# Chapter 5
# The EU's General Data Protection Regulation (GDPR) in a Research Context


**Christopher F. Mondschein and Cosimo Monda**

## 5.1 Introduction

The EU's General Data Protection Regulation (GDPR).[1] has entered into force on 25 May 2018.[2] It replaces the EU's previous legal framework that dates back to 1995; while retaining the overall regulatory approach of its predecessor, the GDPR also introduces a number of new compliance obligations, including higher sanctions than those available under the previous framework.[3] This Chapter introduces the key concepts of data protection law and specifically those of the GDPR to the readership in order to sensitize the readership to this matter. A basic understanding of the telos of the GDPR and the way it strives to achieve the regulatory goals set therein can help researchers understand what compliance tasks will become necessary. The importance of data protection and compliant research has become apparent: the lack

[1] 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), [2016] OJ L 119/1.

[2] Article 99 GDPR.

[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, [1995] OJ L 281/31.

C. F. Mondschein (✉) · C. Monda
Maastricht European Centre on Privacy and Cybersecurity (ECPC), Faculty of Law, Maastricht University, Maastricht, The Netherlands
e-mail: c.mondschein@maastrichtuniversity.nl



P. Kubben et al. (eds.), *Fundamentals of Clinical Data Science*,
https://doi.org/10.1007/978-3-319-99713-1_5

of compliance will inevitably lead to problems with obtaining funding for research, especially through European Union grants.[4]

This chapter will hardly succeed in making the reader an expert on data protection law or the GDPR, given that volumes of books could be filled on this topic. Nevertheless, awareness of the compliance goals and a basic understanding of the functioning of the GDPR can give researchers an edge in identifying and flagging issues at an early stage in their research endeavours. It also aids research organizations in assessing their internal procedures. Here, the presence of a supporting infrastructure for researchers that is able to support them in achieving legal compliance and through which issues can be address at an early stage is an important factor; researchers by themselves hardly can be expected to be GDPR experts.

Considering data protection issues at an early stage of a research project is of great importance specifically in the context of large-scale research endeavours that make use of personal data. In clinical settings, this often includes special categories of personal data, also referred to as sensitive data, that are collected from a wide array of sources (see Chap. 1 of this book) and which can be combined to gain novel insights. In this context, the development of clinical data standards – as described in Chap. 3 of this book – supporting the FAIR principles[5] and ensuring interoperability and shareability pose a potential risk for a data protection perspective, if legal compliance is not assured.

We approach these issues in the following manner:

(i) we introduce the basic tenets of EU data protection law;
(ii) we give a broad overview of the GDPR and its principles, actors and mechanisms;
(iii) we contextualize the research exemption included in Article 89 of the GDPR.

## 5.2 Data Protection Law in the EU

EU data protection law stands on a dual footing: on the one hand, it strives to facilitate the free flow of personal data; on the other hand, it makes the free flow of personal data subject to conformity with legal requirements that are derived from the fundamental rights character of the right to privacy and the right to the protection of personal data of individuals.[6] The fundamental rights character of EU data protection law is anchored in the Charter of Fundamental Rights of the European Union

[4] See Frischhut [1]. In the context of the Horizon 2020 framework, data protection plays a crucial role in the ethics assessment, see European Commission DG Research & Innovation, 'Horizon 2020 Programme: Guidance. How to complete your ethics self-assessment'. Version 5.3. 21 February 2018, http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf

[5] Wilkinson et al. [2, 3].

[6] Article 1(2) and (3) GDPR. Lynskey [4], Ch. 3.

(the Charter), which provides for the right to privacy (Article 7 of the Charter) and the right to the protection of personal data (Article 8 of the Charter).[7]

The right to the protection of personal data demands that personal data be only processed in a lawful and transparent manner, following a set of principles that ensure that the data subject (i.e. the individual whose data is processed) can effectively make use of a number of rights vis-á-vis the entities processing his/her personal data. This is ensured through supervision by independent supervisory authorities at the national level.

The fundamental rights nature of this right necessitates a case-by-case analysis of each processing operation, balancing a wide array of fundamental rights and the interests of the data subject and other stakeholders. This explains the general complexity surrounding data protection when viewed through a regulatory compliance lens.

## 5.3 The GDPR

The GDPR operationalizes data protection under the dual footing described above. It retains many elements contained in its predecessor and adds certain elements, most notably a more severe sanctioning regime, the right to be forgotten and the mandatory assignment of a Data Protection Officer (DPO) for certain processing situations.

