A Risk Assessment and Legal Compliance Framework for Supporting Personal Data Sharing with Privacy Preservation for Scientific Research

Christos Baloukas
christosbaloukas@microlab.ntua.gr
National Technical University of Athens
Greece

Lazaros Papadopoulos
lpapadop@microlab.ntua.gr
National Technical University of Athens
Greece

Kostas Demestichas
cdemest@cn.ntua.gr
National Technical University of Athens
Greece

Axel Weissenfeld
axel.weissenfeld@ait.ac.at
AIT Austrian Institute of Technology
Austria

Sven Schlarb
sven.schlarb@ait.ac.at
AIT Austrian Institute of Technology
Austria

Mikel Aramburu
maramburu@vicomtech.org
Fundación Vicomtech, Basque Research and Technology Alliance (BRTA)
Spain

David Redó
dredo@vicomtech.org
Fundación Vicomtech, Basque Research and Technology Alliance (BRTA)
Spain

Jorge García
jgarciac@vicomtech.org
Fundación Vicomtech, Basque Research and Technology Alliance (BRTA)
Spain

Seán Gaines
sgaines@vicomtech.org
Fundación Vicomtech, Basque Research and Technology Alliance (BRTA)
Spain

Thomas Marquenie
thomas.marquenie@kuleuven.be
KU Leuven
Belgium

Ezgi Eren
ezgi.eren@kuleuven.be
KU Leuven
Belgium

Irmak Erdogan Peter
irmak.erdoganpeter@kuleuven.be
KU Leuven
Belgium

ABSTRACT

In order to perform cutting-edge research like AI model training, a large amount of data needs to be accessed. However, data providers are often reluctant to share their data with researchers as these might contain personal data and thereby sharing may introduce serious risks with significant personal, institutional or societal impacts. Apart from the need to control these risks, data providers must also comply with regulations like GDPR, which creates an additional overhead that makes data sharing even less appealing to data providers. Technologies like anonymization can play a critical role when sharing data that may contain personal information by offering privacy preservation measures like face or license plate anonymization. Therefore, we propose a framework to support data sharing of personal data for research by integrating anonymization, risk assessment and automatic licence agreement generation. The framework offers a practical and efficient solution for organisations seeking to enhance data-sharing practices without compromising information security.

KEYWORDS

Personal Data Sharing, Risk Assessment, Privacy Preservation, License Agreement

ACM Reference Format:
Christos Baloukas, Lazaros Papadopoulos, Kostas Demestichas, Axel Weissenfeld, Sven Schlarb, Mikel Aramburu, David Redó, Jorge García, Seán Gaines, Thomas Marquenie, Ezgi Eren, and Irmak Erdogan Peter. 2024. A Risk Assessment and Legal Compliance Framework for Supporting Personal Data Sharing with Privacy Preservation for Scientific Research. In *The 19th International Conference on Availability, Reliability and Security (ARES 2024), July 30–August 02, 2024, Vienna, Austria.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3664476.3670878

1 INTRODUCTION

Cutting edge research needs massive amounts of quality data. From studies to AI model training, a sufficient amount of data can ensure a successful research outcome. However, data providers like law enforcement agencies, hospitals, or other institutes are reluctant to share their data for fear of leaks that can lead to personal data exposure, ethical violations and other types of social unrest.

This work has been partially funded by EU Horizon Europe program under grant agreement No 101073951 LAGO (https://lago-europe.eu/).

ARES 2024, July 30–August 02, 2024, Vienna, Austria
© 2024 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-1718-5/24/07
https://doi.org/10.1145/3664476.3670878

Moreover, the European Union (EU) has established a number of legal frameworks that aim to safeguard individuals' fundamental rights in the context of various data processing activities while also facilitating the sharing and processing of data to enable innovation. Complying with all relevant legal frameworks before engaging in any sharing activity is imperative to avoid legal issues.

In summary, a safe data-sharing activity for an organisation comprises the following three key elements: (i) **Privacy preservation measures** that reduce or eliminate the amount of personal data present in the dataset. Personal data can be anonymized, and the dataset can still be useful for research. (ii) **Risk assessment** of all possible risks when sharing a specific dataset that covers three key areas, individuals, institutions and society, as some types of data can have a significant ethical and societal impact if leaked or misused. (iii) **A comprehensive legal agreement** that ensures compliance with all appropriate regulatory frameworks and reduces risks by enforcing the intended data use and legally binding the requester to prohibit other uses and activities not foreseen by the initial agreement.

Implementing those vital elements to participate in data-sharing activities requires time and expertise many organisations do not have. Therefore, they prefer to share data with a restricted set of partners or only under certain conditions or even abstain from data sharing altogether.

In this work, we present a risk assessment and legal compliance framework that provides a comprehensive, albeit easy-to-use, way for organisations to: (i) **assess and mitigate relevant risks** prior to sharing datasets that include personal data, taking into account several categories of risks (technological, people-related, institutional, legal, etc.) and potential impact not only to individuals but also institutions and society. (ii) **generate a license agreement** that ensures legal compliance with the relevant frameworks based on the dataset itself and its intended usage, while also taking into account the proposed mitigation actions to include the necessary clauses that reduce risks related to the license agreement (unintended use, distribution to third parties etc.). Figure 1 shows the proposed framework and its various steps.

The paper is organised as follows. Section 2 presents an overview of the related work, while section 3 examines the legal landscape that governs personal data sharing and processing. In section 4, we present the proposed framework in detail, while section 5 demonstrates the applicability of our approach in a realistic data sharing scenario. Finally, in section 6, we discuss key findings and extensions for the future.

2 RELATED WORK

2.1 Privacy preservation for data sharing

Each datatype (Tabular, Text, Image, etc.) containing personal data uses different anonymization techniques. In this work, we focus on techniques that anonymize and maintain the integrity and usability of the data so that the data can be used for further processing. For instance, **tabular** data can be anonymized by different techniques such as the ones presented in [17], [16] or [15]. **Image**-based privacy preservation techniques are centred on faces, mainly in synthetic generation by Generative AI [11] does not reveal original information or - GAN-based method as in [7], [14], [12].

