Sharing is Caring: a Legal Perspective on Sharing Language Data Containing Personal Data and the Division of Liability between Researchers and Research Organisations

Aleksei Kelli
University of Tartu, Estonia
aleksei.kelli@ut.ee

Krister Lindén
University of Helsinki, Finland
krister.linden@helsinki.fi

Kadri Vider
University of Tartu, Estonia
kadri.vider@ut.ee

Pawel Kamocki
IDS Mannheim, Germany
pawel.kamocki@gmail.com

Arvi Tavast
Institute of the Estonian Language, Estonia
arvi@tavast.ee

Ramūnas Birštonas
Vilnius University, Lithuania
ramunas.birstonas@tf.vu.lt

Gaabriel Tavits
University of Tartu, Estonia
gaabriel.tavits@ut.ee

Mari Keskküla
University of Tartu, Estonia
mari.keskkula@gmail.com

Penny Labropoulou
ILSP/ARC, Greece
penny@ilsp.gr

Irene Kull
University of Tartu, Estonia
irene.kull@ut.ee

Age Värv
University of Tartu, Estonia
age.varv@ut.ee

Merle Erikson
University of Tartu, Estonia
merle.erikson@ut.ee

Andres Vutt
University of Tartu, Estonia
andres.vutt@ut.ee

Silvia Calamai
University of Siena Italy
silvia.calamai@unisi.it

Abstract

The article focuses on determining responsible parties and the division of potential liability arising from sharing language data (LD) containing personal data (PD). A key issue here is to identify who has to make sure and guarantee the GDPR compliance. The authors aim to answer 1) whether an individual researcher is a controller and 2) whether sharing LD results in joint controllership or separate controllership (whether the data's transferee becomes the controller, the joint controller or the processor). The article also analyses the legal relations of parties involved in data sharing and potential liability. The final section outlines data sharing in the CLARIN context. The analysis serves as a preliminary analytical background for redesigning the CLARIN contractual framework for sharing data.

Aleksei Kelli, Krister Lindén, Kadri Vider, Paweł Kamocki, Arvi Tavast, Ramūnas Birštonas, Gaabriel Tavits, Mari Keskküla, Penny Labropoulou, Irene Kull, Age Värv, Merle Erikson, Andres Vutt and Silvia Calamai 2021. Sharing is Caring: a Legal Perspective on Sharing Language Data Containing Personal Data and the Division of Liability between Researchers and Research Organisations. *Selected papers from the CLARIN Annual Conference 2020*. Linköping Electronic Conference Proceedings 180: 180 129–147.

1 Introduction

The article focuses on determining responsible parties and the division of potential liability arising from sharing language data (LD) containing personal data (PD). The General Data Protection Regulation (GDPR) defines personal data as *"any information relating to an identified or identifiable natural person ('data subject')*" (Art. 4 (1)). Sharing personal data constitutes its processing[1] which has to follow the GDPR.[2]

A key issue here is identifying who has to guarantee the GDPR compliance and assumes liability for a GDPR violation. The controller and the processor are named as responsible parties (GDPR Art. 4).[3] The GDPR defines the controller as *"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*" (Art. 4 (7)). The processor is defined as *"a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller"* (Art. 4 (8)).

The authors place this question in the context of language research. The following practical questions are addressed: 1) how to differentiate between obligations of the research organisation and individual researchers (e.g. whether an individual researcher is a controller) and; 2) whether sharing LD results in joint controllership or separate controllership (whether the transferee of the data becomes the controller, the joint controller or the processor).

In the first part after the introduction, the authors outline the general principles explaining the relationship between the organisation (e.g. the university) and its employees (researchers). Short case-studies serve as practical examples of how the university-researcher relationship is addressed in European countries. The authors' profile and expertise determined the choice of countries.

In the second part of the article, the authors focus on the legal relations of parties involved in sharing language data. It is essential to distinguish a situation when both parties are controllers (incl. joint controllers) and a situation when one party is the controller, and the other party is the processor (assists the controller in a limited way).

The third part is dedicated to liability and aims to describe what happens if the GDPR requirements are violated. In the last part, sharing language data within the CLARIN framework is briefly analysed.

The article continues and draws on previous research exploring the intersection of language research and personal data protection. The authors started their research by exploring the concept of personal data and analysing legal bases for its processing in the field of language technology (see Kelli et al. 2019; Klavan et al. 2018; Lindén et al. 2020). In this article, the authors with diverse backgrounds address the issue of responsible parties and liability arising from a violation of personal data laws. The paper serves as a preliminary conceptual analysis behind redrafting the CLARIN contractual framework for data sharing (for previous discussions on the contractual framework, see Kelli et al. 2015; Kelli et al. 2018).

Due to the specific focus and limited space, the article does not address the transfer of PD outside the EU, which concerns special provisions of the GDPR and EU case law (e.g. C‑311/18).

2 Duty-bearers for the GDPR Compliance within Research Settings

The key feature of the controller is the **determination** of the **purposes** and **means** of the processing of PD. According to WP29 *"Determination of the 'means' therefore includes both technical and organisational questions where the decision can be well delegated to processors (as, e.g. 'which hardware or software shall be used? ') and essential elements which are traditionally and inherently reserved to the determination of the controller, such as 'which data shall be processed?', 'for how long shall they be processed?', 'who shall have access to them? ', and so on"* (2010: 14).

[1] Article 4 (2) of the General Data Protection Regulation (GDPR) defines processing extensively so that it covers any operation which is performed on personal data (e.g. collection, storage, alteration and sharing).

[2] For the sake of clarity, not all language data (LD) contains personal data (PD). Furthermore, even if LD has PD, it is recommendable to make it anonymous (if possible) since the GDPR does not apply to anonymous data (GDPR Rec. 26). Anonymous data can be freely shared as long as PD protection is concerned. However, the authors focus on the cases when language data contains personal data. Language data or data within the context of this paper refers to language data that has personal data. For further discussion on anonymization see WP29 2014; Guidance 2019; ICO 2012; Sartor 2018.

[3] When it comes to liability, then as a general rule, any person who has suffered damage as a result of a GDPR violation has the right to receive compensation from the controller or processor (GDPR Art. 82 (1)).

A relevant issue for the research community is to analyse whether an individual researcher and/or the university is the controller. The research setting is a unique context since academic freedom is defined as a fundamental right.[4] This often gives researchers more freedom compared with other employees.

Considering relations between companies and their employees WP29 (2010: 15) indicates that *"preference should be given to consider as a controller the company or body as such rather than a specific person within the company or the body. It is the company or the body which shall be considered ultimately responsible for data processing and the obligations stemming from data protection legislation*". According to the European Commission (EC) "*if your company/organisation decides 'why' and 'how' the personal data should be processed, it is the data controller. Employees processing personal data within your organisation do so to fulfil your tasks as a data controller*". DP Handbook (2018: 102) similarly asserts that the legal entity (not its employees) is the controller.

WP29 (2010: 6) further explains that *"Controller and processor and their staff are therefore considered as the 'inner circle of data processing' and are not covered by special provisions on third parties"*. This is compatible with employment law. The employment law literature and case law also set forth that one of the characteristics of an employee is the fact that the employee is merged with the employer's team of other employees. The employee is employed and acts within the employer's economic activities (Risak & Dullinger 2018; C-22/98 para 26; C-66/85; C-256/01).

Although individual researchers conduct research with some freedom, their work is coordinated by the university. The university is responsible for the GDPR violations, and it has to implement appropriate technical and organisational measures (incl. data protection policies) to ensure the protection of PD (GDPR Art. 24) and to maintain a record of processing activities (Art. 30 GDPR).[5] The question is whether academics could be considered the controller as well. The issue is not settled yet. However, European Parliamentary Research Service in its study concerning research (EPRS study 2019: 34) suggests that "*researchers and universities should assume that when processing personal data, their activities render them data controllers"*.

Furthermore, it is worth noting that controllership is an element of fact. Any contractual or other arrangements made by the interested parties (e.g. mere designation of X as the controller or a contract assigning controllership to B, whereas A determines the means and purposes of processing) is not binding on the data subject or data protection authorities.[6]

The approaches of different countries are analysed in alphabetical order to outline a possible model and to understand whether there is a common ground for a unified approach within CLARIN.