The GDPR takes an'omnibus' approach,[8] meaning that it applies as a general law encompassing a wide scope of processing operations and actors (both public bodies and private organizations) and applies a wide definition of what constitutes the processing personal data. This can be contrasted with the US legal framework, which takes a sectoral approach, for example by separately regulating children's privacy or insurance and health privacy, yet lacking an overall (federal) data protection law.[9]

The EU legislator chose to continue the use of a principle- and rights-based approach for the GDPR, which takes a technological neutral perspective. This is connected with the omnibus nature of the GDPR: in order to retain its wide scope, the GDPR utilizes general principles from which compliance has to be deduced by the processing entities under a so-called 'risk-based approach'; this means that organizations must self-assess their operations and take the necessary steps to comply with the GDPR on an on-going basis, a ensuring that the level of compliance is proportional to the level of risk inherent to the processing operations carry. This is not to say that there is no guidance, as there are various sources that aid with the interpretation of the principles such as guidance issued by supervising authorities, case law, established practices and so on that should be used for the legal assessment

[7] For the distinction between the two rights, especially for Big Data application in the health sector, see Mostert et al. [5].

[8] Lynskey [4], p. 15 ff.

[9] Schwartz and Pfeifer [6].

of processing operations. Where this is not the case, this approach introduces a sense of legal uncertainty and requires expertise to ensure compliance. This effect is in part amplified where new technologies or processing approaches are introduced: the GDPR takes a technological-neutral approach, stating that "in order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used."[10] This potentially poses a factor of uncertainty.

The GDPR is said to introduce a higher level of harmonization of data protection law throughout the European Union. However, the fact that it contains a substantial number of opening clauses which create space for Member States to take decisions on the implementation of the GDPR at national level may undermine this attempt. Most notably, Member States may introduce specific derogation for the research exemptions under Article 89(2) GDPR, which may lead to a fragmentation of the rules governing research (see further below). It remains to be seen what level of harmonization will be reached as at the point of writing, not even all Member States have finalized the national laws implementing the GDPR.[11]

A hallmark of the GDPR is the introduction of the principle of accountability. The principle of accountability calls for entities processing personal data to take a proactive and holistic stance towards compliance with the GDPR. An accountable organization is able to prove upon request that they have taken all necessary steps to be in compliance with the GDPR.

## 5.4 Scope of Application of the GDPR

**Temporal Scope** The GDPR entered into force on 25 May 2018 (Article 99 GDPR). Any new processing operations started after this date must be considered to fall under the scope of the GDPR if they fulfil the material and territorial scope set out in Articles 4(7) and 4(8) GDPR respectively. Ongoing processing operations that were commenced before the entry into force of the GDPR are *not* grandfathered under the old legal regime and hence the GDPR also applies to these processing operations. Regarding the reuse data collected prior to the entry into force of the GDPR, an assessment whether the lawfulness criteria of the GDPR are still fulfilled is necessary (especially regarding the collection of consent).

**Material Scope** The GDPR applies to both public bodies as well as private organizations. However, distinct rules for the EU institutions, bodies and agencies exist (Article 2(3) GDPR). The GDPR applies to the processing of personal data (Article 2 GDPR).[12] Two notions have to be considered here: (i) the notion of personal data and (ii) the notion of processing. The GDPR makes use of four distinct categories to

[10] Recital 15 GDPR.

[11] See e.g. Alston & Bird, 'GDPR Tracker', https://files.alston.com/files/Uploads/gdprtracker/index.html (last visited: 03.07.2018).

[12] Article 29 WP Opinion on the concept of personal data, WP136, 20.6.2007.

make sense of the notion of personal data and to delineate legal obligations for the processing of these data:

i) Personal data
ii) Special categories of personal data
iii) Pseudonymous data
iv) Anonymous data

The *notion of personal data* in this context possesses a wide scope: it encompasses any information relating to an identified or identifiable individual. This includes names, identification numbers, location data and so on. An example of the wide scope of this notion is that dynamic IP addresses[13] fall under the definition of personal data as there are means to potentially identify the data subject through legal means that are realistic to achieve. When looking at the data sources described in Chap. 1 of this book, it becomes clear that in almost any context of clinical data science, personal data as defined by the GDPR is used.