Differentiating from other works, the anonymization module in our framework generates a set of statistics that can be used to evaluate the quality of the anonymization and therefore adjust the risk level for the anonymization part of the data sharing process, as displayed in the demonstration section (Section 5).

2.2 Risk assessment for data sharing

Evaluating the risks of personal data processing is the subject of many organisations. Notably, in Europe, the European Union Agency for Cybersecurity (ENISA) has developed a set of guidelines [3] that can guide organisations through a risk assessment methodology to evaluate the risk level of a particular processing operation. The handbook is accompanied by an online tool that implements the methodology [2].

Furthermore, French CNIL provides a set of documents (Privacy Impact Assessment methodology, knowledge base and case studies) aiming to assess the privacy risks of data processing when that processing is likely to result in a high risk to the rights and freedoms of natural persons. CNIL also offers a freely available tool [1] to carry out a PIA (Privacy Impact Assessment) and demonstrate how the organisation complies with GDPR.

Our proposed framework extends the available works by looking at risks beyond the individual, evaluating also the risks for the society and involved institutions, as explained in Section 4.2.

2.3 License agreement generation

Document assembly tools allow users to input information into a template [9], and the software generates a customized contract based on the provided data. This can save time and reduce errors compared to manual drafting. For instance, the approach of Higashi et al. [10] aims to automatically derive licensing rules from clustered license statements, with a specific emphasis on software license agreements rather than data license files.

Contract review and analysis methods can analyze contracts for potential risks, inconsistencies, or clauses that may need revision. These tools can help ensure that contracts comply with relevant laws and regulations. Some studies [6, 19] have introduced an automated solution aimed at verifying the compliance of a provided Data Processing Agreement (DPA) with the regulations outlined in the General Data Protection Regulation (GDPR).

Contrary to other works, our framework is built with interoperability in mind, so the license agreement generation tool takes into account the risks identified in the risk assessment step and provides the appropriate license agreement to mitigation those risks, as explained in Section 4.3.

3 LAWFUL BASIS AND LEGAL CONSIDERATION

The European Union (EU) has established robust legal frameworks with the double aim of protecting data subjects' privacy and data protection rights, while also enhancing the sharing and processing of data to enable innovation. Among these laws, primarily, the GDPR, the LED and the AI Act play pivotal roles in regulating personal data processing within the EU.

The GDPR applies to all entities, both public and private, that process personal data within the EU or concerning EU residents.

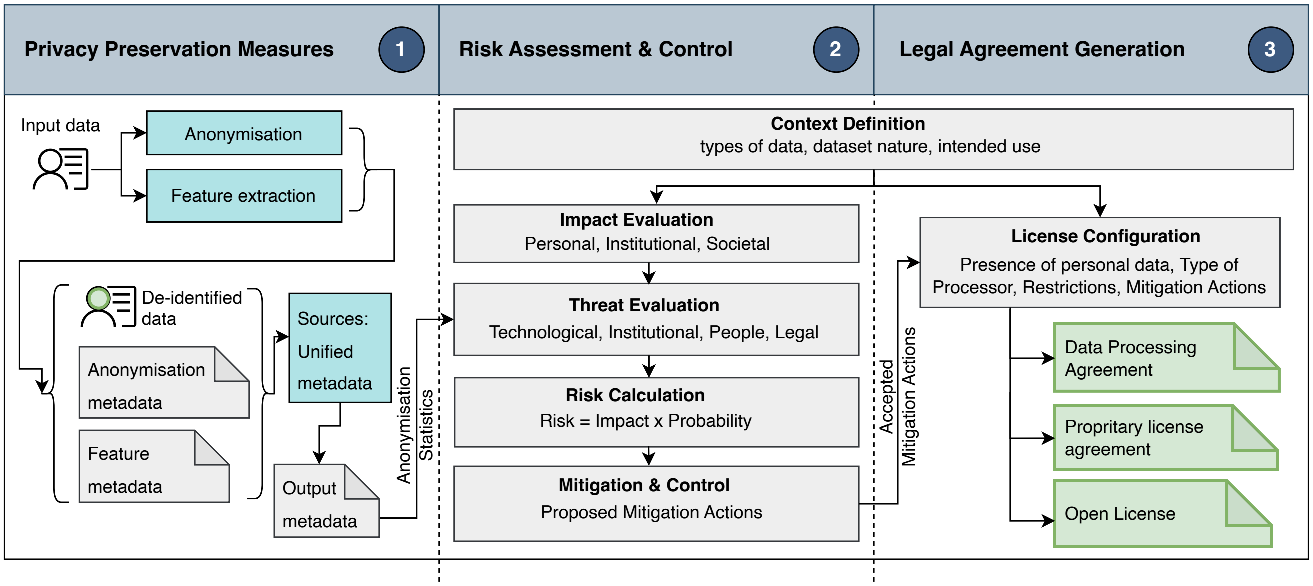

Privacy Preservation Measures
1
Risk Assessment & Control
2
Legal Agreement Generation
3
Input data
Anonymisation
Feature extraction
De-identified data
Anonymisation metadata
Feature metadata
Sources: Unified metadata
Output metadata
Anonymisation Statistics
Context Definition
types of data, dataset nature, intended use
Impact Evaluation
Personal, Institutional, Societal
Threat Evaluation
Technological, Institutional, People, Legal
Risk Calculation
Risk = Impact x Probability
Mitigation & Control
Proposed Mitigation Actions
Accepted Mitigation Actions
License Configuration
Presence of personal data, Type of Processor, Restrictions, Mitigation Actions
Data Processing Agreement
Propritary license agreement
Open License

Figure 1: The Proposed Risk Assessment and Legal Compliance Framework. It anonymizes personal data, generates a detailed risk evaluation report and the appropriate license agreement for a particular data sharing operation

The GDPR establishes data protection principles to be followed in all data processing activities (Article 5). It also differentiates between regular personal data and more "sensitive" data that may lead to discrimination and thus requires further protection (Article 9(1)). It is important to emphasize here that regardless of whether it is sensitive or not, all types of personal data can present a significant risk towards the rights and legitimate interests of individuals, depending on how the data is processed.