2.1 Estonia

According to the Organisation of Research and Development Act (ORDA), a research institution is a legal person or an institution in the case of which the principal activity is carrying out fundamental research, applied research or development, or several of the aforementioned activities (§ 3 (1) clause 1). The activities of Estonian public universities are regulated by special acts explicitly established for them. In this subsection, the authors rely on the example of the University of Tartu (UT) in explaining the responsibilities of a researcher and a research institution.

Under the University of Tartu Act (UTA), UT is a legal person in public law (§ 2 (2)). Despite academic freedom, academic staff do not have a special status. Under the Higher Education Act (HEA), the employment relationships of academic staff are regulated by an employment contract (§ 34). Thus, the division of responsibilities between a research institution and a researcher concerning the processing of personal data for research purposes can be based on the general approach to protecting personal data, according to which the employer is the responsible person (i.e. the employer is the controller).

---

[4] According to the EU Charter of Fundamental Rights *"The arts and scientific research shall be free of constraint. Academic freedom shall be respected"* (Art. 13).

[5] There might be a practical problem when an individual researcher collects data himself and the host university is unwilling to be the controller. One approach could be that if the host university of a researcher is unwilling to become the controller, the CLARIN Centre needs to do a due diligence to make sure that the data has been properly collected. If the due diligence is done correctly, the host of the CLARIN Centre may as well become co-controller of the data set.

6 WP29 (2010: 9): "…*even though the designation of a party as data controller or processor in a contract may reveal relevant information regarding the legal status of this party, such contractual designation is nonetheless not decisive in determining its actual status, which must be based on concrete circumstances*".

As the controller, the research institution must implement appropriate technical and organisational measures (including a data protection policy) to ensure the protection of personal data (GDPR Art. 24 (1)) and to keep records of processing operations (GDPR Art. 30). UT has followed this approach. To ensure the GDPR compliance, UT has adopted the Data Protection Policy that explains the processing of PD and information concerning the privacy of individuals and several internal guidelines on the processing of personal data, including in research.[7] This shows that the university is the controller.[8] The university must introduce the instructions on data processing to the employee processing PD and demand that they are complied with.

If the employee (incl. researcher, professor and other academic employees) violates personal data rights, the university becomes liable. The data subject can claim damages, termination of the violation and so forth. Simultaneously, the employee (researcher) has breached his/her duties and can be held liable by the university.[9] This means that if an employee does not comply with the rules on the protection of PD in force at the university, it is a breach of duty, for which the employee may be warned (that his employment contract is terminated if the violation is repeated) or his employment contract may be terminated. However, if the data subject has filed a claim for damages against the university due to non-compliance with the instructions given regarding the processing of personal data, the university may recover damages from the employee by way of recourse.

There could be cases when the researcher does not have an employment relationship with the research institution. Research work is carried out based on a contract of mandate or contract for services, and a doctoral student (as well as a master's student) who has the status of a student may also participate in the research. Unlike an employee, neither a mandatary and contractor nor a doctoral student is integrated in the research institution through subordination. However, in these cases, the research institution is also the research coordinator and the place of research. If the researcher works on the basis of a contract of mandate or contract for services or is a student and the research institution performs functions that are specific to the controller, the research institution is responsible for the processing of personal data. Considering the particular nature of the research and the academic freedom of the researcher, sometimes a researcher acting on a contract of mandate or contract for services or a student and a research institution may also be co-controllers who must enter into the corresponding agreement and inform the data subject about that agreement (GDPR Art. 26).

2.2 Finland

Universities in Finland are corporations under public law since 2009, at which time all employees, including professors, became regular employees. A professor and related teaching staff can be laid off if the university decides that there is no need for a particular discipline, e.g. no students are applying, or the university wishes to profile the university in a specific direction by deselecting a particular discipline.

The universities operate on a mandate to do teaching and research in the public interest.[10] They are funded based on annual negotiations with the government and by external funding for research. Despite freedom of research being granted in the Universities Act[11] and the Constitution of Finland, researchers

[7] Control over the processing of personal data is also subordinated to UT through the system of the ethics committee. The requirement of the ethics committee arises from the Personal Data Protection Act (PDPA), according to which the prior control of the ethics committee is required for the processing of special types of personal data for scientific purposes (PDPA §6(4)).

[8] UT also has a data protection specialist, which refers to UT's status as the controller.

[9] In exceptional cases, a person working in an enterprise or institution on the basis of an employment contract may be liable to the data subject as the controller pursuant to Art. 82 (1) of the GDPR. The Data Protection Working Party considers that *"the one liable for a data protection breach is always the controller, i.e. the legal person (company or public body) or the natural person as formally identified according to the criteria of the Directive. If a natural person working within a company or public body uses data for his or her own purposes, outside the activities of the company, this person shall be considered as a de facto controller and will be liable as such"* (WP29 2010: 17).

[10] Universities Act of Finland (§2 (1)): *"The mission of the universities is to promote independent academic research as well as academic and artistic education, to provide research-based higher education and to educate students to serve their country and humanity at large"*.

[11] Universities Act of Finland (§ 6 (1)): *"While universities enjoy freedom of research, art and teaching, teachers must comply with the statutes and regulations issued on education and teaching arrangements"*.

as employees of an established research organisation acting on behalf of the organisation are not personally responsible for research activities sanctioned by the organisation as long as they adhere to organisational rules and regulations.

Even if a university relies on the researchers to specify the purpose of their research activities and determine the means for their data processing activities, the university still controls the activity with internal regulations, e.g. concerning data protection. The university usually becomes the controller of personal data involved in the research, although the researcher may remain a co-controller.

The problematic cases are grant-funded researchers who do not have formal employment at a research institution. Such individuals may enter into an agreement with a university for access to research facilities at a favourable cost. In this case, if personal data is collected for research purposes, and the university agrees to assist in the process, the university becomes a co-controller. However, an independent grant-funded researcher may opt to remain the sole controller.

In Finland, many universities help their researchers with guidelines and templates on how to formulate a privacy notice and a record of processing when collecting research material containing personal data (e.g. University of Helsinki, University of Jyväskylä, Aalto University).

2.3 France and Germany

The analysis is likely to be different in countries (like Germany or France) where university professors are not employees of the university, but public servants (*fonctionnaires, Beamten*) appointed for life and independent in the exercise of their missions (not unlike, e.g. judges). In both countries, this status is seen as a fundamental guarantee of freedom of academic research. It is due to this independence of researchers that in both Germany and France, e.g. copyright in the works created by academics in principle belongs to them and not to their university or institution.[12] In light of this rule (referred to as '*professors' privilege'*), it may be hard to argue that despite the fact that professors can reap benefits of their work (precisely because they are free to decide how to do it), it is the university that should bear the responsibility for how researchers process personal data.

Along these lines, the French National Centre for Academic Research (CNRS), in its guide on data processing for research purposes (CNRS guide 2019: 12), defines the director of a unit (an individual, not an institution) as the data controller. Then, the director of a unit designates the CNRS' Data Protection Officer (DPO) as 'his' DPO. This practice is in line with Article 37(2) of the GDPR, according to which *"[a] group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment"*. Once designated, the DPO should be involved *"properly and in a timely manner, in all issues which relate to the protection of personal data"* (GDPR Art. 38 (1)). Having a common DPO for the whole institution is, therefore, an interesting way of providing for 'bottom-up standardisation' of data processing practice. However, the responsibility *stricto sensu* remains decentralised, as the DPO is not personally responsible for data processing. According to the principle of accountability, the responsibility always remains with the controllers.

This interesting approach in the CNRS is not necessarily shared by all French research institutions. Guidelines issued jointly by several institutions from the Paris region clearly state that in a research project, the researcher is a data controller, as long as he or she determines the means and purposes of processing (French University Guidelines 2019: 9).

In Germany, the situation is no less complex. The University of Cologne openly admits on its website that there are two confronting views regarding the data controllership, attributing the controllership either to the university, or to the researcher and that the university subscribes to the latter (University of Cologne, point 3). In an article published in the Frankfurter Allgemeine Zeitung, a leading German scholar on data protection suggests that – precisely for the reasons explained above, i.e. the freedom of research – it would be excessive to assign the liability for data processing to the university, and that it should be shared between the university and the researcher (as joint controllers) (Schwartmann, 2019).