According to Article 9 GDPR, *special categories of personal data*, also referred to as 'sensitive personal data', include (i) racial or ethnic origin, (ii) political opinions, (iii) religious or philosophical beliefs, (iv) trade union membership, (v) genetic data, (vi) biometric data, (vii) data concerning health, (viii) sex life or sexual orientation. These data carry a higher degree of risk for the data subject, thus necessitating further compliance steps for any entity processing them. Data points that can be used as proxies for certain characteristics fall within in the scope of the definition of special categories of personal data. For example, certain dietary requirements in passenger name records were deemed to be sensitive data as data subjects' religious beliefs could be inferred from them.[14] In the research context, Article 9(1)(j) GDPR offers derogations that may be introduced by virtue of EU or Member State's national law. However, Member States may also maintain or introduce hurdles in the form of specific limitations to the processing of genetic, biometric or health data (Article 9(4) GDPR). Hence, Member States have leeway to open or restrict the processing of these categories of data under the GDPR, which is something that has a potentially large impact on the way research is conducted.

*Pseudonymization* of personal data refers to the act of altering personal data to the extent that the data subject cannot be directly identied without having further information, which is stored separately (Article 4(4) GDPR). The Article 29 WP gives a number of examples for pseudonymisation techniques, including where data is (i) encrypted with a secret key; (ii) hashing and salting data; (iii) keyed-hash functions with stored key; (iv) deterministic encryption or keyed-hash functions with deletion of the key; or (v) tokenization.[15] It is important to note that pseudonymised personal data still falls within the scope of the GDPR and it is viewed as a security safeguard under the notion of technical and organizational measures (Article 32(1)(a) GDPR) but these technologies cannot be used to circumvent compliance obligations pursuant to the GDPR (see Recitals 26 and 28 GDPR).

[13] Case C-582/12 *Breyer*, EU:C:2016:779.

[14] Opinion 1/15 *EU-Canada PNR*, EU:C:2016:656.

[15] Article 29 WP Opinion on anonymisation techniques, WP216, 10.4.2014, p. 20.

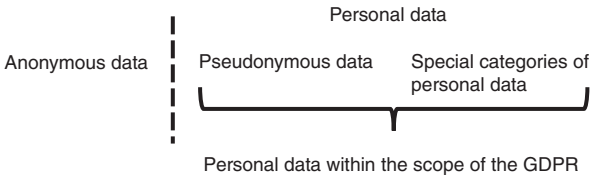


**Fig. 5.1** Categories of personal data under the GDPR

The GDPR does not contain a definition of what constitutes *anonymous data*. However, the fifth and sixth sentence of Recital 26 provide that the "principles of data protection should (…) not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes." Hence, the GDPR does not apply to anonymous data (Fig. 5.1).

This leaves the question where to draw the line between anonymous and pseudonymous data, thus determining when the GDPR applies, and when not. Spindler and Schmeichel highlight the tension between an *absolute approach* and a *relative approach* towards encrypted data and the identifiability of the data subject.[16] The former qualifies that the criterium for identifiability for encrypted data is fulfilled as long as even the remotest possibility of identifying the data subject based on the encrypted data exists, whereas the latter considers the scope of identifiability somewhat narrower, relying on the existence of a realistic opportunity of identifying the data subject. From a legal perspective, it remains to be seen how technological advancements such as fully homomorphic encryption (FHE) or secure multi-party computing (SMC) will be received, albeit it being unlikely that utilizing these technologies will create an exemption to the application of the GDPR due to the wide interpretation of the scope of personal data.[17]

When contemplating secondary use of data for research, one must take into account that the combination of different data points from different categories might lead to a shift in the classification of a processing operation. Here, a functional approach is required to make an assessment of the legal nature of the data processed, which is important in a research setting, especially when applying a Big Data approach and obtaining data from a wide array of sources for secondary use. Here, the temporal aspect of technological change must also be taken into account by asking what changes can be realistically expected in the future and how these changes might impact the processing operation.

In summary, the GDPR grants the notion of personal data a wide scope and it is difficult to argue that the GDPR does not apply by virtue of data not qualifying as personal data. The legal definition of pseudonymization under the GDPR is considerably far-ranging and circumventing compliance obligations under the GDPR by virtue of utilizing anonymous data is rather unlikely, as the usefulness of data for research purposes stands in contrast to the stringent criteria of anonymisation under the GDPR.

[16] Spindler and Schmechel [7].

[17] Spindler and Schmechel [7], p. 174–176.

**The Notion of Processing** Article 4(2) GDPR refers to processing as "[a]ny operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." This complements the broad definition the GDPR gives to the notion of personal data. In short, the notion of processing covers everything one does with personal data.

