DIVERSIFAIR

Quality and Data Management Plan

Co-funded by
the European Union

Document ID:	**D1.2**
Version date:	21/02/2025
Final version:	M36
Abstract:	The plan, following GDPR and other relevant regulations, will include protocols for the management of personal data during the demonstrations to be conducted, describe the entire data management lifecycle, which consists of data collection (including consent, anonymization, minimization, and other GDPR protected rights), storage, analysis, sharing and deletion. Each of the phases constitutes a vulnerable stage in the life cycle of data, which is why they will be individually addressed.
Keywords	Data management, Ethics compliance, Data protection

Disclaimer and acknowledgements

Co-funded by the European Union

This project has received funding from the European Education and Culture Executive Agency (EACEA) in the framework of Erasmus+, EU Solidarity Corps A.2 – Skills and Innovation under grant agreement 101107969.

Disclaimer

DIVERSIFAIR consortium

Authors

Name	Organisation	Role
Gemma Galdon	Eticas Research and Consulting	CEO
Luis Vizuet	Eticas Research and Consulting	Researcher

REVIEWERS

Name	Organisation	Role
Lizette Maljaars	TNO	Consortium manager

VERSION HISTORY

Version	Description	Date
0.1	1st complete draft	16/11/2023
0.2	1st complete draft peer review	24/11/2023
1	Complete draft with comments integrated	30/11/2023
1.1	Alignment of EU logo and disclaimer with GA	02/12/2024

Table of Contents

Executive summary

The deliverable D1.2 Quality and Data Management Plan sets out guidelines for data management during the DiversiFAIR project, including detailed research ethics guidelines included in the following drafts of the document. The Data Management Plan aims to lay down the main legal requirements concerning personal data, summarizing the primary data (including personal data) and identifying sensitive personal data processed by the project. It also seeks to lay down the basis of the consortium policy regarding data protection and security and establish the main measures to be carried out by the consortium to make data FAIR (Findable, Accessible, Interoperable and Reusable).

The Research Ethics Guidelines, develop in further drafts, will provide an overview of issues and guidelines related to conducting ethical research corresponding to the European Commission regulation. This section will also describe the ethics review processes and will give specific guidelines on the main project responsibilities

ETICAS has elaborated D1.5. It will be updated regularly, and the final version will be submitted before the final review (M36) to reflect the relevant changes undergone by the document.

1. Introduction

Diversify with Intersectionally FAIRer Artificial Intelligence (DiversiFAIR) is an EU-funded project addressing the topic ERASMUS-EDU-2022-PI-ALL-INNO-EDU-ENTERP. It began on the 1st of June 2023 and will finish on the 31st of May 2026. The project is strategically conceived to deliver innovative tools and structure them practically in two main knowledge hubs, containing user-friendly educational content in two main areas of fairer AI-Equality4Tech and Tech4Equality, accompanied by transversal use cases connecting across all project activities.

The Equality4Tech area encompasses two main products. First, sector-specific educational kits and Fair AI Scrum methodology for data scientists and AI practitioners. Secondly, non-tech stakeholders AI BIAS awareness training. Tech4Equality detects sectional and intersectional bias from a technological point of view. It develops a Recruitment scenario on intersectional bias mitigation and detection to experiment and bring practical knowledge to AI experts and tech-related professionals.

Each of the areas presented has the objective of boosting innovative ideas for bias detection, mitigation, and prevention in recruitment processes in novel and sustainable ways, adapting to the new challenges. Additionally, the work will enrich the EU-wide policymaking for a dedicated AI Governance Structure through a holistic AI Intersectional bias multidisciplinary program. Consequently, DiversiFAIR will build a deeper understanding of the harms and discriminatory impact of AI-facilitated outcomes on people's lives.

This previously described work will improve the digital skills and capacities of SMEs, educational institutions, and enforcement agencies, and increase their knowledge of intersectional bias and intersectionally fair AI equality standards through training and individual advisory support of the members of the consortium. Lastly, the project will consolidate cross-sectoral and cross-border partnerships among education, business, and research and innovation institutions, as well as labour market players.

The consortium is composed of 8 partners from 6 EU countries – academic/ research institutions create open-source reports, scientific articles, educational materials and lecture series on AI Intersectional fairness and Ethical auditing. VET partner consolidates and disseminates an eco-friendly, fully digitalized AI Intersectional bias educational program to beginner and seasoned AI professionals. The NGO partners craft and deliver AI Bias awareness training for social workers, HRs, policy-builders, and other non-tech stakeholders.