How our framework addresses this point: The risk assessment step treats "special" cases of personal data differently by assigning a higher score when such data are present in the dataset. Moreover, the legal agreement that is generated includes the necessary clauses to address handling these special data.

Additionally, the GDPR imposes strict obligations on data controllers and processors to ensure the security and integrity of personal data throughout its lifecycle. In case of non-compliance with all these stringent requirements, data controllers and processors face the risk of receiving significant administrative fines and other penalties.

How our framework addresses this point: The risk assessment takes into account the security environment of the data requester by checking for compliance with ISO27001 proposed security guidelines. This ensures data protection from cybersecurity threats but also the required data lifecycle. The legal agreement that is generated includes the necessary clauses to legally enforce this compliance.

Following the swift progress of AI technologies, the European Commission introduced the Artificial Intelligence Act in 2021, which is expected to be adopted in the first half of 2024 and enter full force by 2026. The AI Act aims to regulate AI systems' development, deployment, and use across various sectors, ensuring their transparency, accountability, and adherence to ethical principles. The AI Act classifies AI systems into four categories based on their risk levels: unacceptable risk (prohibited AI practices), high risk, limited risk, and minimal risk. For high-risk AI systems, the AI Act mandates compliance with a number of specific requirements, including data governance, risk management, technical documentation, transparency, and human oversight.

How our framework addresses this point: The risk assessment checks for the intended use of the dataset, and in case of an AI-related use, it presents the user with a set of requirements that must be covered in order to comply with the AI act. The generated license agreement also includes the necessary clauses to address compliance with AI-act.

The legal framework explained above presents a complex landscape for compliance, particularly for developers with limited time and resources. Compliance involves navigating multifaceted requirements spanning consent management, data protection principles, risk assessments, and accountability measures. Developers face the challenge of understanding and implementing these regulations effectively across various technological contexts, which demands substantial time, expertise, and resources. Failure to comply can result in significant legal consequences, emphasizing the importance of prioritizing regulatory compliance within development processes despite its inherent complexity and resource demands.

In light of the above, the risk assessment and legal compliance framework described in this work offers a simple, comprehensive solution which has the potential to provide significant relief to all parties involved in the research, development and deployment of AI-based technologies.

4 PROPOSED FRAMEWORK

The proposed framework (Figure 1) has been designed to meet the objective of a safe personal data sharing operation. Through rigorous literature review and interviews with law enforcement agencies (namely Hellenic Police, Swedish Police and Estonian Police) and security experts, we've identified several risk factors that contribute to the risk of a safe sharing operation as shown in Table 1. Each of these risk factors is mitigated at the appropriate step of the proposed framework. In the rest of the section, we look at each of the steps of the proposed methodology of Figure 1.

4.1 Step 1: Privacy Preservation Measures

The anonymization pipeline used in our approach is based on [18], and it consists of four steps:

Identification of personal data. The first step concerns identifying personal data within the whole data or dataset. The objective is to detect where personal information must be protected or, in this case, anonymized so the dataset can be exempt from complying with the GDPR.

Synthetic data creation. This step, parallel to the first one, centres on creating the synthetic data that will replace the personal data.

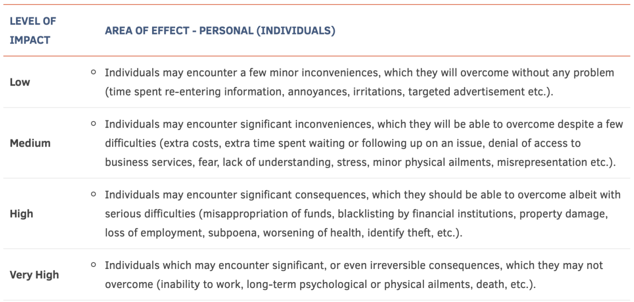
Style transfer. The style transfer process adapts the synthetic data to mirror the personal data's statistics, appearance, features or characteristics (depending on the data type). This step seeks to modify the newly generated synthetic data to resemble the original personal data. This can be done by applying GANs (Generative Adversarial Networks) to transfer the style of an image or by using limits or Gaussian distributions to numeric data. The idea is to take advantage of the detected personal data and modify the features or characteristics of the created synthetic data to resemble the original.

Anonymity by De-identification. The last step is to apply the de-identification process to substitute the personal data with new synthetic data. While covering or replacing the personal data, the other non-personal data is kept as it is in the original. This helps to maintain the data's integrity and does not affect the surrounding data, keeping it as original as possible. This way, it ensures future data utility.

While automatic, the anonymization process could be imperfect and lead to personal data exposure. To understand the risk of a data-sharing operation, the data provider must be aware of the success of the anonymization step. Therefore, we evaluate the anonymization quality based on metrics available from the anonymization module. The risk assessment module will use the calculated anonymization quality to produce a risk level for the anonymization risk factor. The exact method depends on the data type. In this work, we will present our approach for the anonymization of license plates (see Section 5), which can also be extended to other data types.

4.2 Step 2: Risk Assessment & Control

Sharing personal data can introduce the data provider to a range of risks, from legal fines to irreparable damage to the institution's reputation and continuity of operations, if these data are somehow leaked or inappropriately used. Equally important, however, is the impact on individuals and society from personal data exposure, biased research, inappropriate or misconfigured AI models, etc. DPIA and the recent AI act highlight this need, as discussed in detail in Section 3. Therefore, it is imperative to evaluate a sharing operation not only from a security perspective but also from other aspects like ethical, societal and legal aspects.



LEVEL OF IMPACT	AREA OF EFFECT - PERSONAL (INDIVIDUALS)
Low	○ Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, targeted advertisement etc.).
Medium	○ Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, extra time spent waiting or following up on an issue, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, misrepresentation etc.).
High	○ Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, identify theft, etc.).
Very High	○ Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

Figure 2: Impact table for individuals

In essence, there are four major concerns when sharing personal data: **(i) unauthorized access** to the dataset that can lead to many consequences, from legal fines to serious consequences for the organization, **(ii) personal data exposure**, which can lead to legal compliance issues and inconveniences for the individuals, **(iii) bias in research and trained models**, if the quality of the original data is not checked, **(iv) legal compliance** with the appropriate legal frameworks.