[12] The solution is likely to differ when it comes to patents – e.g. in Germany, the professors' privilege in patent law was abolished in 2002, and the rights to a patentable invention developed by an academic now belong to his or her institution. Since in the field of language technologies university patents remain rather exceptional, we believe that in the context of this paper an analogy with copyright is more accurate.

This approach would imply that universities should conclude agreements with their researchers to determine their respective responsibilities for compliance with the obligations under the GDPR (Art. 26). There is no requirement that these responsibilities should be shared equally.

2.4 Greece

Research in Greece is performed at universities and specific research institutes. They are legal entities governed by public or private law and supervised by the General Secretariat of Research and Technology (Ministry of Education). The employment of the respective personnel (academic personnel/professors at universities and research personnel at research institutes) is stipulated in two different legal acts (SOQI and RTDI). There are three ranks at which professors and researchers can be hired. They are elected for three years for the lower rank, while the two upper ranks are associated with permanent tenure. Universities and research institutes can also hire scientific and technical personnel to conduct research with private contracts of a restricted or indefinite term. The conditions under which research can be conducted are stipulated in the law on "Research, Technological Development and Innovation" (RTDI).

Chapter E ("Committees for Research Ethics") of the Act 4521/2018 (Act UWA) implements the GDPR in the context of research. The Act stipulates the constitution of a committee for research ethics at all universities and research institutes. According to Sec. 2, one of the objectives of the committees for research ethics is to *"control whether a research project is conducted respecting the value of human beings, […] their private life and personal data…".* Before the beginning of a funded project that includes research related to human beings, scientific coordinators must submit before the committee an application that *"includes a questionnaire and a short report on the adequacy and compliance of the project with the current law"*. Further specifications on the application and evaluation procedure and required documents are included in the Regulation of Principles and Operation of the Committee of each institute.

A survey of the regulations of research ethics committees of various academic and research institutes[13] indicates the adoption of the same policy across them: the institute is acknowledged as the *"entity responsible for the processing of PD"* (the data controller), but the scientific coordinators and all researchers involved in the processing of PD are also held accountable for the processing (joint controllers). They must make sure that they comply with the GDPR and take appropriate measures to safeguard PD throughout the whole procedure (e.g. obtain the data subjects' consent, use (pseudo-) anonymisation for the published data). Failure to comply with this obligation may result in administrative measures such as the project's termination, the reparation of damages, remunerations of affected subjects, and even the discharge from their positions.

In general, professors, researchers, and employees at the institute are bound by these regulations as a result of their professional affiliation. Also, the scientific coordinators must sign a form stating that they are aware of the institute's Code of Ethics, that they will conform to it, and that no changes will be made to the project as described in the application. If any changes are required, an application must be resubmitted. Individuals engaged specifically for the project with a special contract (contract of services) must sign an additional contract of terms and conditions for the processing of PD.

Simultaneously, the committees for research ethics provide their assistance and guidance to the researchers whenever required. Ready-to-use forms and templates are available to researchers.

2.5 Italy

Italian universities can be either public or private bodies. According to the Constitution of the Italian Republic (Art. 33), every university acts on the principles of independence and responsibility. State-run universities of Italy are under the supervision of the Italian's Ministry of University. Independence means that every university establishes self-government through its competent bodies (its faculty). Due

[13] The survey could not be extensive due to the fact that the Committees of some institutes are still in the process of writing up or updating these regulations. We note here the following: Aristotle University of Thessaloniki [AUTH], Athens University of Economics and Business [AUEB], Foundation for Research and Technology-Hellas [FORTH], University of Crete [UoC], University of Macedonia [UoM], University of Peloponnese [UoP], University of Patras [UoPa], University of Thrace [UoT], University of West Attica [UWA], National Center of Social Research [NCSR].

to the autonomy of the university, researchers and professors working in a public university are considered employees and not public servants/officials.

When the university employee (researcher, professor, temporary research staff) collects research material containing PD, the status of the controller is assumed by his/her university (as a legal entity). The individual scholar is designated as authorised for the treatment, as required by the law in force.

The Personal Data Protection Code (PDPC) sets forward the following principles (Section 2-o):

1. The controller or processor may provide under their responsibility and within the framework of the respective organisation that specific tasks and functions relating to the processing of personal data be allocated to expressly designated natural persons acting under the controller's or processor's authority.

2. The controller or processor shall set out the most appropriate arrangements to authorise the persons acting under their authority to process personal data.

However, the individual researcher cannot be designated as responsible for the processing since this role can only be covered by external subjects who under a contractual arrangement 'act' on behalf of the controller (Art 28 GDPR).

In 2017, the Association of general managers of Italian universities (*Convegno dei Direttori generali delle Amministrazioni Universitarie* – CoDAU) introduced guidelines for personal data processing (CoDAU guidelines). At the same time, the Italian association of Italian University Rectors (CRUI) prepared an internal draft regulation for Italian universities (CRUI regulations), which was last updated in January 2019.

Several universities, starting from CRUI regulations, published their own rules of procedures for processing personal data (e.g. Turin University, Modena and Reggio Emilia University, Bari University).

2.6 Lithuania

In Lithuania, the situation regarding the status of an individual researcher is not self-evident. For example, Vilnius University, the biggest and leading university in Lithuania, has adopted (2018) the Description of the procedure for PD processing at the University of Vilnius (the Description). The Description is silent on the issue if and how the status of the controller is divided between the university and the researcher. This question is not settled in the legal practice nor the legal doctrine.

In such a situation, the general norms and their interpretations should apply. From the outset, it should be noted that the position of professors and other researchers in Lithuanian universities is quite different compared with their counterparts in Germany. Lithuanian researchers have no special status and are regarded as regular employees. The general approach is that employees are not normally deemed the data controllers (DP Handbook 2018: 102).

Paragraph 4 of the Description also indicates that the university is the controller of all data collected during the university activities and internal administration processes as well as the controller of personal data transferred by data subjects and third parties.[14] This provision is further elaborated by paragraph 2 stating that the Description is applicable and compulsory to the data controller, *i.e.* the University of Vilnius and all University employees who are processing personal data in the course of work.

Thus, if professors and other researches are acting in the course of their academic duties (which are specified in their labour contracts, descriptions of positions, other general or local regulations, universities' programs and projects in which researchers participate and similar documents), they should not be regarded as data controllers, but just the employees of the controller (*i.e.* the university). While it is true that researchers have certain discretion while conducting their research, still the general rule is that the overarching goals of the research activities are set by the university and, by signing the employment contract and taking up his/her position, the researcher simply acts on behalf of the university.

Researchers are deemed controllers when they are not acting on behalf of the university. In other words, they act outside their employment duties and set their research purposes and means independently. However, in this scenario, they can no longer be considered university researchers.

[14] The same rule could be found in the earlier document (see Rules for processing PD 2015).

3 Legal Relations of Parties Involved in Sharing Language Data

The determination of a legal basis for processing (incl. sharing) language data is a key issue for language research. The suitable legal grounds could be the data subject's consent, public interest research or legitimate interest (GDPR Art. 6 (1) (a), (e), (f)).

The consent of the data subject should guarantee high-level protection of the data subject's rights and freedoms. However, this is not always possible (e.g. data was collected a long time ago, and there are no contact details). At the same time, the GDPR does not say that one legal ground is to be preferred over the others. Therefore, all suitable legal grounds (consent, public and/or legitimate interest) are equally applicable.

Since the issue has been previously studied (see, Lindén et al. 2019; Kelli et al. 2019) and due to the specific focus of the article, legal grounds are not further analysed here, and attention is given to legal relations of parties involved in data sharing.

3.1 Legal Relations between the Data Controllers

A key issue here is how much freedom parties have in determining who has which obligations under the GDPR. The European Data Protection Board (EDPB) has indicated that the concepts of the controller, joint controller and processor play a crucial role in the application of the GDPR since they determine who shall be responsible for compliance with different data protection rules and how data subjects can exercise their rights in practice (EDPB 2020: 3). According to WP29, *"Being a controller is primarily the consequence of the factual circumstance that an entity has chosen to process personal data for its purposes"* (2010: 8). WP29 clarifies further that the control could originate from the factual influence and the assessment of contractual relations is helpful since relevant actors often see themselves as facilitators rather than controllers. The contractual terms, however, are not decisive (2010: 11). EDPB (2020: 3) adds that the controller is a body that decides certain key elements of the processing, controllership may be defined by law or may stem from an analysis of the factual elements or circumstances of the case, and certain processing activities can be seen as naturally attached to the role of an entity (an employer to employees, a publisher to subscribers or an association to its members).