DiversiFAIR is divided into five Work Packages. This document is the second deliverable within Work Package 1 (project management and coordination) and is based on work carried out in Task 1.5 In the Grant Agreement, Task 1.5 is described as follows:

“Data management: Aims to guarantee legal & correct data management within project activities. A Data Management Plan (DMP) will be elaborated reflected in D1.2 with a preliminary plan submitted on M6 and a final version on M36 listing the final data governance

scheme used during the project. The plan, in accordance with GDPR and other relevant regulations, will include protocols for the management of personal data during the demonstrations to be conducted, describe the entire data management lifecycle, which consists of data collection (including consent, anonymization, minimization, and other GDPR protected rights), storage, analysis, sharing and deletion. Each of the phases constitutes a vulnerable stage in the life cycle of data, which is why they will be individually addressed."

D1.2 includes a Quality and Data Management Plan for DiversiFAIR, which lays out the requirements for protecting (personal) data that will be produced during the project lifespan, as well as the consortium's strategy to make data FAIR (Findable, openly Accessible, Interoperable and Reusable). To integrate by-design requirements and conduct validation activities, DiversiFAIR will potentially involve managing sensitive data belonging to protected groups associated with addressed technologies. All the measures that the consortium will put in place to maximise the transparency and accountability of any data generated throughout the project increase its impact and visibility. In this way, DiversiFAIR will also comply with the national and European Union legislation on data protection to be addressed as part of this deliverable. According to the Grant Agreement, this DMP will be updated in M36.

This document is PUBLIC and will be used by all members of the DiversiFAIR consortium.
It should be noted that other deliverables will tackle some of the above questions in more depth. Lastly, D1.2 include protocols for the management of personal data during the demonstrations to be conducted and describes the entire data management lifecycle, which consists of data collection (including consent, anonymization, minimization, and other GDPR protected rights), storage, analysis, sharing and deletion. Each of the phases constitutes a vulnerable stage in the life cycle of data, which is why they will be individually addressed.

2. DMP ground, legal framework and guidelines

D1.2 is elaborated according to the guidance given by the Commission regarding the content that should be included in a DMP. It also includes a succinct overview of the privacy and data protection legislation due to the central role they play in terms of the processing of personal data.

In regard to the level of comprehensiveness of this document, the consortium abides by the guidelines established by the European Commission on the issue:

“It is not required to provide detailed answers to all the questions in the first version of the DMP that need to be submitted by month 6 of the project. Rather, the DMP is intended to be a living document in which information can be made available on a finer level of granularity through updates as the implementation of the project progresses and when significant changes occur. Therefore, DMPs should have a clear version number and include a timetable for updates. As a minimum, the DMP should be updated in the context of the periodic evaluation/assessment of the project. If there are no other periodic reviews envisaged within the grant agreement, an update needs to be made in time for the final review at the latest.”

Along these lines, this document will be updated to incorporate the successive changes that may need to be reflected in it and the event of a review performed by the European Commission. These subsequent updates and plan adjustments will be reflected in the final version of this Deliverable (M36).

In terms of data protection and the impact of the research on fundamental rights and values, the relevant legislation listed below shall be considered:

1. The Charter of Fundamental Rights of the EU (2000/c 364/01);
2. General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679);
3. Convention No. 108 of the Council of Europe for the Protection of Individuals about
4. Automatic Processing of Personal Data adopted on 28 January 1997;
5. Recommendation No. R (97) 18 of Committee of Ministers to Member States concerning the protection of personal data collected and processed for statistical purposes, adopted on 30 September 1997;
6. Directive 96/9/EC of the European Parliament and the Council of 11 March 1996 on the legal protection of databases; and
7. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

Regarding the GDPR (“Regulation 2016/679 on the protection of natural persons about the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC”), it is a Regulation, which means that it enters into force in all Member States without the need for transposition. The main definitions and concepts contained within the regulation are briefed below:

- **Definition of data controllers and data processors**:

  Article 4 (7): "'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;"

  Article 4 (8): "'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."

Following the above, it is vital to distinguish the above figures as far as compliance with the GDPR is concerned, given that the data controller bears the bulk of the responsibility in terms of compliance. However, the processor is also responsible for assisting controllers in complying with the GDPR requirements.

- **Definition of personal data:**
  Article 4(1): "'personal data' means 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 to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

This deliverable reports on personal and non-personal data, as the questionnaire used for collecting information from partners, shown in the next section (WP1, WP2, and WP3). Additionally, from the key definitions of the GDPR, the DMP must cover the principles of the regulation.