Such a risk assessment approach can only be qualitative as it depends on the actual data itself and the particulars of the sharing agreement. The particular steps of the proposed risk assessment methodology are described below[1]:

Context Definition. In this section, the users enter information about the dataset to be shared, in particular, the types of data contained in the dataset (license plates, faces, credit card info, addresses, etc.), the intended use (research, AI training, etc.) and information about the requester (organization, research institute, law enforcement agency (LEA), etc).

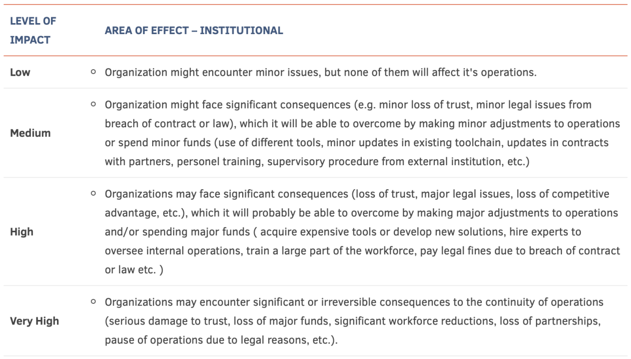
Impact Evaluation. The data provider is asked to reflect on the impact that this sharing operation could have in the case of unauthorised access, bias in the dataset, personal data exposure or lack of legal compliance. Through extensive analysis of the landscape and interviews with Law Enforcement Agencies, we defined several impact levels in different areas of effect (personal, institutional, societal) that can help the user assess the impact of the operation. Special care has been given to the language and presentation of the impacts, with several examples that help guide the user in selecting the correct level for their particular case. Figures 2, 3 and 4 present the various impact levels.

Threat Analysis. At this step, the data provider is asked a few questions regarding the potential threats that may lead to unauthorised access, a biased dataset, personal data exposure or a lack of legal compliance. Each question is accompanied by an explanation and several examples to make sure that the user answers correctly, as can be seen in Figure 5. The set of threats has been derived from the risk register presented in Table 1. To facilitate the evaluation from the user about the probability of each threat materialising, we divided the threats into four categories: **(i) Technological threats**,

[1] the proposed methodology is implemented as a web-based online risk assessment tool, available online at: https://lago.microlab.ntua.gr

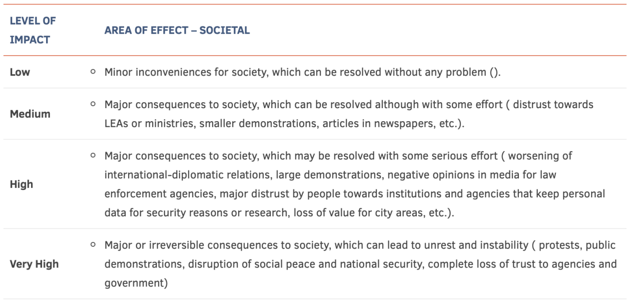
Table 1: The risk factors (*RF*) for a safe data sharing operation. Risks are categorized by type in data, technical & organizational measures to ensure data security, license agreement and application domain. The identified risks are mitigated by either the anonymization tool (AT) or the license generation tool (LT).

#	Short Description	Mitigation Actions (examples)
1	Data contains personal information.	Anonymize data, if applicable. [AT]
2	Anonymisation not 100% successful.	Provide statistics about anonymization success. [AT]
3	Categorization of personal data (e.g. health data).	Describe type of data. [LT]
4	Data provider obliges confidentiality.	Confidentially clause. [LT]
5	Data transfer method lacks state-of-the-art (SOTA) security measures.	Oblige requester to use SOTA technologies. [LT]
6	Lack of data access protection at the requester premises.	Oblige requester to use SOTA technologies. [LT]
7	Employees handling the data lack sufficient training.	Involve DPO or refer to ISO standard for training employees. [LT]
8	Cybersecurity measures at the premises of the data requester lacks SOTA security measures.	Oblige requester to use SOTA technologies. [LT]
9	No data lifecycle control at the requester.	Oblige requester to be certified e.g. ISO 27001. [LT]
10	No license agreement between the data provider and requester.	Create a valid license. [LT]
11	License agreement not restricting data distribution.	Restrict distribution of data. [LT]
12	License agreement not compliant with GDPR if data contains personal information.	Ensure GDPR compliance. [LT]
13	Biased data.	Add disclaimer & oblige data requester to report any identified bias. [LT]
14	Data is used to create AI models as defined by the AI-act.	Limit the data usage & exclude certain risk groups. [LT]
15	Data can be used for arbitrary purposes.	Limit the data usage to specific purpose/ domain. [LT]
16	License agreement not compliant with AI-Act.	Ensure compliance to AI-Act. [LT]



LEVEL OF IMPACT	AREA OF EFFECT – INSTITUTIONAL
Low	○ Organization might encounter minor issues, but none of them will affect it's operations.
Medium	○ Organization might face significant consequences (e.g. minor loss of trust, minor legal issues from breach of contract or law), which it will be able to overcome by making minor adjustments to operations or spend minor funds (use of different tools, minor updates in existing toolchain, updates in contracts with partners, personel training, supervisory procedure from external institution, etc.)
High	○ Organizations may face significant consequences (loss of trust, major legal issues, loss of competitive advantage, etc.), which it will probably be able to overcome by making major adjustments to operations and/or spending major funds (acquire expensive tools or develop new solutions, hire experts to oversee internal operations, train a large part of the workforce, pay legal fines due to breach of contract or law etc.)
Very High	○ Organizations may encounter significant or irreversible consequences to the continuity of operations (serious damage to trust, loss of major funds, significant workforce reductions, loss of partnerships, pause of operations due to legal reasons, etc.).