WP29 (10/2006) found that an entity (SWIFT) was a controller despite presenting itself as a processor based on a functional influence test. This demonstrates that any designation of controller/processor which does not correspond to the facts is void, and the actual situation is decisive, not the contract. The controller is who factually determines the purposes for which the personal data are processed.

When sharing language data for scientific purposes, it can be assumed that both parties (the party sharing data and the recipient) are acting as the controllers. "*Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers"* (GDPR Art. 26 (1)). EDPB (2020: 3) explains that joint participation can take the form of a common decision taken by two or more entities or result from converging decisions by two or more entities, where the decisions complement each other, and they have a tangible impact on the determination of the purposes and means of the processing. EDPB (2020: 3) indicates, *"An important criterion is that the processing would not be possible without both parties' participation in the sense that the processing by each party is inseparable, i.e. inextricably linked"*. EDPB (2020: 21) has issued an example of joint controllership, which allows drawing parallels to assess the relationship between institutions sharing of language data: *"Several research institutes decide to participate in a specific joint research project and to use to that end the existing platform of one of the institutes involved in the project. Each institute feeds personal data it holds into the platform for the purpose of the joint research and uses the data provided by others through the platform for carrying out the research. In this case, all institutes qualify as joint controllers for the personal data processing that is done by storing and disclosing information from this platform since they have decided together the purpose of the processing and the means to be used (the existing platform). Each of the institutes, however, is a separate controller for any other processing that may be carried out outside the platform for their respective purposes"*.

EDPB (2020: 20) also notes that "*the use of a common data processing system or infrastructure will not in all cases lead to qualify the parties involved as joint controllers, in particular where the processing they carry out is separable and could be performed by one party without intervention from the other*".

In the case of a joint controllership, a transparent arrangement between the joint controllers must be agreed upon to comply with the GDPR (Art. 26 (1)). The essence of this arrangement should be made available to the data subjects (Art. 26 (2)). WP29 (2010: 24) explains it as follows *"Parties acting jointly have a certain degree of flexibility in distributing and allocating obligations and responsibilities among them, as long as they ensure full compliance"*. The controller's responsibilities must be clearly defined in accordance with actual data processing. The arrangement must reflect the respective roles and relationships of the joint controllers *vis-à-vis* the data subjects (GDPR Art. 26 (2)). EDPB (2020: 41*)* adds, *"It should be made clear here that all responsibilities have to be allocated according to the factual circumstances in order to achieve an operative agreement".* Joint controllers need to define who is in charge of answering requests of data subjects, providing needed information and fulfilling lawfully the requests of data subjects ("right to be forgotten*",* etc.). They need to ensure that the whole processing fully complies with the GDPR (EDPB 2020: 41). Otherwise, as indicated by WP29 (2010: 24), the processing is considered *"unlawful due to a lack of transparency and violates the principle of fair processing"*.

Although the GDPR does not specify the legal form of arrangement between joint controllers and therefore, parties are free to agree on the arrangement. The EDPB (2020:43) recommends that such arrangement be made in the form of a binding document such as a contract or other legally binding act under EU or Member State law to which the controllers are subject. EDPB (2020: 43) adds: "*the use of a contract or other legal act will allow joint controllers to demonstrate that they comply with the obligations imposed upon them by the GDPR".*

3.2 Legal Relations between the Controller and the Processor

The controller (language data owner) can use limited and clearly defined assistance in processing data (e.g. structuring data, making it available). If a CLARIN consortium member makes the language data available itself, it is the controller. The person/entity assisting the controller is the processor.[15] The described situation is also applicable to the case when someone deposits language data with a CLARIN consortium member (see Sec 5). Any processing of PD by the processor must be governed by a contract (GDPR Art. 28).

The GDPR requires that the controller uses only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing meets the requirements of the GDPR and to ensure the protection of the rights of the data subject (Art. 28 (1)). The processor can process the personal data only on documented instructions from the controller (Art. 28 (3) a). Therefore, special attention should be given to the content of this agreement. The controller and the processor may choose to compile their contract including all the compulsory elements or to rely upon, in whole or in part, on standard contractual clauses (SCCs) adopted by the European Commission (Art. 28 (6).[16] The contract may be concluded under terms negotiated separately between the parties or may be based on contract terms drafted in advance for use in standard contracts or which the parties have not negotiated individually for some other reason (standard terms and conditions). The use of standard terms in data processing contracts is the most common way in practice due to a large number of parties. In the sharing of language data, it is also the most reasonable to use a drafted in advance standard data processing agreement by standardising the requirements applicable to data sharing procedures.

The GDPR requires the contract to regulate the following: *"the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller"* (Art. 28 (3)).

The parties must sufficiently describe the nature of responsibilities, taking into account the real risks and activities carried out under the specific research project to ensure that all appropriate safeguards are provided (see Art. 89 (1)). EDPB explains it as follows: *"clauses which merely restate the provisions of Article 28(3) and (4) are inadequate to constitute standard contractual clauses. /…/ a contract under*

[15] WP29 (2010: 1) explains that the processor has to meet two conditions: 1) a separate legal entity with respect to the controller; 2) it processes PD on behalf of the controller.

[16] On the 14. January 2021 the EDPB and European Data Protection Supervisor (EDPS) have adopted joint opinions on two new updated sets of contractual clauses (SCCs): one opinion on the SCCs for contracts between controllers and processors and one on the SCCs for the transfer of personal data to third countries. Available at https://edpb.europa.eu/our-work-tools/consistency-findings/edpbedps-joint-opinions_en (27.1.2021).

Article 28 GDPR should further stipulate and clarify how the provisions of Article 28(3) and (4) will be fulfilled" (2019: 5).

In addition to the list of obligations and rights in Article 28, the GDPR also contains other parties' obligations that should be agreed upon in the contract. For instance, one such obligation is the processor's obligation to notify the controller of data breaches (Article 33 (2)). The parties could agree on the reasonable deadlines of notifying breaches or refer to written documented instructions governing more specific data sharing procedures in such cases. Additionally, it is necessary to agree on other conditions of the parties' rights and obligations not mentioned in the GDPR, including reimbursement of expenses and remuneration, procedures for amendments, and the contract's termination.

The agreement between the controller and the processor must be concluded in written form, including electronic form (Art. 28 (9)). EDPB (2020: 30) has pointed, that non-written agreements (regardless of how thorough or effective they are) cannot be regarded as sufficient laid down in Article 28. Therefore, to avoid any difficulties in demonstrating that the contract is actually in force, the EDPB recommends ensuring that the necessary signatures are included. Otherwise, the competent supervisory authority will be able to direct an administrative fine against both parties (2020: 31).[17] The electronic form has been clarified by the European Parliament (2018): "*However, the rules for entering into contracts or other legal acts, including in electronic form, are not set forth in the GDPR but in other EU and/or national legislation. The e-commerce Directive (Directive 2000/31/EC) provides for the removal of legal obstacles to the use of electronic contracts. It does not harmonise the form electronic contracts can take. In principle, automated contract processes are lawful. It is not necessary to append an electronic signature to contracts for them to have legal effects. E-signatures are one of several means to prove their conclusion and terms".*

The GDPR does not determine whose responsibility is to ensure that the contract for personal data processing is concluded correctly. It is important to note that the requirements of the GDPR are infringed where data processing starts without a binding written contract, and the processor cannot demonstrate the existence of documented instructions (Art. 28 (3)). In such a case, the processor may be considered as the controller in respect of such processing and is subject to the obligations and increased liability of the controller (Art. 28(10)).[18] The obligation to use only processors who are providing sufficient guarantees does not end when the contract is concluded. It is a continuous obligation, and the controller should regularly verify the processor's guarantees through audits and inspections to ensure that the actual data processing is correspondent to the contract and properly and lawfully executed (EDPB 2020: 30).

