# The General Data Protection Regulation (GDPR, 2016/679/EE) and the (Big) personal data in cultural institutions: thoughts on the GDPR compliance process

Georgios Papaioannou[1] and Ioannis Sarakinos[2]

[1] University College London in Qatar
[2] Attorney at Law, Researcher / GDPR specialist, Greece
g.papaioannou@ucl.ac.uk

**Abstract.** This paper addresses GDPR in cultural heritage and memory institutions handling (Big) personal data. We discuss the compliance's necessity, common risk factors, needs to be taken into account, and we propose a GDPR process of phases and deliverables.

**Keywords:** GDPR, Heritage Data, Big Data.

## 1 Introduction

The introduction of the General Data Protection Regulation (GDPR) has been a reality since the 25 May 2018, introducing rigorous obligations and big challenges. It is a new regulation centralizing all existing regulations on data protection and updating them for the digital age. As one can see at the *2018 reform of EU data protection rules* [1], organizations that process EU residents' personally identifiable information (including visitors to the EU) must ensure compliance with the rules set out in the regulation and the rights of individuals are greatly enhanced. Cultural heritage and memory institutions as handlers of (Big) personal data have (or should have) taken provision towards compliance.

## 2 Background

### 2.1 What is Personal Data

Under the GDPR, personal data of a person include all data relating to a *living, natural person*. Specifically, personal data includes: "*Any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to physical, physiological, genetic, mental, economic,*

*cultural or social identity of that natural person"* (art. 4 of the GDPR). GDPR also introduces an updated category of data, the so called "*special category of personal data*" (art. 9 of the GDPR). It is an updated version of the previously, under Directive 95/46/EC, established category of "*sensitive personal data*", relating to personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, sex life and/or sexual orientation.

Cultural / memory organizations handle personal (Big) data, such as: name, identification number, address, telephone number, CV, social security number, genetic & biometric data, email address, employee or volunteer ID, login or physical access credentials, cookies, IP address, behavioral identifiers (e.g. geolocation), health data (e.g. disabilities, health records, treatments), opinions/preferences (e.g. political, cultural, religious, sexual and philosophical), criminal record, membership in cultural / memory organizations etc. Data relating to deceased people are regulated by national laws (GDPR Recitals 27, 158 & 160). Overall, data relating to employees, volunteers and/or visitors of a cultural / memory organization are all of GDPR interest. Processing relates to any operation or set of operations performed on personal data, whether or not by automated means (e.g. collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction). Processing for the purpose of the GDRP is everything from displaying to storing, both electronically and/or in physical form. Posting or displaying a photo of a natural person is also a processing activity.

### 2.2 The necessity to comply

Organizations in the area of cultural heritage and memory institutions are affected [2,3], since they hold and generate (Big) personal data in need of processing and GDPR compliance [4]. As such, cultural and memory institutions need to comply with GDPR's main objective, i.e. to ensure that personal data are collected, processed and transferred lawfully. There have been attempts towards some guidelines to this end. An example is that of Shone (2017) [5] for cultural organizations in the UK belonging to the Association of Independent Museums. Also, the Network of European Museum Organisations (NEMO) prepared an one-hour webinar [6, 7]. There are also training sessions [8] and services addressed to cultural sector [9].

## 3 The GDPR compliance process

### 3.1 Common risks factors and needs

Risk factors relate to (a) employees', visitors', volunteers', customers' and vendors' data collection, processing and storage processes, (b) personal data flows with third

parties (partners, outsourcers, etc.), (c) paper-based records, and (d) sensitive personal data (e.g. employees', members' and friends' health and financial data, etc.) handling.

Cultural and memory organizations need to review and update the following: (a) *Marketing & Fundraising* activities. Direct marketing can only be done if one of the six lawful bases under Art. 6 of the GDPR apply. These are *consent, contract, legal obligation, vital interests, public tasks*, and *legitimate interests*, with consent and legitimate interests being the most regular ones. (b) *Amend their Code of Ethics, Collection and Privacy policies-notices* in order to be GDPR compliant, especially in regards to the information towards living, natural persons (visitors, employees, vendors etc.). (c) *Maintenance and display of collections* must be done lawfully. This should mean that collections in display must fall under at least one of the aforementioned six lawful bases. If this type of activity may be considered as "filing system" under the GDPR, special provisions must apply. (d) *Keeping documentation of collections* in a safe, secure and well organized environment. The same applies to *personal data storage* of employees, volunteers, object creators and/or third parties, whether in physical or electronic form. (e) *Transferring of items and the personal data of their creators* observing GDPR. Except from the agreement signed, consent needs to be sought by the creators. (f) *Archiving* process should be subject to technical and organizational measures which are in place in order to ensure, in particular, the principle of data minimization. (g) *Profiling of donors* must be coupled with the right of donors to request from the institution to refrain from screening activities as a way of selecting them. (h) *CCTV & Voice recording*. *A*ppropriate notifications and documentations must be prepared and put in place for the lawful processing of data created through their use. (i) *Friends / Membership groups*. Museum and/or galleries tend to have membership and/or Friends groups, either as part of the institution or as separate entities. Individual consent to share and use personal data must be secured.