**Territorial Scope** By virtue of Article 3 of the GDPR, the GDPR applies to all processing operations of controllers or processors that are established within the EU. Here, it is not important whether the processing activities take place within the EU or not; the connecting factor triggering the application of the GDPR is the fact that the entities have a legal establishment in the EU. Next to that, the GDPR applies where personal data of data subjects located within the EU is processed by entities without an establishment in the EU if (i) it pertains to offering goods or services to data subjects within the EU, independent of whether payment is required, or (ii) the behaviour of data subjects within the EU is monitored. Lastly, the GDPR might apply where public international law so dictates. It is important to highlight that the applicability of the GDPR is not linked to nationality of a Member State or to EU citizenship but applies to all data subjects located within the EU. Within the research context it is also important to highlight that datasets imported to the EU for further processing fall within the scope of the GDPR.

## 5.5 Key Concepts of the GDPR

**Controller and Processor** The notions of controller and processor are used to delineate and assign the tasks, responsibilities and liability of entities that processes personal data under the GDPR. The notions were already present in the 1995 Directive; however, the GDPR has assigned more responsibilities to data processors. The controller is the entity which decides (or jointly together with another controller) on the purpose and the means of the processing (Article 4(7) GDPR). The processor is the entity that processes the data on behalf of the controller (Article 4(8) GDPR). These notions are used to identify obligations and liability of entities processing personal data. Numerous different combinations of controllership and processor relations are possible (controller and processor are one entity; controller and processors are separate entities; joint controllers; sub-processors; etc.). Here, it is best map the dataflow and check which entities have what role. It is important to note that as soon as a processor deviates from the instructions of a controller, the processor becomes a controller and incurs the higher level of responsibilities and liability attached to this notion. The setup and due diligence in identifying the roles in this context is of utmost importance prior to starting data processing operations.

**Principles Relating to Lawful Processing** Article 5 GDPR lays down the principles allowing for lawful processing of personal data. These principles are:

i) ***Lawfulness, fairness and transparency:*** processing of personal data is lawful when it is based on one of the six legal bases listed in Article 6 GDPR. The principles of fairness and transparency relate to the fact that data subjects must be informed in a comprehensive manner about the purpose and scope of the processing as laid down is Articles 12–14 GDPR.
ii) ***Purpose limitation:*** In line with the principle of transparency, data can only be processed for a specific purpose, which has to be communicated to the data subject. In the context of research, Article 89 GDPR provides for certain derogations if the requirements under that article are fulfilled, allowing for further processing (see further below).
iii) ***Data minimisation:*** this principle requires controllers to minimize the data they collect and keep.
iv) ***Accuracy:*** the controller is obliged to ensure the accuracy of the data.
v) ***Storage limitation:*** this principle requires controllers to specify the time limit for after which data is deleted. In the context of research, Article 89 GDPR provides for certain derogations if the requirements under that article are fulfilled (see further below).
vi) ***Integrity and confidentiality:*** this principle requires that the integrity and confidentiality of personal data is ensured. It links with the obligations of data security, having in place adequate technical and organizational measures as well as the requirement to report data breaches to the supervisory authority and/or data subjects under certain circumstances as specified in Articles 33–34 GDPR.

**Legal Basis** In order to be able to process personal data in a lawful manner, the controller must specify a legal basis for the data processing operation. There is a closed list of six legal bases to be found in Article 6 GDPR:

i) ***Consent:*** to be a lawful legal basis, consent by the data subject must fulfil the conditions listed in Article 7 GDPR. Consent must be (i) freely given, (ii) specific, (iii) informed, (iv) unambiguous, (v) and the age of consent must be fulfilled (this can vary in Member States from 13 to 16 years).[18] The consent must be given through a clear affirmative act (for example, pre-ticked boxes on a consent form are prohibited). The burden of proof to demonstrate that consent was lawfully obtained lies with the controller. Hence, good documentation and archiving of consent forms is required.
ii) ***Performance of a Contract***
iii) ***Compliance with a legal obligation***
iv) ***Vital interest of the data subject:*** the scope of vital interest must be interpreted narrowly. This legal basis for example pertains to life-threatening situations in which a data subject cannot consent to the transfer of vital medical data.
v) ***Performance of a task carried out in the public interest or in the exercise of official authority vested in the controller***
vi) ***Legitimate interest of the controller or by a third party:*** this legal basis requires an assessment of the necessity and the purpose of the processing operation as

[18] See further Article 29 WP, Guidelines on consent under Regulation 2016/679, WP259 rev.01, 10.4.2018. Kosta [8].

well as a balancing test between the interests of the data subject against those of the controller and third parties: this means that the legitimate interest of the controller and that of any stakeholder must be weighed against the interests and fundamental rights – especially data protection and privacy – of the data subject. The outcome of the balancing exercise must be that the legitimate interest of the controller or any third party *outweighs* the interests and fundamental rights of the data subject in order for the processing to be lawful under this legal basis.[19] This legal basis is not available to public authorities when fulfilling a public task.