4 Legal Remedies in Case of Non-compliance with the GDPR

The GDPR provides severe administrative penalties for failure to comply, and the personal data protection authority has been given broad powers. In addition to that, a claim for compensation may be submitted by the person (data subject) who has suffered damage as a result of a breach of data protection requirements (Art. 82 (1)). In some cases, claims for damages may also be filed by family members or heirs (Wybitul, Haß & Albrecht:113-118; Cordeiro 2019: 492-499). A claim can be filed against the controller or the processor. For example, suppose the requirements of the GDPR have been violated in the processing of data for research purposes. In that case, the data subject may file a claim for damages with the university (but not against specific employees who process the data).

A precondition for satisfying a claim for damages is a breach of obligations provided for in the GDPR and in the Member State laws specifying rules of the regulation (Rec. 146).[19] Controllers have obligations that can be described as obligations to *achieve a specific result*. For example, personal data must be collected for legitimate purposes and processed in a way compatible with those purposes (GDPR Art.

[17] Infringements of the obligations of the controller and the processor pursuant to Article 28, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher (GDPR Art. 83 (4) a)).

[18] Otherwise, the processor is liable to the data subject for the damage caused by the processing only if processor has failed to comply with the requirements of the GDPR specifically addressed to the processors or processor has not complied with the legal instructions of the controller or has acted against them (Art. 82 (2)).

[19] See also Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). Brussels 10.1.2017. COM (2017) 10 final. 2017/0003(COD). Awaiting Parliament's position in 1st reading.

24 (1)). Most of the controller's obligations can be characterised as obligations to make *reasonable efforts* to do something. For example, Article 6 (1) (d) of the GDPR provides that the controller must take *"every reasonable step"* to ensure that data that is inaccurate or incomplete shall be erased or rectified. To ensure and be able to prove the GDPR compliance, the controller must implement appropriate technical and organisational measures as provided by Art 25 (1) and Art. 32 (1) (for further discussion, see Van Alsenoy 2016). When data is processed on a contractual basis, it is necessary to consider which measures are appropriate for the fulfilment of specific instructions and obligations and to describe them as precisely as possible to assess whether the data controller has fulfilled its obligations. The contract should consist of the technical and organisational measures that are used to demonstrate the GDPR compliance (Art. 24 (1)). When processing is based on consent, the controller must be able to present evidence that the data subject has consented to the processing of his personal data (GDPR Art. 7 (1)).

The processor involved in the processing is liable for breaches of its obligations if it has not complied with the controller's legal instructions or has acted against them. However, the controller is not released from liability if the processor has violated the data processing requirements. The controller may, in turn, claim from the processor compensation for the damage caused by the breach of obligations by the processor and compensated the data subject by the controller (GDPR Art. 82 (5)). The parties may agree in the contract how the compensated damage will be shared (Alsenoy 2016: 285).

It is presumed that the controller and processor are liable for events that result in damage suffered by data subjects. This means that in court proceedings, the controller is required to prove that it is in no way responsible for the damage (GDPR Art. 82 (3)). Here the compliance certificates (GDPR Art. 43) can be of major practical importance. However, the certificate is not a safeguard against civil liability but can be used as a piece of evidence that the GDPR standards were implemented and that a party is not responsible[20]. The processor also has some options to defence, especially if damage occurred is due to actions outside or contrary to the lawful instructions of the controller. In conclusion, the controller's liability is strict, i.e., the processor is released from liability only if he can prove that the data processing requirements have not been breached (Van Alsenoy 2016: 276, Strugala 2020: 77).

A personal data breach may result in physical, material or non-material damage to natural persons such as loss of control over their PD or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned (GDPR Rec. 85). On such occasions, the data subjects may claim full and effective compensation for the damage suffered, which means that both material and non-material damage is subject to compensation (Truli 2018).

The data subject's various costs (e.g. legal costs) could be considered as material damage. In addition, material damage may occur in the form of loss of income. For example, the data subject may lose income in the case of termination of an employment contract due to the disclosure of certain data or if stricter contractual conditions were imposed on him or her by financial institutions (Cordeiro 2019: 495). As the GDPR does not give any guidelines about the assessment of damages, national case law on non-material damage varies widely. In some Member States, the mere processing of data contrary to data protection legislation is not a sufficient violation to justify an award of non-material damage (Sein et al. 2018: 112). The person must have suffered noticeable disadvantage, and it had to be an objectively comprehensible impairment of personality-related interests with a certain weight (Oberlandsgericht Dresden 2019; Landesgericht Karlsruhe 2019)[21]. In some Member States, the mere fact of misuse of data can be sufficient to justify non-material damages (van Alsenoy 2016: 271; Rechtbank 2020). There is a significant risk that the GDPR infringement cases will give rise to a very differentiated court practice regarding the assessment of damages for non-pecuniary harm (Strugala 2020: 68).

If the controller or the processor has paid full compensation for the damage suffered in a situation where more than one controller or processor are involved in the same processing of personal data, the

[20] According to the Recital 81 of the GDPR the controller should use only processors who can provide sufficient guarantees in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures, including for the security of processing. So, the adherence of the processor to an approved code of conduct or an approved certification mechanism may be used as an element to demonstrate compliance with the obligations of the controller.

[21] For example, the German Higher Regional Court of Dresden held that minor loss did not give rise to any claim for non-material damages pursuant to Article 82.

controller or processor is entitled to claim back from the responsible parties the compensation corresponding to their part of the responsibility for the damage ((Art. 82 (5); see also Van Alsenoy 2016). This rule is based on the general principle provided for in the Art. 28 (4) of the GDPR that the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

In addition to filing a claim for damages, the data subject can also demand the termination of the activity, causing the damage and refrain from doing so in the future.[22]

5 Sharing Language Data within the CLARIN Framework

When it comes to data sharing inside the CLARIN community, we can distinguish between two different situations: 1) an external individual or entity deposits LD with a national CLARIN consortium member; 2) a national CLARIN consortium member itself makes LD available.

The first case involves the conclusion of a deposition agreement between the depositor and the CLARIN consortium member. The depositor determines the access and use conditions which makes the depositor the controller under the GDPR, and the CLARIN consortium member acts as the processor since it processes personal data on behalf of the depositor.

In the second scenario, the CLARIN consortium member shares LD on its behalf and is the controller.

The main question in both scenarios is whether the sharing of LD leads to joint controllership between the party who shares and the party who receives the data. According to the GDPR joint controllers jointly determine the purposes and means of processing.[23] They need to determine their respective duties (Art. 26). The European Court of Justice (ECJ) has explained that *"a broad definition of the concept of 'controller', the effective and comprehensive protection of the persons concerned, the existence of joint liability does not necessarily imply equal responsibility of the various operators engaged in the processing of personal data. On the contrary, those operators may be involved at different stages of that processing of personal data and to different degrees*" (C‑40/17 para 70). This means that processing at different stages can result in joint controllership. The court has also maintained that *"a religious community is a controller, jointly with its members who engage in preaching, of the processing of personal data carried out by the latter in the context of door-to-door preaching organised, coordinated and encouraged by that community, without it being necessary that the community has access to those data, or to establish that that community has given its members written guidelines or instructions in relation to the data processing"* (C‑25/17 para 75). It says that it is possible to be a joint controller even without having access to PD. This could apply to data sharing situation as well.

From the CLARIN perspective, the proposed agreement structure for the transfer of personal data aims to establish a CLARIN Centre as a data processor serving the national CLARIN consortium with each of the consortium members, or an external party, as a controller of its data sets. To this end, the Finnish CLARIN consortium proposes a CLARIN Framework Deposition Agreement (FADA).

The CLARIN FADA is intended to establish a framework of standard deposition rules for data sets that can be communicated by a CLARIN Centre. Individual data sets are added as attachments to the CLARIN FADA, which thereby reduces to a 1-page main document for each data set referring to the general conditions and four data set specific appendixes:

1) the data identification, description and citation texts,
2) the deposition license conditions with an end-user license agreement template,
3) a list of third-party copyrights or database rights,
4) the personal data description and the purpose of use of the data set.

Appendixes 3 or 4 may explicitly be left empty if there are no third-party rights or no personal data in the data set.

[22] For example, Estonian case law has satisfied the requirement to submit an application to the information search systems Google, AltaVista and Yahoo to stop disclosing defamatory personal data in order to end a situation that damages a person's reputation. See Riigikohus 2010, p 11.