### 3.2 Phase-to-phase compliance guide and deliverables

The above must be achieved through a process called *GDPR compliance process*.

**Phase 1 –** Appointing a team of experts in the fields of legal, IT and Security, to perform the GDPR compliance process. Team's characteristics: knowledge on data laws, privacy laws, operations and specifics of cultural/memory organizations.

**Phase 2 –** Project setup and raising awareness within the cultural / memory organization (staff, employees and members of the board) on key GDPR aspects, requirements and needs. Deliverable: GDPR organization-specific education materials.

**Phase 3 –** Identification of personal data that the cultural / memory organization holds. This is usually done through a file called "Data Processing Activity Register" (art. 30 of the GDPR). Basically, the appointed team, assisted by each department of the cultural / memory organization ("Data Privacy Champions"), will review, identify and register what personal data each department holds, how, for how long, why etc. Deliverable: Data Processing Activity Register.

**Phase 4 –** Assessment of current GDPR compliance, i.e. assess current maturity levels against GDPR's requirements, understand risks, identify compliance gaps.

Deliverables: Assessment summary and the Data Privacy Impact Assessment report (DPIA). DPIA is necessary in high risk cases, e.g. use of CCTV cameras.

**Phase 5 –** Addressing identified gaps and proposing actions. Deliverable: Measured compliance steps, identified gaps and proposed remediation actions.

**Phase 6 –** Implementation. The appointment of a Data Protection Officer (DPO) is advised, fulfilling GDPR compliance tasks and sustainability on a service contract.

## 4 A concluding remark

GDPR presents a great opportunity for cultural institutions to revise and improve the ways they handle (Big) personal data and information, develop competitive advantage and, ultimately, contribute towards creating personal data protection culture for the community in general. It is an opportunity that should not be missed.

## References


1. 2018 reform of EU data protection rules (2018). Official website of the European Commission. Retrieved July 16, 2018, https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en, last accessed 2018/09/22.
2. White, B. (2018, May 24). General Data Protection Regulation 2018 – Ready? Set? Go?. Cultural Heritage Institutions Privacy Alliance (CHIPA). Retrieved July 17, 2018, from https://www.privacyalliance.co.uk/2018/03/24/general-data-protection-regulation-2018-ready-set-go/
3. MGS blog (2018, April 4). Don't Panic! 4 things to do now before GDPR [Blog post]. Museums Galleries Scotland Blog. Retrieved July 16, 2018, from http://www.mgsblog.org/connect/dont-panic-4-things-now-gdpr/
4. Zarsky, T.Z. (2017). Incompatible: The GDPR in the Age of Big Data, *Seaton Hall Law Review* 47, 995-1020.
5. Shone, H. (2017). *Success Guide. Successfully managing privacy and data regulations in small museums*, Ludlow: Association of Independent Museums (AIM). Retrieved July 16, 2018, from https://www.aim-museums.co.uk/wp-content/uploads/2017/10/SG-9.pdf
6. NEMO (2018, February 02). What Museums Need to Know to Comply with the New General Data Protection Regulation (GDPR), from https://www.ne-mo.org/news/article/nemo/what-museums-need-to-know-to-comply-with-the-new-general-data-protection-regulation-gdpr.html
7. M+H Advisor (2017, November 30). Advisor FREE Webinar GDPR – and what you need to know – The Resources, from https://advisor.museumsandheritage.com/news/advisor-webinar-general-data-protection-regulation-need-know/
8. Korn, N. (2018, May 22). Museums and their GDPR data protection obligations [Blog post]. Retrieved July 16, 2018, from https://naomikorn.com/2018/05/22/museums-and-their-gdpr-data-protection-obligations/
9. Sutton, M.M. & Ingram, H. (2018, January 11). *Data Protection and Art & Cultural Heritage*, Collyer Bristol Law Firm website. Retrieved July 16, 2018, from https://www.collyerbristow.com/item/2156-data-protection-and-art-cultural-heritage