In case the same personal data is collected for different purposes, this must be specified in a transparent way and communicated to the data subject. A granular approach is necessary in order to give effect to the data subject rights.

Regarding the choice of a legal basis, generally, consent and legitimate interest may seem as an attractive option, yet, choosing either entails a number of caveats which must be addressed. As outlined above, legitimate interest requires a prior assessment and weighing of interests and front-loads the risk (it is up to the controller to make the assessment and this assessment might be challenged at a later time, hence, when dealing with complex situations and uncertainty the risk level is increased). Consent might seem as an attractive legal basis in many situations due to the perceived ease with which it can be applied; however, consent is a volatile legal basis in the sense that consent can be withdrawn by the data subject at any time. In practice, this necessitates a consent tracking and management solution as the controller must also be able to prove that valid consent was given by the data subject. If possible, other legal bases should be given priority over consent – however, for the purpose of research, consent will most likely be the only choice as a legal basis.

**Sensitive Data and Explicit Consent** Where sensitive data are processed, the GDPR requires explicit consent from the data subject (Article 9(2)(a) GDPR). Explicit consent requires a stronger affirmative action by the data subject: "The term explicit refers to the way consent is expressed by the data subject. It means that the data subject must give an express statement of consent. An obvious way to make sure consent is explicit would be to expressly confirm consent in a written statement. Where appropriate, the controller could make sure the written statement is signed by the data subject, in order to remove all possible doubt and potential lack of evidence in the future."[20] However, the controller can also rely on other means such as a two-step verification or the "data subject may be able to issue the required statement by filling in an electronic form, by sending an email, by uploading a scanned document carrying the signature of the data subject, or by using anelectronic signature".[21]

**Data Subject Rights** Data subjects have a number of rights vis-à-vis entities processing personal data.

[19] Article 29 WP Opinion on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP217, 9.4.2014.

[20] Article 29 WP, Guidelines on consent under Regulation 2016/679, WP259 rev.01, 10.4.2018, p. 18.

[21] Article 29 WP, Guidelines on consent under Regulation 2016/679, WP259 rev.01, 10.4.2018, p. 18–19.

i) Right to transparent information, communication and modalities to exercise rights
ii) Right to information relating the processing (both where data is obtained by first and third parties)
iii) Right to access of one's personal data
iv) Right to rectification, erasure and restriction of processing
v) Right to data portability
vi) Right to object

**Compliance** In order to be accountable, entities processing personal data must fulfil a set of compliance criteria. Most fundamentally, they must adhere to the data protection principles when processing personal data. In relation to the data subject, the entities processing personal data must enable and effectuate data subject rights; this includes responding to data subject requests for access and informing data subjects on the processing in a fair and transparent manner. According to Article 30 GDPR, controllers and processor are required to keep documentation of the processing operations and must be able to demonstrate compliance on request of the supervisory authority. In line with the risk-based approach taken by the GDPR, it might become necessary to consult the supervisory authority prior to commencing a risky processing operation (Article 36 GDPR). In case a processing operation is deemed to have a high risk, the controller must conduct a data protection impact assessments (DPIAs) prior to commencing processing (Article 35 GDPR). Processing operations that potentially have a high risk attached to them include operations where new technologies are used (e.g. Big Data approaches), and based on factors such as the nature, the scope, the context and purpose of the processing. Article 35 GDPR specifically mentions the processing and systematic and extensive evaluation of persons, including profiling as well as the large-scale monitoring of public areas. Important for the research context is that the large-scale processing of sensitive data requires a DPIA (Article 35(3)(b) GDPR). Such risky operation potentially must be notified to the supervisory authority. In line with the principle of integrity and confidentiality, controllers and processors must ensure security of the personal data (Article 32 GDPR): the extent of the technical and organizational measures that will be required to secure personal data depends on a number of factors as the entities processing personal data must take "into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons". Next to this, the GDPR introduces the notions of *privacy by design* and *privacy by default* (Article 25 GDPR).