[23] In practice, 'purposes' are much more important than 'means' for determining the controller, cf. WP29 opinion: *"while determining the purpose of the processing would in any case trigger the qualification as controller, determining the means would imply control only when the determination concerns the essential elements of the means"* (2010: 14). It can be argued that in the CLARIN context, where the *'essential elements of the means'* are generally similar and known to everyone (computational analysis), only purposes matter.

In the CLARIN infrastructure, there are three main licensing categories dividing language resources into three groups: 1) Publicly available (PUB); 2) For academic use (ACA) and; 3) For restricted use (RES) (for further discussions, see Oksanen et al. (2010) and Kelli et al. (2018). The CLARIN RES licensing category (for restricted use) is suitable for sharing data sets with PD.

In the suggestions for how to implement the ethical intent of the GDPR in a research setting, Pormeister (2020) recommends that the original controller stays informed about all further use of a personal data set to inform the data subjects about such further use when necessary. The CLARIN RES license requires that data sets not be communicated to a third party by the end-user because a new legitimate end-user can always obtain a copy directly from CLARIN. As the CLARIN Centre, in most cases, remains a mere processor of personal data with the task to communicate such data to research organisations. The original controller stays informed about all requests for further use of a data set.

If there is a request for using a data set for a research purpose that is not sufficiently compatible with the original purpose of use, the data subjects need to be informed. From the CLARIN perspective, it is a practical question whether the CLARIN Centre as a processor is commissioned to inform the data subjects or the original controller notifies them, and how one goes about informing them in practice, i.e. will personal communication be possible or is a public announcement sufficient.[24]

6 Conclusion

The language research community is aware of personal data protection. At the same time, it is not clear who has to guarantee the GDPR compliance, which contractual arrangements are needed and what the legal consequences and remedies are in case of non-compliance. The following graph summarises the main analysed aspects concerning the sharing of the data:

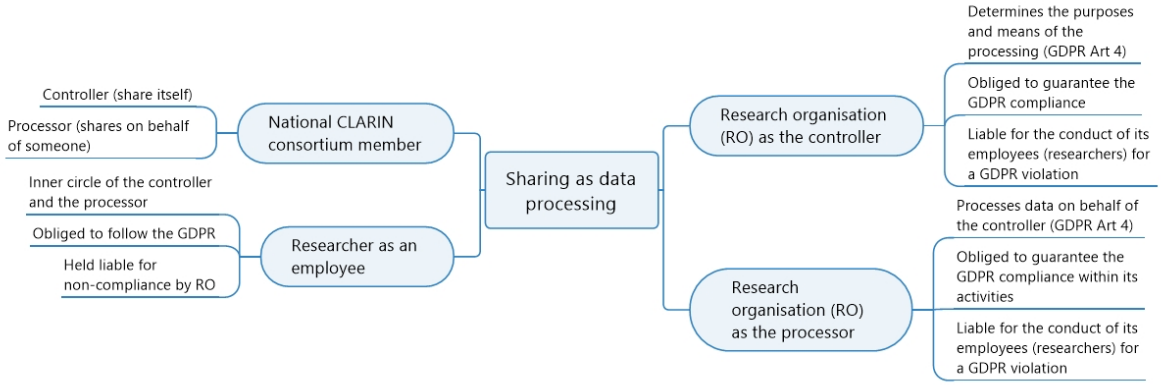

Figure 1. Sharing as data processing

According to the GDPR, the controller is the main responsible party since the controller "*determines the purposes and means of the processing of personal data"* (GDPR Art. 4 (7)). In academic settings, it is not always clear who the controller is. It should also be emphasised that a key feature of academic settings is academic freedom. Therefore, the relevant question is whether the university or an individual researcher is the controller? To answer the question, the authors analysed regulations, policy documents and case law to determine a general framework. Additionally, the authors conducted small case studies in several countries. Generally speaking, the issue is not settled yet. However, it can be assumed that the tendencies are that the university is considered the controller. There are practical reasons for this approach. Firstly, despite academic freedom, the university still controls and directs its employees. Secondly, the university has more resources to compensate for possible damage to the data subject and to take measures ensuring that the damage does not occur.

Researchers are not usually considered controllers. This does not mean that they are not responsible for their actions. In the case of a GDPR violation, they have to answer to their host universities.

[24] It seems to depend on whether the data were collected from the data subject (Art. 13 has only one exception to the obligation to provide information) or not (Art. 14 considers impossibility or disproportionate effort).

The authors also explored the relations between controllers and joint controllers. This may be relevant when two or more universities jointly conduct research (collect data, share it, etc.). The main conclusion is that controllership is not anything that can be contractually determined. It is a factual question. It is crucial that processing PD is transparent for the data subject.

In some case, the controller could use assistance in processing PD. The assisting party is called the processor when the assistance is clearly defined and limited. For example, this could be the case when another party is asked to help to structure or share data. To protect the data subject, the GDPR has several mandatory requirements, which are discussed in the article.

There is always a possibility that something goes wrong and someone's rights are violated. Therefore, the article also covers legal remedies in case of non-compliance with the GDPR. Since remedies and violations are two sides of the same coin, it was necessary to cover some obligations of the controller as well. One of the conclusions is that the controller has to demonstrate the GDPR compliance and take all possible measures to avoid harm to the data subject. Acting in good faith is a starting point.

The last section aimed to preliminarily place the previous analysis in the CLARIN context. Sharing language data within CLARIN requires specific arrangements depending on the nature of the relationship between the contractual parties. If a third party deposits data with a CLARIN consortium member, then the third party is the controller and the CLARIN consortium member is the processor. If a CLARIN consortium member shares data on its own behalf, it is the controller.

Several contractual arrangements are needed for sharing language data. However, the main reason for a CLARIN consortium member to be the controller of the PD is that researchers are often very mobile. Sometimes they no longer stay in academia, and sometimes researchers pass away. If someone needs access to the data later, a CLARIN Centre can still carry on with that role. Even if the researcher no longer is in a position to grant access to the data, the data is accessible also with a CLARIN Centre in a joint controller position where both a CLARIN Centre and the researcher separately have control of the data.

References

[Aalto University] Aalto University. How to handle personal data in research? Available at https://www.aalto.fi/en/services/how-to-handle-personal-data-in-research (18.1.2021).

[Act UWA] Foundation of the University of West Attica and other provisions. Act 4521/2018. Available at https://www.kodiko.gr/nomothesia/document/345491/nomos-4521-2018 (27.1.2021).

[AUEB] Regulation of Principles and Operation of the Research Ethics Committee of the Athens University of Economics and Business. Available at http://rc.aueb.gr/el/static/home (13.3.2021).

[AUTH] Regulation of Principles and Operation of the Research Ethics Committee of the Aristotle University of Thessaloniki. Available at https://www.rc.auth.gr/Documents/Uploaded/b4498638-1d32-45c9-b380-ec88ec6d143d.PDF (27.1.2021).

[Bari University] Regolamento in materia di protezione dei dati personali in attuazione del Regolamento UE 2016/679 del Decreto Legislativo 30 giugno 2003, n. 196 Codice in materia di Protezione dei Dati personali. Available at https://manageweb.ict.uniba.it/ateneo/bollettino-ufficiale/Regolamento_protezione_dati_dr1587_13032019.pdf (27.1.2021).

[C-311/18] Case C-311/18. Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (16 July 2020). Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1598506855221&uri=CELEX:62018CJ0311 (17.3.2021).

[C-40/17] Case C-40/17. Fashion ID GmbH & Co. KG *vs*. Verbraucherzentrale NRW eV, interveners: Facebook Ireland Ltd, Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (29 July 2019). Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1587057502926&uri=CELEX:62017CJ0040 (17.3.2021).

[C-25/17] Case C-25/17. Tietosuojavaltuutettu, intervening parties: Jehovan todistajat (10 July 2018). Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1587066001018&uri=CELEX:62017CJ0025 (17.3.2021).

[C-22/98] Case C-22/98. Criminal proceedings against Jean Claude Becu, Annie Verweire, Smeg NV and Adia Interim NV (16 September 1999). Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1587999262601&uri=CELEX:61998CJ0022 (17.3.2021).

[C-66/85] Case C-66/85. Deborah Lawrie-Blum *vs*. Land Baden-Württemberg (3 July 1986). Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1587999733855&uri=CELEX:61985CJ0066 (17.3.2021).