Figure 3: Impact table for institutions



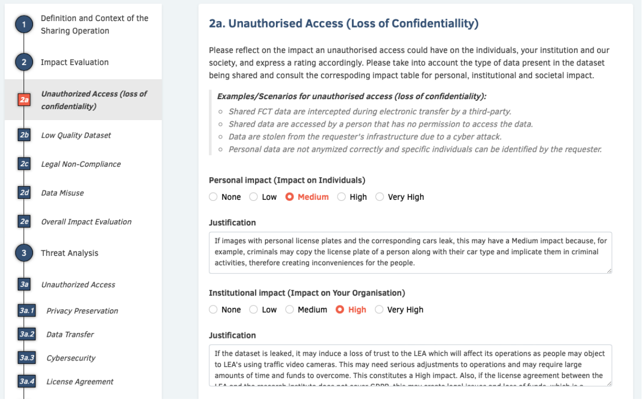
LEVEL OF IMPACT	AREA OF EFFECT – SOCIETAL
Low	○ Minor inconveniences for society, which can be resolved without any problem ().
Medium	○ Major consequences to society, which can be resolved although with some effort (distrust towards LEAs or ministries, smaller demonstrations, articles in newspapers, etc.).
High	○ Major consequences to society, which may be resolved with some serious effort (worsening of international-diplomatic relations, large demonstrations, negative opinions in media for law enforcement agencies, major distrust by people towards institutions and agencies that keep personal data for security reasons or research, loss of value for city areas, etc.).
Very High	○ Major or irreversible consequences to society, which can lead to unrest and instability (protests, public demonstrations, disruption of social peace and national security, complete loss of trust to agencies and government)

Figure 4: Impact table for society

which include anonymization, data annotations, the data transfer method, etc. **(ii) Parties/Persons involved**, which assesses the experience of the people involved in handling the data, the involvement of third-parties in data processing, etc. **(iii) Institutional threats**, which examines the environment of the data requester regarding their cybersecurity protocols, data governance schemes and if they follow general data access protection guidelines. **(iv) Legal threats**, which examines threats stemming from the legal agreement between the two parties, such as data distribution to third parties, publishing parts of the data in scientific works, etc. The license agreement must control, if possible, all aspects of the data lifecycle so that the intended use for the dataset is also enforced legally to the requester. The final threat level comes after calculating the score for each individual category and is mapped onto three levels: low, medium and high.

Risk Evaluation. In this section, the data provider is presented with an evaluation of the risk for each area of effect, namely personal, institutional and societal. Special attention has been given to the explainable result. The data provider is presented with a set of explanations for the evaluation so that they are aware of the reasons that led to this particular result. This feature can help data providers feel more comfortable sharing their data because they understand all the various risks that are involved.

Risk Mitigation. Finally, the risk assessment tool provides a list of security measures and other mitigation actions to reduce the residual risk remaining from Step 4. Based on these mitigation actions, the risk assessment proposes a set of restrictions to the license generation so that risks like personal data exposure and legal compliance are covered. Such restrictions could be the addition



2a. Unauthorised Access (Loss of Confidentiallity)

Please reflect on the impact an unauthorised access could have on the individuals, your institution and our society, and express a rating accordingly. Please take into account the type of data present in the dataset being shared and consult the correspoding impact table for personal, institutional and societal impact.

Examples/Scenarios for unauthorised access (loss of confidentiality):

- *Shared FCT data are intercepted during electronic transfer by a third-party.*
- *Shared data are accessed by a person that has no permission to access the data.*
- *Data are stolen from the requester's infrastructure due to a cyber attack.*
- *Personal data are not anymized correctly and specific individuals can be identified by the requester.*

Personal impact (Impact on Individuals)

○ None ○ Low ● Medium ○ High ○ Very High

Justification

If images with personal license plates and the corresponding cars leak, this may have a Medium impact because, for example, criminals may copy the license plate of a person along with their car type and implicate them in criminal activities, therefore creating inconveniences for the people.

Institutional impact (Impact on Your Organisation)

○ None ○ Low ○ Medium ● High ○ Very High

Justification

If the dataset is leaked, it may induce a loss of trust to the LEA which will affect its operations as people may object to LEA's using traffic video cameras. This may need serious adjustments to operations and may require large amounts of time and funds to overcome. This constitutes a High impact. Also, if the license agreement between the

Figure 5: Risk Assessment - Explanations & Examples

of the appropriate clauses prohibiting data distribution to other partners, GDPR clauses if personal data are present, etc.

As such, the risk assessment tool has been designed to facilitate compliance with the relevant regulatory frameworks. Under European data protection law, the GDPR and LED mandate the performance of a so-called Data Protection Impact Assessment (DPIA) when the envisioned data processing activities are likely to result in a high risk to the rights and freedoms of natural persons. As these heightened risks are particularly prominent when processing sensitive data relating to criminal offences or using new technologies such as AI applications, it is almost inevitable that the collection, processing and sharing of FCT (Fight Crime & Terrorism) data to support innovative research and the development of novel tools would require the execution of a DPIA. In practice, this requires the data controller to provide an extensive description of the planned processing activities, assess the risks they pose to the rights and freedoms of individuals, and take appropriate measures to mitigate these risks.

Accordingly, the scope of the risk evaluation tool is not limited to mere security-adjacent threats but instead encompasses a broader field of risks in order to better support data controllers with demonstrating legal compliance. It is for this purpose that the risk assessment also includes concerns relating to the potentially adverse effects of biased datasets being used to train decision-making and support systems as well as the impact that the processing of sensitive data might have on societal interests like equality and human rights such as privacy and non-discrimination.

The proposed risk assessment approach presents a simple but comprehensive way for organizations without prior risk assessment experience to assess the risks of sharing their data with other partners for research. Being aware of the various threats and the risks that these threats lead to can raise awareness and make organizations and institutes more willing to participate in data-sharing activities.

4.3 Step 3: License Agreement Generation

In order to share datasets or models, it is important to have an appropriate and valid license file that is signed by both the data provider and requester. This license file serves as a legal agreement between the two parties and outlines the terms and conditions for sharing the dataset or model. The license file should clearly state the rights and responsibilities of both the data provider and requester. It should also specify the terms of use, such as the intended use of the data or model or any restrictions on its use.

The focus of the developed license generation module[2] lies on usability and is intended to support users, particularly those without formal training or experience in legal matters. Hence, the tool is based on two pillars. Firstly, the risk assessment provides mitigation actions, which can be read by the license generation module. In this way the suggested mitigation actions can be automatically considered in the license agreement. Hence, the identified risks can be reduced as proposed by the assessment. Note that inputting mitigation actions into the license generation module is optional. Secondly, the creation of a license file relies on the data provider's response to a series of tailored inquiries. The questions are crafted to be easily understandable and supplemented with comments containing explanations and examples, enabling users to utilize the software without extensive training.