**Appointment of a DPO** Controllers and processors must appoint a DPO under certain conditions (Article 37 GDPR): (i) In case the processing operation is carried out by a public body, (ii) "the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale", (iii) the processing of special categories of personal data (Article 9 GDPR) or data relating to criminal offences (Article 20 GDPR). The Article 29 WP issued

guidelines on these matters.[22] An example to contrast where the designation of a DPO becomes necessary in the medical field: a DPO is necessary for processing of patient data in the regular course of business by a hospital; a DPO is not necessary where patient data is processed by an individual physician; where there is a joint practice of physicians, the appointment of a DPO becomes necessary.[23]

Regarding the position of the DPO, it is important to note that the DPO has an advisory function and is not personally responsible for non-compliance with the GDPR. Regarding the appointment of a DPO, a possible conflict of interest must be avoided where the DPO also holds another position in the organization; to that extent, a DPO cannot at the same time hold a leadership role (for example, "chief executive, chief operating, chief financial, chief medical officer, head of marketing department, head of Human Resources or head of IT departments").[24]

**Transfers to Third Countries** The general approach regarding the transfer of personal data from the EU to any third country is that it is prohibited unless there is one of the following measures in place:

i) Adequacy decision
ii) Binding Corporate Rules (BCRs)
iii) Model Contract Clauses
iv) Explicit Consent
v) (Derogations)

Since this provision functions as a prohibition with a closed list of exemptions, any transfer of personal data from the EU to a third country must fall within the scope of one of these exemptions in order to be deemed lawful (Fig. 5.2).

## 5.6 The GDPR's Research Exemption

The GDPR acknowledges the need to facilitate different types of research, citing scientific and historical research, statistical research, and archiving in the public interest (Article 89 GDPR).

The GDPR does not contain a formal definition of what constitutes scientific research. It applies a wide definition to the notion of research, stating that "the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research."[25] In the clinical research context, the relation between the GDPR and the Clinical Trials

[22] Article 29 WP, Guidelines on Data Protection Officers ('DPOs'), WP243 rev.01, 5.4.2018.
[23] Article 29 WP, Guidelines on Data Protection Officers ('DPOs'), WP243 rev.01, 5.4.2018, p. 16.
[24] Article 29 WP, Guidelines on Data Protection Officers ('DPOs'), WP243 rev.01, 5.4.2018, p. 24.
[25] Recital 159 GDPR.