The GDPR is structured around the following seven main principles, which must guide DiversiFAIR research development based on Article 5 (1) a: "personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')."

Processing data lawfully means that it must be processed based on some of the circumstances and following a specific legal basis established in Article 6 of GDPR (consent, performance of a contract, a legitimate interest, a vital interest, a legal requirement, and a public interest). In the case of DiversiFAIR, personal data will be processed based on informed consent in most already identified scenarios and listed in the section of the Data Management Plan.

According to the collection of personal data for specific, explicit and legitim purposes, based on:

"Article 5 (1)

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in

accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

DiversiFAIR partners, organizations and researchers must clearly state what this purpose(s) is, communicate this goal to data subjects when possible and only collect data for as long as is necessary to achieve that purpose. The personal data collected in the context of the project will be no more than the minimum required to achieve its purposes. This Deliverable will explain the criteria and measures in place to ensure that all the personal data that will be processed within DiversiFAIR will be relevant and limited to the purposes of the research project.

The partners must take every reasonable step to update or remove inaccurate or incomplete data. All data subjects whose personal data is managed by the project have the right to request that project partners erase or rectify without delay erroneous data that concerns them according to Articles 16 and 17 of GDPR. Additionally, according to subparagraph "e", the partners must delete personal data when they no longer need it and, under all circumstances.

Regarding the Data Protection Impact Assessment (DPIA), the GDPR Article 35 establishes the conditions under which a DPIA must be carried out:

"Article 35
1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar risks
[...]
3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

a) systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
c) systematic monitoring of a publicly accessible area on a large scale.2"

During the development of the project and if it is necessary, partners must consider the pseudonymisation and anonymisation of data. According to Article 26 of the GDPR, the principles of data protection do not apply to anonymous information. This is information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable, directly or indirectly. Therefore, the GDPR does not concern processing such anonymous information, including for statistical or research purposes.

Since GDPR does not apply to anonymous information, it is crucial to distinguish between anonymized and pseudonymized data. Pseudonymized data is data that can no longer be attributed to a specific data subject without the use of additional information (Art. 4 (5) GDPR). While anonymization processes ensure that no information about individuals can be recovered from a dataset, pseudonymization involves the replacement of a value, usually an identifier (an attribute that identifies the individual to whom it refers directly, for example, name), by another value to render it more challenging to re-identify. Following this principle, pseudonymizing personal data should ensure that additional information can be kept separately. It should also be subjected to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. Many authors have underlined the limitations of pseudonymization techniques in some contexts, as individual records can be re-identified due to various de-anonymization attacks (Lubarsky, 2017; Article 29 Working Party, 2014). This means that, under certain technical circumstances, data relying on pseudo-identifiers could be turned into identification data. Along these lines, Article 28 of the GDPR states the following:

"The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations. The explicit introduction of 'pseudonymisation' in this Regulation is not intended to preclude any other measures of data protection."

DiversiFAIR partners shall take all steps to pseudonymize and/or anonymize data when and if necessary. Specifically, personal data should be anonymized before dissemination outside the Consortium and/or before use for future research and/ or scientific purposes. This should be the generally applicable criteria unless the data subjects grant explicit and informed consent for disseminating certain types of personal data and the Consortium decides to allow its processing per the terms of the Grant Agreement. When it comes to pseudonymization, following Article 4(5) GDPR, pseudonymization should always be applied when it allows for achieving the purposes of data collection and is in line with the protocols or technological systems at hand.

2.1 Data management requirements

Data management is composed of the following five phases:

1. Data collection;
2. Data storage;
3. Data protection;
4. Data sharing/transfer; and
5. Data retention/destruction.

All those elements are addressed within the present DMP, which will be updated to include more information as soon as it is available or significant changes are made to the project. When going through the above data processing phases, there are three main legal principles and requirements that should be taken into consideration by partners regarding data management, given their importance:

- Article 30: “Record of processing activities”, according to which an accurate description of the processing activities shall be kept by the data controller and the data processor and, upon request, made available to supervisory authorities. This article also establishes the obligation to keep a record of processing activities. However, this obligation does not always apply. Article 5 establishes the situations in which the obligation of keeping records will apply.

- Article 32: “Security of processing”. This article aims to ensure that the data controller and the data processor process and keep the data security to avoid data being destroyed, lost, altered, disclosed or accessed accidentally or unlawfully. Therefore, the controller has an obligation to ensure that data is kept in a secure manner. The measures adopted to ensure compliance in this sense are included in Section 3 of this deliverable.