[C-256/01] Case C-256/01. Debra Allonby v Accrington & Rossendale College, Education Lecturing Services, trading as Protocol Professional and Secretary of State for Education and Employment (13 January 2004). Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1587999966374&uri=CELEX:62001CJ0256 (17.3.2021).

[CNRS guide 2019] CNRS Les sciences humaines et sociales et la protection des données à caractère personnel dans le contexte de la science ouverte. GUIDE POUR LA RECHERCHE. Available at https://inshs.cnrs.fr/sites/institut_inshs/files/pdf/guide-rgpd_2.pdf (17.3.2021).

[Constitution of the Italian Republic] Costituzione della Repubblica Italiana. Available at https://www.cortecostituzionale.it/documenti/download/pdf/Costituzione_della_Repubblica_italiana.pdf (16.3.2021).

[Cordeiro 2019] Cordeiro, António Menezes. Civil liability for processing of personal data in the GDPR. European Data Protection Law Review 2019/5(4), 492-499.

[CoDAU guidelines] Convegno dei Direttori generali delle Amministrazioni Universitarie (CoDAU). Linee guida in materia di privacy e protezione dei dati personali in ambito universitario. Versione 1.1 – novembre 2017. Available at http://www.codau.it/sites/default/files/verbali/all_3_linee-guida_privacy_gdpr_ravera.pdf (27.1.2021).

[CRUI regulations] Regolamento in materia di protezione dei dati personali in attuazione del Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio e del decreto legislativo 30 giugno 2016, n. 196 Codice in materia di protezione dei dati personali. Available at https://www.fondazionecrui.it/wp-content/uploads/2019/02/bozza_schema_regolamento_privacy.pdf (27.1.2021).

[DP Handbook 2018] European Union Agency for Fundamental Rights and Council of Europe (2018). Handbook on European data protection law 2018 edition. Available at https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf (17.3.2021).

[Data Protection Policy] Data Protection Policy of the University of Tartu. Available at https://www.ut.ee/en/data-protection-policy (17.3.2021).

[Description] Order No. R-316 of the Rector of the University of Vilnius of 25 May 2018 concerning the approval of the description of the procedure of personal data processing at the University of Vilnius. Available at https://www.vu.lt/en/privacy-policy#general-provisions (18.1.2021).

[EC] European Commission. What is a data controller or a data processor? Available at https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en (17.3.2021).

[EDPB 2020] European Data Protection Board. Guidelines 07/2020 on the concepts of controller and processor in the GDPR. Version 1.0. Adopted on 02 September 2020. https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf (16.03.2021).

[EPRS study 2019] European Parliamentary Research Service. How the General Data Protection Regulation changes the rules for scientific research. July 2019. Available at https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634447/EPRS_STU(2019)634447_EN.pdf (17.3.2021).

[European Parliament 2018] European Parliament (2018). Parliamentary questions. Available at https://www.europarl.europa.eu/doceo/document/E-8-2018-003163-ASW_EN.html (17.3.2021).

[EU Charter of Fundamental Rights] Charter of Fundamental Rights of the European Union. 2012/C 326/02. OJ C 326, 26.10.2012, p. 391-407. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT (17.3.2021).

[FORTH] Research Ethics committee of the Foundation for Research and Technology-Hellas. Available at https://www.forth.gr/index_main.php?c=46&l=g&s=&p=1 (27.1.2021).

[French Universities Guidelines 2019] Université Paris Lumières, Université Paris Nanterre, Université Paris 8, Règlement général pour la protection des données. Fiches pratiques à destination des chercheurs. Available at: http://triangle.ens-lyon.fr/IMG/pdf/guide_rgpd_2019_web.pdf (17.3.2021).

[GDPR] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). OJ L 119, 4.5.2016, p. 1-88. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1555312258399&uri=CELEX:32016R0679 (17.3.2021).

[Guidance 2019] Data Protection Commission (2019). Guidance on Anonymisation and Pseudonymisation. Available at https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190614%20Anonymisation%20and%20Pseudonymisation.pdf (23.3.2021).

[HEA] Higher Education Act (Kõrgharidusseadus). Entry into force 1.09.2019. Available at https://www.riigiteataja.ee/en/eli/525062020001/consolide (27.1.2021)

[ICO 2012] Information Commissioner's Office (2012). Anonymisation: managing data protection risk code of practice. Available at https://ico.org.uk/media/1061/anonymisation-code.pdf (23.3.2021).

[Kelli et al. 2019] Aleksei Kelli, Krister Lindén, Kadri Vider, Pawel Kamocki, Ramunas Birštonas, Silvia Calamai, Penny Labrpolou, Maria Gavrilidou, Pavel Straňák (2019). Processing personal data without the consent of the data subject for the development and use of language resources. In: Inguna Skadina, Maria Eskevich (Ed.). Selected papers from the CLARIN Annual Conference 2018. Linköping University Electronic Press, 72-82. Available at http://www.ep.liu.se/ecp/159/008/ecp18159008.pdf (17.3.2021).

[Kelli et al. 2018] Aleksei Kelli, Krister Lindén, Kadri Vider, Penny Labropoulou, Erik Ketzan, Pawel Kamocki, Pavel Straňák (2018). Implementation of an Open Science Policy in the context of management of CLARIN language resources: a need for changes? In: Maciej Piasecki (Ed.). Selected papers from the CLARIN Annual Conference 2017. Linköping University Electronic Press, 102-111. Available at http://www.ep.liu.se/ecp/147/009/ecp17147009.pdf (17.3.2021).

[Kelli et al. 2015] Aleksei Kelli, Kadri Vider, Krister Lindén (2015). The Regulatory and Contractual Framework as an Integral Part of the CLARIN Infrastructure. In: Koenraad De Smedt (Ed.). Selected Papers from the CLARIN Annual Conference 2015. Linköping University Electronic Press, 13-24. Available at http://www.ep.liu.se/ecp/article.asp?issue=123&article=002 (17.3.2021).

[Klavan et al. 2018] Jane Klavan, Arvi Tavast, Aleksei Kelli (2018). The Legal Aspects of Using Data from Linguistic Experiments for Creating Language Resources. Frontiers in Artificial Intelligence and Applications, 307, 71 −78. Available at http://ebooks.iospress.nl/volumearticle/50306 (28.1.2021).

[Landesgericht Karlsruhe 2019] LG Karlsruhe, Urteil vom 02.08.2019-8 O 26/19. OpenJur 2020, 69001. Available at https://openjur.de/u/2293311.html (17.3.2021).

[Lindén et al. 2020] Krister Lindén; Aleksei Kelli, Alexandros Nousias (2020). A CLARIN Contractual Framework for Sharing Personal Data for Scientific Research. In: Kiril Simov, Maria Eskevich (Ed.). Selected Papers from the CLARIN Annual Conference 2019 (75−84). Linköping University Electronic Press. Available at https://ep.liu.se/en/conference-article.aspx?series=ecp&issue=172&Article_No=10 (28.1.2021).

[Lindén et al. 2019] Krister Lindén, Aleksei Kelli, Alexandros Nousias, (2019). To Ask or not to Ask: Informed Consent to Participate and Using Data in the Public Interest. Proceedings of CLARIN Annual Conference 2019: CLARIN Annual Conference, Leipzig, Germany, 30 September – 2 October 2019. Ed. K. Simov and M. Eskevich. CLARIN, 56-60. Available at https://office.clarin.eu/v/CE-2019-1512_CLARIN2019_ConferenceProceedings.pdf (17.3.2021).

[Modena and Reggio Emilia University] Modena e Reggio Emilia University Regolamento in materia di protezione dei dati personali in attuazione del Regolamento UE 2016/679 del Parlamento Europeo e

del Consiglio e del Decreto Legislativo 30 giugno 2003, n. 196 Codice in materia di Protezione dei Dati personali. Available at https://www.unimore.it/hreg/RegolamentoPrivacy.pdf (27.1.2021).

[NCSR] Regulation of Principles and Operation of the Research Ethics Committee of the National Centre of Social Research. Available at https://www.ekke.gr/uploads/announcements/privacy policy/fek ekke privacy policy.pdf (27.1.2021).