The responses from the data provider are then used alongside the mitigation actions to generate the license. Depending on the type of data and additional constraints from the data provider, the software enables the creation of different types of licenses. Handling personal data needs to follow the GDPR [20] rules in the EU. Hence, if the data is classified as personal data, then the license file needs to include GDPR compliance. Highlighting the importance of complying with data privacy regulations is crucial for any organization dealing with personal data. Ensuring the possession of a valid license file is vital to minimizing possible legal consequences in the future. In the event that GDPR regulations apply, contract drafting is significantly constrained as the requirements of GDPR [4] must be adhered to. Particularly, the security measures at the data processor's end should align with the current state of technology and take into account the sensitivity of the data. It is important to note that a generic description of technical and organisational measures is not sufficient. Instead, a concrete description must be included in the DPA.

If the data does not involve personal information and there are no other usage restrictions, the module recommends to use an open license such as the Creative Commons licenses[3] and follows the open data initiatives; e.g. [8]. Further details concerning open licenses can be found in, e.g. [5, 13]. If the non-personal data is classified as a type that requires individually negotiated contracts, then the license file should reflect this. There could be restrictions on its usage such as commercial use restriction, so that the data may not be used for any commercial purposes or confidentiality obligations, in case the data contains sensitive information. In this case the module generates a proprietary license agreement.

5 DEMONSTRATION OF PROPOSED FRAMEWORK

In order to demonstrate the applicability of the proposed framework and argue about its usefulness for supporting the data exchange

[2] tool is available online at: https://dsi-demo.ait.ac.at/license-generation-web
[3] https://creativecommons.org/

for research purposes we will examine a hypothetical yet realistic scenario from the FCT research field.

For this scenario, we consider a data sharing request from a research institute to a law enforcement agency. Before sharing any data, the Law Enforcement Agency requests some information from the research institute to build a requester profile like the one presented in Table 2. The research institute wants to develop an AI model for tracking vehicle movement through the city. A law enforcement agency wants to share a set of videos from CCTV and traffic cameras throughout the city. A summary of this scenario can be seen in the Table 3.

Below, we examine each step of our proposed framework as presented in Figure 1.

5.1 Step 1: Privacy Preservation

The proposed pipeline for license plate anonymization on images follows the general methodology explained in Section 4.1, which consists of four steps that correspond to the above-mentioned ones: license plate detection, synthetic license plate generation, style transfer, and inpainting.

License Plate Detection. This block is in charge of detecting all the license plates in the input data. To perform such a task, a regression network that estimates the four corner points of the polygon that wraps the license plate is employed. Conventional object detectors only provide bounding box information, which would remove additional information around the original license plate when the inpainting step is executed.

Synthetic License Plate Generation. Concurrently, a non-existent license plate number is created and rendered on a 2D template for EU-like license plates. Since any anonymization procedure must not reveal personal data, the license plate number is randomly generated with a seven-element sequence of numbers, characters, and spaces.

Style transfer. To mirror the statistical properties of the original data, this module is in charge of transferring the style of the detected license plate into the synthetic one using Generative Adversarial Networks (GANs) techniques.

Inpainting. The last step involves replacing the original data with the synthetic one. This is performed by first projecting homographically the four corners of the customized license plate into the detected corners from the first module and then rendering the projected image on top of the original image.

During the license plate de-identification process, all vehicles and license plates in the image are identified before proceeding with the anonymization process. From this step, we extract the metadata of the position of the license plate (four corner points) and the license plate's detection score. For further metadata extraction, a vehicle detection and position estimation [21] extracts the position defined by a BBOX and the detection score.

The license plate and vehicle metadata measure the quality of the anonymization. For each detected vehicle, there should be a license plate. And this license plate detection should be inside the vehicle's detection. However, this is not always true, as there are multiple cases where a vehicle could be detected, but the license plate is not. For instance, a license plate in an image could be occluded by other vehicles or objects, such as trees, signals, etc. The variety of these cases is vast and can not be underestimated. The overlapping of two or more vehicles can be deduced using the vehicles' position. This way, if two vehicles appear in the same area, it can be considered that at least one of the license plates is not visible because it is covered.

The size of the detected vehicle compared to the image can also play a crucial role when considering whether a license plate is visible. If the size of the vehicle is petite, which can be compared with the total image size, the license plate might also be too small to be detected. In this case, the size makes the license plate's characters unrecognisable. Thus, the license plate is considered anonymous as it does not reveal personal information. The detection scores from the license plates and vehicles can elucidate why a license plate is not considered. The quality of the image can affect the detection score of the vehicles. If a detection score is not high enough, it could serve as a threshold to consider a vehicle not visible and, therefore, the license plate unrecognisable.

Table 2: Profile of the data requester

Data Requester Profile	
entity type	research institute
cybersecurity	follows the ISO27001 standard
data governance	follows the ISO27001 standard
external security auditing	no external auditor
people experience	the people that will be handling the data have years of experience working with sensitive data

Table 3: Demonstration Scenario: Traffic camera feed exchange for AI tool development

Demonstration Scenario: Traffic camera feed exchange	
use case	traffic camera video feed
intended use	development of an AI tool for tracking vehicle movement throughout a city
dataset nature	real data
data types	video, cars, license plates
personal data included	license plates
special data included	none
constraints	confidentiality, dataset may only be stored and used withing the EU, potential bias
data transfer method	secure web service at the premises of the requester
data distribution	no distribution of data to third-parties, no publishing of parts of data to scientific works

From experimentation and manual verification, we concluded that a detection score of over 0.8 indicates a properly detected vehicle. Therefore, by dividing the total number of license plates by the number of vehicles detected (with a score > 0.8), we can accurately represent the number of license plates that were anonymized correctly. The dataset to be exchanged contains a few thousand images taken from traffic camera feeds. These images contain personal data that must be anonymized before being sent to the requester. Our privacy preservation module anonymizes the license plates in each image as explained in Section 4.1. The anonymization statistics produce an anonymization quality assessment of 0.92, mapped to a medium threat level. This statistic is passed on to the Risk Assessment module for Step 2.