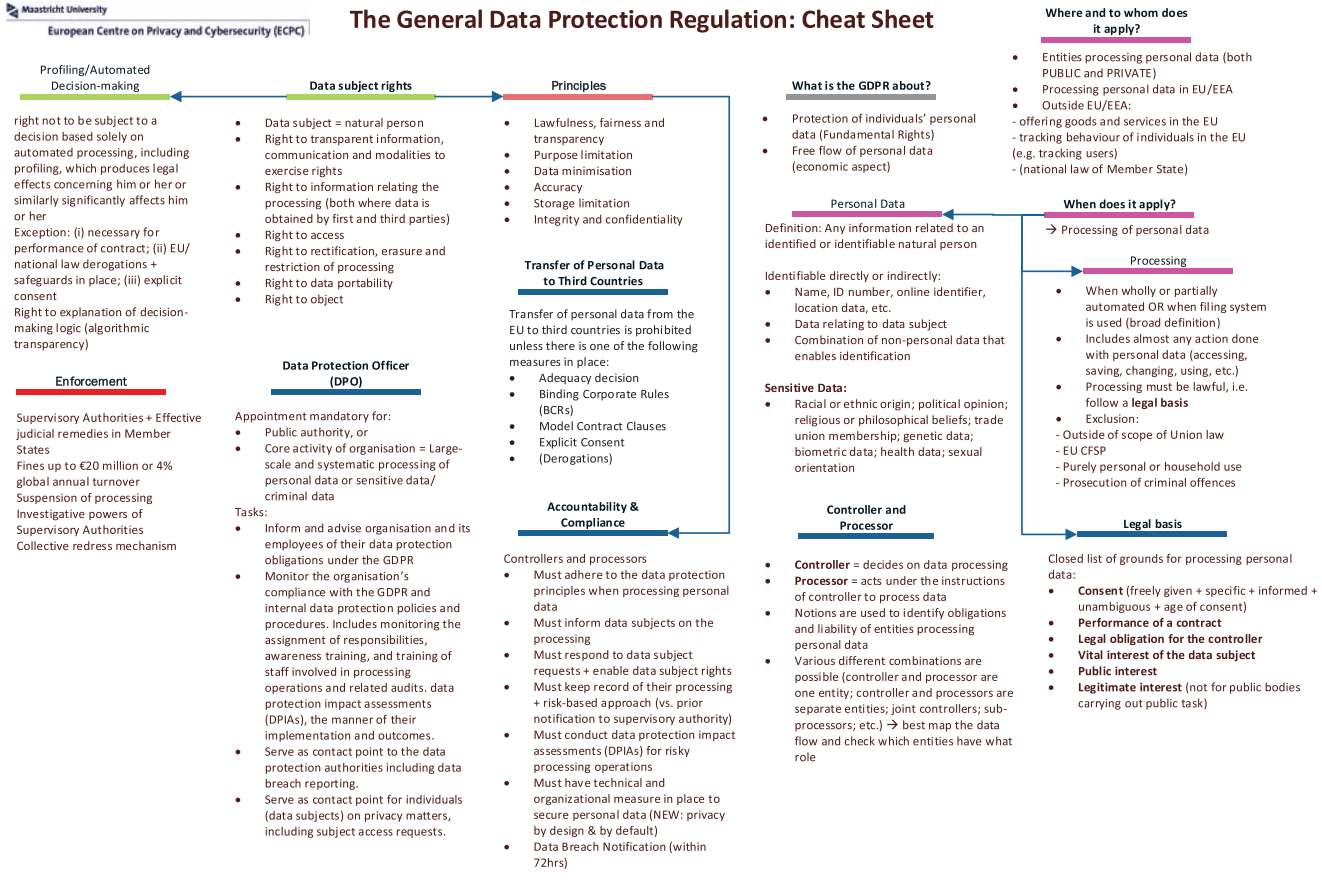


**Fig. 5.2** ECPC GDPR cheat sheet

Regulation (CTR)[26] has to be specified: the CTR contains specific rules for a wide variety of clinical trial settings (Article 2(2)(1)–(4) CTR). In this context, the CTR requirement to collect informed consent for clinical trials falling within the scope of the CTR applies as *lex specials* to the GDPR. The CTR allows for broad consent for clinical trials that fall within the scope of the CTR and if so permitted at in the Member States.[27]

Regarding the secondary or further use of data collected during clinical trials, the CTR states that "[i]t is appropriate that universities and other research institutions, under certain circumstances that are in accordance with the applicable law on data protection, be able to collect data from clinical trials to be used for future scientific research, for example for medical, natural or social sciences research purposes. In order to collect data for such purposes it is necessary that the subject gives consent to use his or her data outside the protocol of the clinical trial and has the right to withdraw that consent at any time. It is also necessary that research projects based on such data be made subject to reviews that are appropriate for research on human data, for example on ethical aspects, before being conducted."[28] Here, the CTR makes reference to EU data protection law as the framework for further processing of personal data, now being the GDPR.

The GDPR adds to this by the stating in Recital 33 GDPR that "it is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects *should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects* to the extent allowed by the intended purpose."[29]

The GDPR provides for aresearch exemption in Article 89 GDPR, inter alia for scientific and research purposes. The exemption under the GDPR relies largely on the same discretionary framework as in the 1995 Directive.

As noted above, the scope of the notion of research under the GDPR is wide. Article 89 GDPR functions by setting a baseline in that requires that any derogation is subject to the existence of appropriate safeguards for the rights and freedoms of data subjects. Here, the GDPR stresses that safeguards shall include:

i) Data minimization;
ii) Technical and organizational measures;
iii) Privacy by Design and by Default;
iv) Pseudonymization/further processing.

[26] Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC Text with EEA relevance, [2014] OJ L 185/1.

[27] Chassang [9], p. 10.

[28] Recital 29 CTR.

[29] Emphasis added.

The respect of relevant and recognised ethical standards as well as the requirements for obtaining ethical approvals are part of these safeguards.[30] This means that any research project has to fulfil the recognized quality standards and processes required for conducting research as this is inextricably linked to the research exemption.

If these safeguards are in place, derogations to the following points may be applied:

i) Further processing and storage limitation (Articles 5(1)(b) and (e) GDPR);
ii) Processing of special categories of data (Article 9(2)(j) GDPR);
iii) Information provided by third parties (Article 14(5)(b) GDPR);
iv) Right to erasure (Article 17(3)(d) GDPR);
v) Right to object (Article 21(6) GDPR).