[Oksanen et al. 2010] Ville Oksanen, Krister Lindén, Hanna Westerlund (2010). Laundry Symbols and License Management: Practical Considerations for the Distribution of LRs based on experiences from CLARIN' in Proceedings of LREC 2010: Workshop on Language Resources: From Storyboard to Sustainability and LR Lifecycle Management. Available at https://helda.helsinki.fi/handle/10138/29359 (17.3.2021).

[Oberlandesgericht Dresden 2019] Oberlandesgericht Dresden 2019, Beschluss v. 11.06.2019 - Az.: 4 U 760/19. Available at https://www.datenschutz.eu/urteile/Bei-bloßen-Bagatellverstoeßen-ohne-ernsthafte-Beeintraechtigung-fuer-das-Selbstbild-oder-Ansehen-einer-Person-besteht-kein-Schadensersatzanspruch-nach-Art-82-DSGVO-Dresden-Oberlandesgericht-2019061 (27.01.2021).

[ORDA] Organisation of Research and Development Act (Teadus- ja arendustegevuse korralduse seadus). Entry into force 02.05.1997. Available at https://www.riigiteataja.ee/en/eli/503062019008/consolide (17.3.2021).

[PDPA] Personal Data Protection Act (Isikuandmete kaitse seadus). Entry into force 15.01.2019. Available at https://www.riigiteataja.ee/en/eli/523012019001/consolide (17.3.2021).

[PDPC] Personal Data Protection Code containing provisions to adapt the national legislation to 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. Available at https://www.garanteprivacy.it/documents/10160/0/Data+Protection+Code.pdf/7f4dc718-98e4-1af5-fb44-16a313f4e70f?version=1.3 (17.3.2021).

[Pormeister 2020] Kärt Pormeister (2020). Transparency in Relation to the Data Subject in Genetic Research - an Analysis on the Example of Estonia. Doctoral dissertation. Irene Kull; Jaak Vilo; Katrin Õunap; Barbara Evans (sup). University of Tartu. Available at https://dspace.ut.ee/handle/10062/66697 (17.3.2021).

[Rechtbank 2020] Rechtbank Noord-Nederland, 15-01-2020, C / 18 / 189406 / HA ZA 19-6. Available at https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBNNE:2020:247 (17.3.2021).

[Riigikohus 2010] Riigikohtu tsiviilkolleegium, 9. detsember 2010, otsus nr 3-2-1-127-10. Available at https://www.riigikohus.ee/et/lahendid?asjaNr=3-2-1-127-10 (17.3.2021).

[RTDI] Research, Technological Development and Innovation Act and other provisions. Act 4310/2014. Available at https://www.kodiko.gr/nomothesia/document/100926/nomos-4310-2014 (17.3.2021).

[Risak & Dullinger 2018] Martin Risak, Thomas Dullinger. The Concept of ' Worker' in EU Law: Status Quo and Potential for Change. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract id=3190912 (17.3.2021).

[Rules for processing PD 2015] The Rules concerning the processing of personal data for scientific purposes at Vilnius University of 23 November 2015. Available at https://www.vu.lt/teises-aktai (18.1.2021).

[Sartor 2018] Nicolas Sartor (2018). Data Compliance in the GDPR – How anonymization allows you to stay compliant in your data analysis. Available at https://aircloak.com/data-compliance-in-the-gdpr/ (23.3.2021).

[Schwartmann 2019] Rolf Schwartmann. Wer schützt die Forschungsdaten? Frankfurter Allgemeine Zeitung, 23 September 2019. Available at: https://www.faz.net/-hfh-9ri6m (3.2.2021).

[Sein et al. 2018] Karin Sein, Monika Mikiver, Paloma Krõõt Tupay (2018). Pilguheit andmesubjekti õiguskaitsevahenditele uues isikuandmete kaitse üldmääruses. Juridica 2, 94-115.

[SOQI] Structure, operation, quality assurance of studies and internationalisation of higher education institutes. Act 4009/ 2011. Available at https://www.kodiko.gr/nomothesia/document/120922 (27.1.2021)

[Strugala 2020] Strugala, Radoslaw. Art. 82 GDPR: Strict Liability or Liability Based on Fault? European Journal of Privacy and Law&Technologies (*EJPLT*). Special issue, 2020, 71-79.

[Truli 2018] Emmanuela Truli. The General Data Protection and Civil Liability, Chapter 12 In: Mohr Backum et al., Personal Data in Competition, Consumer Protection and Intellectual Property: Towards a Holistic Approach? Springer Verlag 2018, 303-329.

[Turin University] Turin University Regolamento in materia di protezione dei dati personali in attuazione del Regolamento UE 27 aprile 2016, n. 679 del Parlamento Europeo e del Consiglio e del Decreto Legislativo 30 giugno 2003, n. 196 Codice in materia di Protezione dei Dati personali. Available at https://www.unito.it/sites/default/files/reg_protezione_dati_personali_870_2019.pdf (27.1.2021).

[University of Cologne] Universität zu Köln, Stabsstelle 02.3 - Datenschutz und IT-Sicherheit, Forschungsdatenschutz. Available at: https://verwaltung.uni-koeln.de/stabsstelle02.3/content/forschungsdatenschutz/index_ger.html (17.3.2021).

[Universities Act of Finland]. Universities Act of Finland. 558/2009. English translation available at https://www.finlex.fi/en/laki/kaannokset/2009/en20090558_20160644.pdf (18.1.2021).

[University of Helsinki] University of Helsinki. Research data management. Available at https://www.helsinki.fi/en/research/services-for-researchers-and-research-policy/research-data-management (18.1.2021)

[University of Jyväskylä] University of Jyväskylä. Instructions for researchers. Available at https://www.jyu.fi/en/university/data-privacy/tietosuojaohjeet/researchers (18.1.2021).

[UoC] Regulation of Principles and Operation of the Research Ethics Committee of the University of Crete. Available at https://www.ehde.uoc.gr/index.php/el/157-category-leitourgia-epitrophs/384-kwdikas-deontologias-gr-2 (27.1.2021).

[UoM] Code of the Research Ethics Committee of the University of Macedonia. Available at https://www.uom.gr/ethics/kodikas-hthikhs-kai-deontologias-ths-episthmonikhs-ereynas (27.1.2021).

[UoP] Code of the Research Ethics Committee of the University of Peloponnese. Available at https://elke.uop.gr/?page_id=2194 (27.1.2021).

[UoPa] Code of the Ethics Committee for Scientific Research of the University of Patras. Available at https://ehde.upatras.gr/wp-content/uploads/2020/11/kodikas_hthikis_kai_deontologias_pp-1.pdf (27.1.2021).

[UoT] Regulation of Principles and Operation of the Research Ethics Committee of the University of Thrace. Available at https://ethics.duth.gr/ (13.3.2021).

[UT Data Protection Policy] University of Tartu. Data Protection Policy. Available at https://www.ut.ee/en/data-protection-policy (27.1.2021).

[UTA] University of Tartu Act (Tartu Ülikooli seadus). Entry into force 21.03.1995. Available at https://www.riigiteataja.ee/en/eli/527122019004/consolide (27.1.2021).

[UWA] Code of Research Ethics and Conduct Committee. Available at https://research-ethics-comittee.uniwa.gr/kodikas-deontologias/ (27.1.2021).

[Van Alsenoy 2016] Brendan Van Alsenoy (2016). Liability under EU Data Protection Law. From Directive 95/46 to the General Data Protection Regulation. Journal of Intellectual Property, Information Technology and Electronic Commerce Law 7, 271-288. Available at https://www.jipitec.eu/issues/jipitec-7-3-2016/4506 (3.02.2021).

[WP29 2014] WP29. Opinion 05/2014 on Anonymisation Techniques Adopted on 10 April 2014. Available at http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf (23.4.2021).

[WP29 2010] Article 29 Working Party. Opinion 1/2010 on the concepts of "controller" and "processor". Adopted on 16 February 2010. Available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf (17.3.2021).

[WP29 2006] Article 29 Working Party. Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT). Adopted on 22 November 2006. Available at https://www.dataprotection.ro/servlet/ViewDocument?id=234 (27.4.2021).

[Wybitul, Haß & Albrecht 2018] Wybitul, Tim, Haß, Detlef, Albrecht, Jan Philipp. Abwehr von Schadensersatzansprüchen nach der Datenschutz-Grundverordnung. NJW 2018/3, 113-117.