# Initial Data protection impact assessment on blueprint architecture


| | |
|---|---|
| Publication Date | 2018-09-14 |
| Authors: | David Groep (Nikhef); Uros Stevanovic (Kit) |
| Contractual Date: | 31-08-2018 |
| Actual Date: | 29-03-2018 |
| Grant Agreement No.: | 730941 |
| Work Package: | WP3 |
| Task Item: | T2 Service-centric policies |
| Lead Partner: | AARC2 Collaboration |
| Document Code: | MNA3.7 |



The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).

**Abstract**

*The AARC Blueprint Architecture (BPA) introduces several concepts, such as the proxy and the community attribute management system, where personal data are processed. Going beyond direct interaction between the source of this personal information (identity provider, or the end-user) and the services that process such information, it adds new elements that are unique to the AARC BPA. The policy and best practice activity tracks the impact of the BPA on data protection and – in collaboration with the e-Infrastructures and experts from the NREN and REFEDS community - continuously provides guidance on appropriate measures to protect such data. Guidance to date includes the data protection impact assessment (DPIA) guidance for proxy operators (published as AARC-G042 and submitted as project deliverable DNA3.4) and a reference example based on the Life Sciences (LSAAI) pilot on how to achieve compliance with the GEANT Data Protection Code of Conduct version 2 (draft) which provides the current best understanding for protecting personal data for federated AAIs in the context of GDPR.*

# Table of Contents

# 1. Data Protection Impact Assessment guidance and the Blueprint Architecture

The AARC Blueprint Architecture (BPA) [1] comprises a set of technical elements as well as an interaction model on attribute aggregation and conveyance. Some of these attributes, such as the "REFEDS Research and Scholarship" category [2] set and the (community or infrastructure-assigned) omnidirectional identifier are personal data and as such in Europe subject to the General Data Protection Regulation GDPR [3]. The AARC2 project activity on policy and best practice harmonisation (WP3) has undertaken several activities to support communities and infrastructures in assessing the impact of the GDPR on the authentication and authorization infrastructure (AAI) components in the BPA:

- Guidance on the risk assessment needed to decide on the necessity of a Data Protection Impact Assessment for the infrastructure's AAI in the BPA (Guideline AARC-G042)
- Guidance on how an AAI service can implement adherence to the GEANT Data Protection Code of Conduct (DPCoCo) version 2 [4] (draft) which implement the requirements of GDPR as scoped to the federated identity management communities. This was done in the form of guidance for a specific community (the Life Sciences AAI) in order to demonstrate how abstract policy guidance can be concretely implemented in a BPA compliant AAI (Guideline AARC-G040).

Meanwhile, there is ongoing work on recommendations to the Infrastructures on how to both existing (AARC-1 DNA3.5 [5]) guidance on processing as well as the coherent presentation of privacy statements from a group of service providers (e.g. bound together through a set of Snctfi-based [6] policies) to the users in a way that does not require the users to repeatedly acknowledge the same kind of information.

## 1.1. Risk assessment for Data Protection Impact Assessments

In April 2018, the AARC2 project published the "Data Protection Impact Assessment - an initial guide for communities" as DNA3.4 (D3.1) – which was subsequently re-released as AARC Guideline G042 [7]:

This report presents the results of the desk study on the evaluation of risks to (personal) data protection as considered in the European General Data Protection Regulation (GDPR), for Infrastructures and their service providers that leverage federated identity management (FIM) to connect research and collaboration users. Specifically, it considers personal data collected as a result of using the infrastructure (not any risks relating to the research data itself, which is a community responsibility) and provides guidance to the Infrastructures concerning Data Protection Impact Assessment (DPIA) in the FIM context. The authors present recommendations to Research Communities for determining the necessity of formal DPIA and guidelines for its execution.

Based on the regulatory guidance available and the inherent safeguards built into the FIM model or service access, we show that significant aspects of GDPR compliance are already satisfied, specifically in data minimisation, reduction of the spread of personal data (and critical elements like credentials and passwords), and data security. Adherence to community best practices, limiting data to that based on REFEDS Research and Scholarship, and by implementation of the GEANT Data Protection Code of Conduct, Sirtfi, and the use of the Snctfi policy framework to ensure coherent behaviour of services 'behind' the BPA Community and Infrastructure Proxies, significantly mitigates any residual risk.

## 1.2. Preliminary Policy Recommendations for the LS AAI (application to R&S and CoCo)

The Life Sciences AAI Service (LS AAI), developed in joint collaboration with EGI, EUDAT and GÉANT, will result in a production-equivalent service to be operated for the Life Sciences community by the joint e-Infrastructures. As the pilot enters its second phase the LS AAI has to declare compliance to R&S and CoCo towards the R&E federations. This document provides preliminary guidance for the operators of the pilot LS AAI.

Section 3 of the Guideline [8] specifically deals with the data protection issues, and uses the Snctfi framework [6] as a basis for structuring data protection in the context of the BPA.

Since there are several different ways in which an BPA-compliant AAI can stricture itself organisationally (varying from a straightforward outsourcing of all AAAI functions to federated and collaborative models, or embedding the AAI as part of an existing consortium or project) guidance on the processor vs. controller role of the AAI provider (or providers) must always be specific. It is not the intention of the AARC BPA to prescribe a particular model in this case.

# 2. Summary

The AARC project provides guidance on personal data protection on an ongoing basis. In project month 16 a sufficient body of guidance is available to allow BPA AAI implementers to comply with the (draft) Data Protection Code of Conduct version 2 and to decide whether a data protection impact assessment (DPIA) as meant in the GDPR is required for their processing.

# References

[1] AARC collaboration, “AARC Blueprint Architecture 2017,” 2017. [Online]. Available: https://aarc-project.eu/guidelines/aarc-g012/. [Accessed September 2018].

[2] REFEDS, “Research and Scholarship Entity Category,” 8 September 2016. [Online]. Available: https://refeds.org/category/research-and-scholarship. [Accessed 2018].

[3] European Parliament and the Council of the European Union, “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,” *Official Journal of the European Union,* vol. 119, pp. 1-88, 2016.

[4] REFEDS, “Code of Conduct version 2.0 project,” REFEDS, 2014-2018. [Online]. Available: https://wiki.refeds.org/display/CODE/Code+of+Conduct+ver+2.0+project. [Accessed September 2018].

[5] AARC consortium, “AARC Template Policy for the Processing of Personal Data (DNA3.5),” December 2016. [Online]. Available: https://aarc-project.eu/wp-content/uploads/2016/12/AARC-DNA3.5_Recommendations-for-Processing-Personal-Data_2016_11_07_v4_DG.pdf. [Accessed September 2018].

[6] IGTF and the AARC consortium, “Scalable Negotiator for a Community Trust Framework in Federated Infrastructures,” April 2017. [Online]. Available: https://www.igtf.net/snctfi/. [Accessed September 2018].

[7] AARC Collaboration, “AARC-G042 Data Protection Impact Assessment – an initial guide for communities,” 30 April 2018. [Online]. Available: https://aarc-project.eu/guidelines/aarc-g042/. [Accessed September 2018 ].

[8] AARC Collaboration, “AARC-G040 Preliminary Policy Recommendations for the LS AAI (application to R&S and CoCo),” 1 March 2018. [Online]. Available: https://aarc-project.eu/guidelines/aarc-g040/. [Accessed September 2018].