5.2 Step 2: Risk Assessment

Impact Levels. The risk assessment starts by evaluating the impact level of this sharing operation. We consider the impact that a set of personal license plate numbers will have on the individual, institution and society. Based on the impact levels presented in Figures 2, 3 and 4, we can deduce the following impact levels: (i) **Personal**. If images with personal license plates and the corresponding cars leak, this may have a **Medium** impact because, for example, criminals may copy the license plate of a person along with their car type and implicate them in criminal activities, therefore creating inconveniences for the people. (ii) **Institutional**. If the dataset is leaked, it may induce a loss of trust in the LEA, affecting its operations as people may object to LEA's using traffic video cameras. This may require serious adjustments to operations and large amounts of time and funds to overcome. This constitutes a High impact. Also, if the license agreement between the LEA and the research institute does not cover GDPR, it may create legal issues and loss of funds, a Medium impact according to Figure 3. So, the final impact level for the institution is **High**. (iii) **Society**. If there is a dataset leak, people may display distrust towards LEAs, ministries and government in general, which is a **Medium** impact level according to Figure 4.

For the threat occurrence probability, we examine each threat category separately, and the user, based on the particulars of the sharing operation and the contents of the actual data, can infer how each threat can compromise a safe sharing operation by contributing to the risks of unauthorised access, biased dataset, personal data exposure or lack of legal compliance.

Technological Threats probability. The anonymization quality assessment is 92% successful (as given by the privacy preservation module), which means that there were a lot of images that have not been anonymized and the license plate remained as is. This can create issues for people but also for the institution from a legal compliance perspective. Furthermore, the data are transferred through a secure and encrypted web service at the requester's premises that has been tried and tested. The dataset contains no annotations that may leak parts of the data. Taking the above into account, the threat occurrence probability can be assessed as medium.

People Related Threats probability. In this scenario, we assume that the dataset will be accessed only by senior research staff and won't be available to other personnel. The senior researchers have years of experience handling sensitive data from research projects, so the probability of threat occurrence should be low.

Institutional Threats probability. Based on their profile (Table 2 the requester implements the ISO27001 standard at their premises, where the data will be kept. However, they are not audited by an external authority, which means that some parts of the standard may not be implemented correctly or may have been neglected over time. This means that from a cybersecurity, data governance, and data access protection standpoint, there may be flaws that may lead to unauthorised access either from within the organisation (other staff getting access to the data) or from outside the organisation (through a breach of security). For these reasons, the threat occurrence probability should be medium.

Legal Threats probability. The dataset contains personal data (license plates) requiring GDPR compliance. The data controller requests the processor to use the dataset only in-house. Therefore, the license agreement must prohibit any distribution of the data or part of it. Finally, the license should have an expiration date; at that point, the licensee must provide evidence of deletion. The last part is necessary for the data provider to control the existence of their data and minimize risks. If the risk assessment module is used as a standalone tool, the user would be asked to evaluate all those aspects of their legal agreement with the requester and provide a probability level of threat occurrence. However, since our framework takes care of generating the appropriate license that covers the identified legal considerations with the appropriate frameworks. Therefore, the threat occurrence probability for this evaluation area is low.

Each threat category receives a score based on the occurrence probability level, which is added to calculate the overall threat occurrence probability like in Table 4. After evaluating the impact levels and the threat occurrence probability, we can calculate the overall risk level per area of effect, by mapping the impact level to the threat probability in a 3x3 matrix. This produces the following risk levels as presented in Figure 6.

The risk assessment module automatically proposes a set of mitigation measures to reduce the risk. In this scenario, it suggests to conduct a thorough manual review of the anonymized dataset to verify that any non-anonymized license plate information is safe for sharing (e.g., ensuring that license plate numbers are not discernible). Alternately, only share the anonymized portion of the dataset. Manual reviews, however, can be costly and impractical, especially when dealing with large volumes of data. In this particular scenario, a manual review is not possible, so that GDPR regulations still apply. From the set of mitigation actions, the ones related to the license agreement are forwarded from the risk assessment module to the license agreement generation module.

Table 4: Threat Occurrence Probability for the Demonstration Scenario

Threat Category	Probability	Score
Technological	Medium	2
People Related	Low	1
Institutional	Medium	2
Legal	Low	1
Overall	**Medium**	6

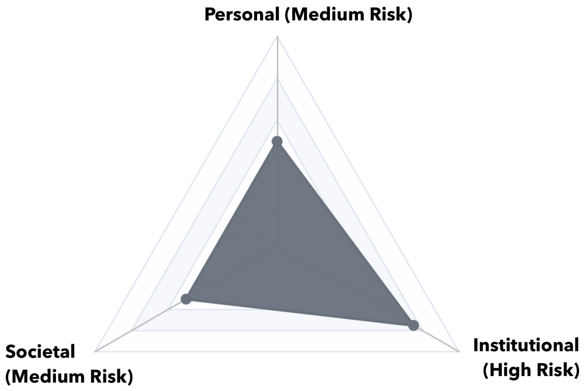


Figure 6: Overall Risk Level Assessment

The data provider can take the risk evaluation as PDF document to discuss it internally and decide if they want to move on with the sharing operation. If the provider decides to continue, Step 3 will generate the appropriate license agreement.

5.3 Step 3: License Agreement Generation

The license agreement generation is the last step of the risk assessment and legal compliance framework. In this scenario, the risk mitigation actions from Step 2 are a key input to the license agreement generation process. The following mitigation actions have been identified (compare with Table 1): (i) Comply with GDPR clauses (*RF 12*), (ii) Oblige the processor (requester) to perform an external audit with an expert regarding SOTA cybersecurity measures (*RF 8*), (iii) Consider bias in dataset (*RF 13*), (iv) Define purpose of data processing (*RF 15*), (v) Prohibit publishing of any data or parts of it in scientific works (*RF 11*).