- Article 25: “Data protection by design and by default”, including procedures for pseudonymization and data minimization. This article establishes that, after performing a contextual analysis of the risks that the processing can cause, appropriate data protection measures must be put in place. This obligation has been partially fulfilled by means of the present deliverable, which takes stock of the personal data collected within the context of DiversiFAIR and the preventative measures adopted to mitigate the risks associated with their processing.

3. Data Management Plan

The table below provides a general view of the data that is going to be generated or used and provides information regarding its format and origin:

Table 1. Overview of the data that is going to be generated or used, its format and origin.

Data / Data source	Data format	Data origin							
		Consortium meetings	Interviews	Training	Demonstrations / Tests	Deliverables preparation	Literature review	Toolkit (app)	Partner
		All WPs	WP1, 2, 3 & 5	WP2 & 3	WP5	All WPs	All WPs	WP4	
Literature	Word (.doc/.docx) Pdf					X	X		ALL
References	Endnote database (.enl) Word (.doc/.docx)					X	X		ALL
Consent forms	Word (.doc/.docx) Pdf	X	X		X				NUID, ETICAS, TURING

Questionnaires	Word (.doc/.docx) Pdf		X	X			TURING
Images	TIFF, JPEG, PNG, JPEG/JFIF, GIF etc.	X		X			TURING
Audio files	WAVE, AIFF, MP3, MXF, FLAC etc.		X	X			TURING
Video files	MOV, MPEG-4, AVI, MXF etc.		X	X			TURING
Deliverables	Word (.doc/.docx) Excel (.xls/.xlsx) Pdf	X		X			ALL

Software	Several software languages			X			WOMEN IN AI
Software data	Database Management Systems			X			WOMEN IN AI
Contact details		X	X	X			ALL
List of individuals with special needs				X			WOMAN IN AI

The table puts together data that was collected from the different partners. Answers were received by the end of October 2023. Concerning types of data processed, Table 2 summarizes partners collecting personal data and their input regarding data storage security used in their management.

Table 2. Identifying personal data and applied storage security measures

Partner	Collecting personal &/or sensitive data?	Deliverable
Turing College	NO	Specialized course on preventing/mitigating intersectional bias
Turing College	NO	Results of all students who completed the course

According to the principle of data minimisation, personal data collected from individuals must always be limited to the minimum needed to accomplish the purpose of the processing. As it has been previously said, DiversiFAIR will implement policies and measures to ensure that the minimisation principle is properly executed. The following list lays out the files, including personal data that will be collected within the project and its relation to the project's objectives:

- Consent forms: They will be written in a way that guarantees the rights of research participants (Art 6 GDPR). They will include personal data such as name, date, place, and signature to ensure that research participants engage in data collection activities based on informed consent as defined in the GDPR.
- Non-disclosure agreements: These documents will identify a natural person representing an organisation that has decided to collaborate with the project, such as users and stakeholders.
- Questionnaires: They will be used to gather information from relevant stakeholders (end users, vulnerable individuals, and others) and members of the public (if it is necessary) to achieve the research objectives as part of various tasks.
- Images, audio and video files: Consortium members, in case to be required, will be based on informed consent. Research participants will have to agree to the possibility of the media taking pictures or recording video material, including them, to participate in the pilots or the project dissemination activities.
- Deliverables: They have been classified according to the nature of the information between Public and Sensitive based on the European Commission's guidelines (European Commission, 2016).
- Contact details: Name and surname of participants, e-mail address, name of company/organisation, or other information will be processed to manage the project research and dissemination activities in WP 5.

3.1 Data governance

The technical and organisational measures put in place by the consortium in order to safeguard the rights and freedoms of the data subjects and research participants. The DiversiFAIR consortium has decided to establish itself as a joint single controller using a joint controller's agreement (see Article 26 GDPR) to facilitate compliance with the principle of accountability, given that personal data will be shared between the different members of the consortium for research purposes. Moreover, the main users of personal data will be Turing College partner, who has been asked to appoint a Data Protection Officer (DPO). The DPO has the following responsibilities:

- To inform and advise the consortium partner's research team on their obligations under the Regulation (EU) 2016/679 General Data Protection Regulation (GDPR) and national law when personal data is gathered or processed during research activities; in particular, the DPO advises and supports the research team to fill in the Research Ethics Protocol;
- To monitor the consortium partner's research team compliance with EU and national data protection laws during project activities; and
- To function as the main consortium partner's contact point for project members and project management team, including National Data Protection Authority.

