disposal of records will also have a new dimension. Until now, all disposals were approved regarding the set of records, as a whole. In contrast, the practice under GDPR may ask for disposal only for parts of records, containing personal data. Will this fall also under the authority of National Archives? Will this be a matter of disposition actions, that should be highlighted in the retention schedules? In my opinion, it would be nice to, but it may be difficult. Taking into consideration that classification scheme and retention schedule (which, in our practice, are one integrated tool) is supposed to be the real "X-ray" of the documentary production of an organization, here would be the perfect place to indicate if anonymization or pseudonymization actions should be carried out, when and on which data. This will also increase awareness of this tool within the organization and would lead to an integrated management of information. This is a strategic issue, that required a coordinated position of the National Archives and national data processing supervisor.

Approval of records managers appointment

According to the current law, when a (public) organization appoints a person as records managers, it should also ask for a professional approval from the National Archives. This process implies an examination of studies and training that the records manager graduated. The appointment is time-limited, since in rare cases a record manager will work in the same organization/same position for ever.

The casefile for approval contains a set of sensitive records, from the point of view of personal data: all the person's certificates of studies, records of name changes and so on. Until now, all these were assigned to the creator monitoring file and kept permanent. With the limitations introduced by GDPR, this approach may be problematic, considering the purpose for collecting those records. In our opinion, those records should be weeded out at latest when the person ceases the duty of records managers and the approval from National Archives also ceased or when the prescription period for a misdemeanor in approval activity intervened. On the other hand, the number and nature of the records required should be also examined, to check if it is not a case of excessive gathering of personal data.

Authorization of private recordkeeping operators[6]

Since 2013, legislation allows for private operators to be authorized for undertaken archival operation. Five services are subject to authorization: file binding, processing records, storage, restauration and use.

The procedure for authorization requests fulfilling certain requirements, including the existence of trained staff and various approvals from Commerce Register or Fire Inspectorate (for storage), but also the proof of existence and implementation of archival procedures of work. Due to the new regulations, in my opinion the internal procedure needs also to cover the issues of private data protection, due to the fact an authorized operator will have access to creator's records and, if authorization procedures is followed, they should be granted as trusted processors.

3. Article 5 e of GDPR.

4. Recital 18 of GDPR.

5. Due to different interpretation of term „permanent", maybe it is worth to mention that in Romanian archival legislation "permanent" is reserved for records of having archival/historical value.

6. Order..., passim.

During the process of authorization, National Archives acquires a lot of records containing personal data of the employees of the private operators. While these documents are necessary for the process, the question of the retention period may arise. Since authorization process should be renewed every 3 years, the retention period for records containing personal data should be somewhere around this period, also under the provisions of the prescription for misdemeanor in the activity of approval.

Use of records by the public

If other function of the National Archives of Romania deals with partners as organizations, the response to public requests, either for reading room or for releasing certified copies of relevant records implies a direct relation with the citizen as a person. It is here one of the main area where impact of GPDR can be identified.

a) public requests

According to the National Archives Law, citizens are entitled to receive at request certified copies of the records, if those records deals with matters regarding their rights. Based on this legal provision, a request does not only contain personal data for the identification of the demander, but also has attached a set of other records attesting personal rights in question. Moreover, people often attach to their request much more personal documents than required, on the principle "it may help". By reading those records, full of personal data, one can see sometimes the whole *cursus honorum* of one person or the whole genealogy of a family.

Retention period for citizens' requests is 10 years. The length may need to be reexamined, since it proved in many cases to be not justified by legal or other practical needs. The issue that is also worth reexamination is if the attached probative documents, the ones not really needed for the case, are also required to be retained for 10 years, since it may be considered as excessive collection of personal data. If such a resolution is taken, then the workflow needs to be reengineered, since a–criteria should be set for removing the unnecessary probative documents from the set and b–a special procedure for destruction of such documents needs to be implemented.