To address *RF 12*, the module automatically generates a Data Processing Agreement (DPA) that complies with GDPR requirements. To mitigate *RF 13* two specific clauses are added to the DPA, which warns the processor that the data may be biased and on the other hand requires the processor to report any detected bias in the data. *RF 11* is addressed by a clause which ensures that neither the data nor parts of the data may be used in any types of publications.

The DPA contains a description of technical and organisational security measures implemented by the processor. This specific description is automatically extended by a clause (*RF 8*) that obliges the processor to carry out an external audit with an expert. Furthermore, the GDPR requires the controller to describe the specific purpose for which the personal data is processed by the processor. This description cannot be automatically generated, but the module ensures that this question is answered by the controller (*RF 15*).

Finally, the module generates a license (data processing agreement), which can be signed by both parties.

6 CONCLUSIONS

Sharing datasets that include personal data is both a necessary but also a potentially high-risk operation. Researchers need access to these data in order to perform state of the art research and develop tools that can propel our FCT efforts. However, understanding the impact of sharing personal data at scale and evaluating the risks is essential for the protection of individuals, but also institutions and society in general. Our proposed framework can help organisations handle data sharing with confidence by making them aware of all potential risks to the aforementioned areas so that these risks can then be controlled and an appropriate license agreement can be generated automatically that will ensure legal compliance with all relevant legal frameworks.

REFERENCES

[1] CNIL [n. d.]. *CNIL, Privacy Impact Assessment.* CNIL. https://www.cnil.fr/en/privacy-impact-assessment-pia

[2] ENISA [n. d.]. *On-line tool for the security of personal data processing.* ENISA. https://www.enisa.europa.eu/risk-level-tool

[3] 2016. ENISA's guidelines for SMEs on the security of personal data processing. https://www.enisa.europa.eu/tools

[4] 2016. 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). , 88 pages.

[5] Emad Alamoudi, Rashid Mehmood, Wajdi Aljudaibi, Aiiad Albeshri, and Syed Hamid Hasan. 2020. Open source and open data licenses in the smart infrastructure era: Review and license selection frameworks. *Smart Infrastructure and Applications: Foundations for Smarter Cities and Societies* (2020), 537–559.

[6] Orlando Amaral, Muhammad Ilyas Azeem, Sallam Abualhaija, and Lionel C Briand. 2023. Nlp-based automated compliance checking of data processing agreements against gdpr. *IEEE Transactions on Software Engineering* (2023).

[7] Simone Barattin, Christos Tzelepis, Ioannis Patras, and Nicu Sebe. 2023. Attribute-Preserving Face Dataset Anonymization via Latent Code Optimization. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*. 8001–8010.

[8] Jean-Claude Burgelman, Corina Pascu, Katarzyna Szkuta, Rene Von Schomberg, Athanasios Karalopoulos, Konstantinos Repanas, and Michel Schouppe. 2019. Open science, open data, and open scholarship: European policies to make science fit for the twenty-first century. *Frontiers in big data* 2 (2019), 43.

[9] Helena Haapio and Margaret Hagan. 2016. Design patterns for contracts. In *Networks. Proceedings of the 19th international legal informatics symposium IRIS*. 381–388.

[10] Yunosuke Higashi, Masao Ohira, and Yuki Manabe. 2023. Automating License Rule Generation to Help Maintain Rule-based OSS License Identification Tools. *Journal of Information Processing* 31 (2023), 2–12.

[11] Tobias Kamelski and Francisco Olivos. 2024. AI-Replicas as Ethical Practice: Introducing an Alternative to Traditional Anonymization Techniques in Image-Based Research. (2024).

[12] Mohammad Hossein Khojasteh, Nastaran Moradzadeh Farid, and Ahmad Nickabadi. 2023. GMFIM: A generative mask-guided facial image manipulation model for privacy preservation. *Computers & Graphics* 112 (2023), 81–91. https://doi.org/10.1016/j.cag.2023.03.007

[13] Ignasi Labastida and Thomas Margoni. 2020. Licensing FAIR data for reuse. *Data Intelligence* 2, 1-2 (2020), 199–207.

[14] Lamyanba Laishram, Jong Taek Lee, and Soon Ki Jung. 2024. Face De-Identification Using Face Caricature. *IEEE Access* 12 (2024), 19344–19354. https://doi.org/10.1109/ACCESS.2024.3356550

[15] Abdul Majeed and Sungchang Lee. 2021. Anonymization Techniques for Privacy Preserving Data Publishing: A Comprehensive Survey. *IEEE Access* 9 (2021), 8512–8545. https://doi.org/10.1109/ACCESS.2020.3045700

[16] Joana Ferreira Marques and Jorge Bernardino. 2020. Analysis of Data Anonymization Techniques. In *International Conference on Knowledge Engineering and Ontology Development.* https://api.semanticscholar.org/CorpusID:227129790

[17] Suntherasvaran Murthy, Asmidar Abu Bakar, Fiza Abdul Rahim, and Ramona Ramli. 2019. A Comparative Study of Data Anonymization Techniques. In *2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*. 306–309. https://doi.org/10.1109/BigDataSecurity-HPSC-IDS.2019.00063

[18] Qianru Sun, Liqian Ma, Seong Joon Oh, Luc Van Gool, Bernt Schiele, and Mario Fritz. 2018. Natural and Effective Obfuscation by Head Inpainting. In *2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition*. 5050–5059. https://doi.org/10.1109/CVPR.2018.00530

[19] Amar Tauqeer, Anelia Kurteva, Tek Raj Chhetri, Albin Ahmeti, and Anna Fensel. 2022. Automated GDPR contract compliance verification using knowledge graphs. *Information* 13, 10 (2022), 447.

[20] Paul Voigt and Axel Von dem Bussche. 2017. The eu general data protection regulation (gdpr). *A Practical Guide, 1st Ed., Cham: Springer International Publishing* 10, 3152676 (2017), 10–5555.

[21] Cong Xiong, Anning Yu, Senhao Yuan, and Xinghua Gao. 2023. Vehicle detection algorithm based on lightweight YOLOX. *Signal, Image and Video Processing* 17 (2023), 1793–1800. Issue 5. https://doi.org/10.1007/s11760-022-02390-1