The DPO's primary role is to ensure that her organisation processes the personal data of its staff, customers, providers or any other individuals (also referred to as data subjects) in compliance with the applicable data protection rules. You should note that EU institutions and bodies are obliged to appoint a DPO following the Data Protection Regulation (Regulation (EU) 2018/1725).

Table 3. Identified Data Protection Officers (DPOs) and contact data

Project Partner	DPO name	DPO contact
Turing College	Benas Šidlauskas (specifically for the Turing College part of the project)	

The next table compiles the main security measures about the data and documents handled by the consortium that is more relevant from a data protection standpoint, especially those including sensitive personal information:

Table 4. Type of materials including personal data and standard security measures

Material	**Security measures**
Non-disclosure Agreements	Turing College: • We use Terms and Conditions and Privacy policy;

	● Tools: Metabase (for data visualization) ○ Security Measures: Regularly update documentation and associated data in Metabase. ○ Implement data erasure practices for outdated or unnecessary information.
Consent forms	Turing College: ● Tools: Typeform ○ Security Measures: Regularly update consent forms and associated data in Typeform. ● Define user roles within Typeform to limit access based on job responsibilities. ● Clearly outlining the purpose of data collection in the consent forms; ● Ensuring that consent is freely given, specific, informed, and unambiguous; ● Regularly reviewing and updating consent forms to reflect any changes in data processing activities;
Questionnaires	Turing College: ● Tools: Typeform, Satismeter, Salesforce ○ Security Measures: Regularly update questionnaires and associated data in Typeform, Satismeter, and Salesforce. ● Define user roles within each tool to control access based on job responsibilities. ● Limiting the collection of personal data to what is strictly necessary for the questionnaire (Privacy Policy) ● Use pseudonymization or anonymization techniques where applicable.
Contact details	Turing College: ● Tools: Salesforce, Metabase ○ Security Measures: Regularly update contact details and associated data in Salesforce and Metabase. ● Define user roles within Salesforce and Metabase to restrict access to authorized personnel. ● Implementing strict access controls to limit who can view and edit contact information. ● Regularly update contact databases to remove outdated or unnecessary information. ● Providing clear information on how individuals can update or request the deletion of their contact details.
Photos, videos and audio files	Turing College: ● Tools: VideoAsk, Zoom ○ Security Measures: Regularly update and review media files in VideoAsk and Zoom. ○ Define user roles within each tool to limit access to authorized personnel. ● Implement secure methods for storing and sharing media files.

f

4 Conclusion

This first draft version of D1.2 will be summited on M6 of the project, followed by a final version on M36. The ongoing communication necessary between Task leaders and the rest of the consortium members to find out about the relevant information concerning the different partners has been smooth and ongoing. In addition, the information collected about the types of data to be used in the research and its methods and forms of treatment will be of great use going forward. The In the following deliverable will be developed a Research Ethics section which will provide the project with a substantial foundation for framing all ethical issues concerning DiversiFAIR. Given the DMP is delivered in M6 allows the project to account for questions regarding data protection, security and research ethics from the beginning. This document will be updated in M36 to reflect the necessary changes before the final review.

References

1. European Commission. (2016, October 13). Template Horizon 2020 Data Management Plan (DMP).
2. All European Academies. (2017). The European Code of Conduct for Research Integrity. Berlin.
3. Article 29 Working Party. (2014, April 10). Opinion 05/2014 on Anonymisation Techniques.
4. Council of Europe, Committee of experts on internet intermediaries. (2017). Study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications.
5. European Commission. (2016). Guidelines for the classification of information in research projects.
6. European Commission. (2016). Guidelines on FAIR Data Management in Horizon 2020.
7. European Commission. (2016, October 13). Template Horizon 2020 Data Management Plan (DMP).
8. European Parliament (Committee on Civil Liberties). (2016). Report on fundamental rights implication of big data: privacy, data protection, non-discrimination, security and law enforcement.
9. Regulation (EU) No 1291/2013 of the European Parliament and of the Council of 11 December 2013 establishing Horizon 2020. (2013).
10. Lubarsky, B. (2017). Re-identification of "Anonymized Data". Georgetown Law Technology Review, 202(1), 202-212. https://perma.cc/86RR-JUFT.
11. Article 29 Data Protection Working Party. (2014). Opinion 05/2014 on Anonymisation Techniques. Retrieved from https://www.pdpjournals.com/docs/88197.pdf