The finding aids for this kind of documentation used to be paper-based, consisting of incoming-outgoing register and name index. Since 2013, an electronic system (CRM) is in place. As a customer relationship manager, the system is built around the Person entity, associating it with the whole range of interactions that one Person has with National Archives. That is, in any moment now, one can see how many requests a person had, their status, all connected with personal data like name, address, national ID number and email address. The system also allows for users to open an account on National Archives portal for electronic services, for online requests and it is integrated with the archival management system, allowing also to submit application for reading room. System was designed for e-government purposes, to offer on line access, to reduce the need to re-identify the person and to allow access to all the Archives services in one authentication process.

Except for the reading room, the people need records from the Archives only when in some moments of their life: retirement, divorce, inheritance. That means that the interactions for asking certified copies may occur once or two times in their life. That implies our registration system may be filled up with personal data for persons that may use Archives services, but it is unlikely they have the need to do it. On the other hand, one can hardly anticipate the use of archival services.

Such considerations make difficult a real assessment of personal data sets need in the automatic system. If the records of the process of requesting are disposed after 10 years, the control tool should be also disposed, at the same time or soon afterwards or, at least, personal data should be removed. The problem is that integrated architecture of the system, and the user-centric architecture, make this almost impossible. Technically speaking, since the user is in the center of the system, removing names means removing a mandatory key of the database records, which will generate issues in correct functioning of the system. Removing nominative data by pseudonymization will lead to the unavailability of online services. It is here a case of concurrent use of the same set of basic nominative data and the retention period in this case should be the highest from all the possible uses. If this is the best legal answers, it is something yet to be determined.

b) reading room

To have access as a user of the reading room, a person must fill up a form delivering personal data as name, address, phone contact and email address. A reading card is normally valid for 2 years, followed, upon request, by its renewal. One issue here is concerned with the retention period of access forms. Currently the retention schedule states that access requests form are preserved for 5 years. It is noticeable this implies preservation of information for 3 years longer than the "contractual" period between the institution and the user, which may be considered excessive. In our opinion, except for the case when a legal issue it is expectable or exists, this retention period should be shortened to 3 years from the issuing of the reader card. But this may imply other complications, concerning the electronic system (that it will be addressed bellow).

While the collection of information for the reading card is clear and expectable, the further processes in the reading room is less expectable to record personal data, but they do. In this regard, there are several records containing personal data. First, the attendance register in the reading room: every user is indicating full name, the reader card's number, signature and date. Its main purpose for us is to keep track of users, to register the intensity of the work in the reading room, the frequency of users' return and so on. The main issue with this record is that it is literally an "open book", where any person can see the range of users before, associated with visit data and personal signature. For exemplification, we had two concerning experiences in this regard. First, it was a matter of public discussion if a famous researcher was more interested in the public archive of a private archive. Argument: he attended to the reading room of the public archive 3 months before his death, while the private archive was visited 1 month before... Another example: a researcher claimed at his office he would come to the Archives for research. One week later, his director, attending the reading room, noticed his employee was not recorded in the attendance register and this was a reason for further actions. Letting aside the pathetic topics, it is a fact that this information was taken from the attendance register and they were used by third parties in purposes different than the ones intended for collect. A resolution in this case was not yet achieved within the National Archives, but the possible solution envisaged: remove of this record and entrust the reading room archivist with the task of monitoring the attendance or remove the name as information to be collected and only let card's number, signature and visit date.

Another records collecting personal data in the reading room refers to the loan orders for records and copies requests. These records associate name of the researcher with all the orders in the reading room. The request slips are in general preserved for one year, then they are disposed. The requests and register for copies are kept for 3 years. The register for records order in the reading room, however, it is considered to have permanent value. This retention period is, in my opinion, rather questionable. In theory, having an image on long term on which fonds and which records were requested in certain periods may be relevant for the research trends for the institution (though in 20 years of my service I am not aware anybody used these kinds of data for such purposes...); but this not imply at all nominative data. Moreover, while in paper flow it would have been rather difficult for a reprocessing, once these records are currently dematerialized, profiling can be possible by exporting nominative data along with corresponding orders and, basically, leave no trace for this operation. Which implies that there is a possible action not clearly declared from the beginning and no proof for being done or not. A solution for this may be, of course, remove of nominative data after a certain period and only use management information; but here come the IT system constraints.

Our archival management (or information) system provides a module for recording "Partners" for the Archives, which are also organizations and persons. Persons are, in general, the users of the archives[7], and that module is connected with the module managing loan and copies order in the reading room. Technically speaking, User entity is mandatory for a loan or for an order. That is, not including this information in an order does now allow for the order to be saved. Also, once an order is closed, then any amendment to the record is not possible, by a regular user. If an administrator opens the record, then processing dates are changed and this influence the statistical information in Business Intelligence component. One possible solution is to anonymize the records by overwritten the name of the partner and its identification elements (address, for instance). In this case, though, all the functionalities of online ac-

7. Data here are, in general synchronized with the CRM mentioned above. Any change in CRM would impact the partners in ScopeArchiv.

count are lost and all the history of a user - assuming it is an active one - are also lost. Bottom line -with current technical functionalities it is not possible to manage in a satisfactory way the personal data in the reading room.

One last issue concerning personal data in the reading room process implies the circulation record: each item loaned has attached a form, where the user must fill the name, date of loan and purpose of using that item (research, copy etc.). The record is in fact a list, where the last user can see all the previous users. Is this a matter of privacy? In our opinion, yes. A mal-intended user took advantage of this information to claim that another researcher did not read that information, although it should have done it (but, in fact, it may have been a simple omission of recording the name). The issue is that the circulation record takes the "permanent" character of the file, so the question is if this personal data set is really of historical value or in fact its purpose expires already after 3 years, all along with other records of the usages of records in the reading room. One possible solution is to use circulation record only as an internal document, that is to keep it in the repository, as a slip record, where the name of the researcher to be noted by the assistant archivist. Another solution is to ask users to only note their reading card number, instead of their name. Another possibility may be offered by the IT system, since it records all usages, so all other records can be disposed. But, as it was explained above, the management of those electronic sets of personal data are also problematic.

Conclusions

At time of writing, the issues concerning the administrative implication of GPDR in National Archives of Romania are still under scrutiny. Up to now, notification forms for the purposes of collecting personal data have been prepared and implemented, but many other aspects are still to be checked and decided upon.

The experience so far showed implementation of GDPR, despite many issues, mostly at technical level, it is a great opportunity to re-examine and re-engineer, if the case, the workflows, the retention periods and even the red-tape habits already existed. A smart implementation of GDPR would require such actions, in my opinion.

In the same time, implementing GDPR in various organization is an opportunity for National Archives to promote records management provisions and good practice of information governance. It would be, again, a smart line of action, considering that traditional paper-based management approaches are challenged and best practices of managing information-as-records rather than paper-as-records should be acknowledged to all records creators.

Bibliography

GDPR *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)* (Text with EEA relevance) at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

LAN Legea Arhivelor Naționale [National Archives Law] at http://arhivelenationale.ro/site/wp-content/uploads/2017/07/LegeaArhivelorNationalenr_16din1996_republicata.pdf

Order *ORDIN nr. 137 din 27 septembrie 2013 pentru aprobarea Normelor metodologice privind aplicarea unor dispoziții ale Legii Arhivelor Naționale nr. 16/1996* [Order for approval of methodological standards about enforcing some provisions of National Archives Law] at http://legislatie.just.ro/Public/DetaliiDocument/151703

SUMMARY

This paper presents some considerations about the implementation of GDPR in National Archives of Romania (NAR). Unlike most of the approaches, which in general deals with the way historical records containing personal data will be processed and preserved, this paper focusses on records produced by the National Archives during the performance of its functions, records containing personal data and that must be aligned with GDPR provisions. The approach started with identifying the services performed by NAR (relation with creators of records, relation with records private operators, request for legal copies, reading room activities) and continues with examining the data collected, analyzing the grounds for collecting and retention periods associated with it. Although at the time of writing no compliance procedures are implemented, nor all the raised issues have answers, in author's opinion this analysis must be considered, as it might be the happy flow of implementing the proper measures: analyzing the functions of NAR, work process analysis, collecting data policy, retention periods ground, technical issues. Conclusions of the paper is that, although it is a rather hard administrative task, GDPR implementation may be a good opportunity of red-tape scrutineer and rethinking the way records are created and kept.

Typology: 1.01 Original scientific article

Submission date: 29.07.2018

Acceptance date: 08.08.2018