It is important to note that if any derogation to the points listed above is applied, this must be done by taking into account the principles of *proportionality* and *necessity*. Such assessment must be conducted before the derogations are applied and must be documented.

Next to the derogations listed above, EU or Member State law may allow for derogations on the following points:

i) The rights to access;
ii) The right to rectification;
iii) The right to restrict processing;
iv) The right to object.

The application is restricted by the requirements to also apply the safeguards mentioned above. A further qualifier is added in that any derogation must be justified by the fact that the full application of any of the rights listed rights listed above "are likely to render impossible or seriously impair the achievement of the specific purposes" and that such derogations "are necessary for the fulfilment of those purposes".[31]

Lastly, where processing personal data serves multiple purposes, one of which falling within the ambit of derogations for research as per Article 89 GDPR, the processing operations that do not fall within the scope research cannot benefit from these derogations.

It becomes obvious that the research exemption in the GDPR is quite undefined and leaves much space for interpretation by Member States. This may have an adverse effect on the scope of research that can be conducted in different Member States and may impair the function of a European Research Area.[32] Part of the problematic lies in the fact that the EU does not possess the competency to create fully harmonized rules for health and research.[33]

[30] Chassang [9], p. 11.

[31] Article 89(2) GDPR.

[32] Pormeister [10], p. 145–146.

[33] Chassang [9], p. 11.

## 5.7 Contentious Issues for Research Under the GDPR

A number of contentious issues regarding to the GDPR and research remain that we wish to discuss:

- **Modes of consent in a research context:** the scope of valid consent for research purposes under the GDPR is a contested issue. Generally, modes of consent often discussed in a research context include (i) specific, informed consent, (ii) democratic consent, (iii) dynamic consent management, (iv) sectoral consent, and (v) open/general/broad/blanket consent.[34] Broad consent requires a single affirmative action that will allow the data to be utilized for research purposes in general and without a strict temporal limitation. Especially, applying the notion of broad consent to any further processing for research purposes is a contested issue, as it clashes with the principle of purpose limitation and storage limitation. In the context of the research exemption of the GDPR, the lack of specificity arguably goes against the spirit of the GDPR and the text states that "[d]ata subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects" (Recital 33 GDPR) under certain conditions.[35] A further factor of uncertainty is that the acceptance of broad consent in the research context is largely dependent on the Member State's national implementation and in this respect may lead to a divergence within the EU. This may have a negative impact on the creation of a European Research Area as the utility of research data might vary tremendously within the EU.
- **Research purposes as a legitimate interest:** it is debated whether the legitimate interest legal basis (Article 9(1)(f) GDPR) is suitable for research purposes – bypassing the consent of the data subject when applied correctly. It is argued that the interpretation of the Article 29 WP in their Opinion on legitimate interest opens this possibility, referring to processing for research purposes – specifically marketing research – as potentially falling within the scope of the legitimate interest legal basis.[36] This is echoed in the GDPR in Recital 47, linking direct marketing and the legitimate interestlegal basis. At the same time, the balancing test required "would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place."[37] The link between research and the legitimate interest legal basis is somewhat weak. Further, the lack of experience with the legal basis and the rather unclear scope of the balancing test lead to a rather high degree of legal uncertainty as the risk assessment has to be conducted by the controller prior to the processing and any mistake, especially in the research context, might have dire consequences.

[34] Hallinan and Friedewald [11], p. 4–5.

[35] Rumbold and Pierscionek [12].

[36] G. Maldoff, 'How GDPR changes the rules for research', IAPP, https://iapp.org/news/a/how-gdpr-changes-the-rules-for-research/ (last visited 3.7.2018).

[37] Recital 49 GDPR.

## 5.8 Checklists

Prior to commencing a processing operation, one should assess the following points as a starting point:

**General**:

- What kind of information is being processed (sensitive or general)?
- What is your purpose – what are you trying to achieve?
- Can you reasonably achieve it in a different way?
- Do you have a choice over whether or not to process the data?
- Are you a public authority?

When deciding to make use of the **legitimate interest** legal basis:

- Who does the processing benefit?
- What kind of impact could processing have on the data subject?
- Are they vulnerable?
- Would individuals expect this processing to take place?
- What is your relationship with the individual?
- Are some of the individuals concerned likely to object?
- Are you able to stop the processing at any time on request?

For the application of the **research exemption**:

- Are the conditions of Article 89 GDPR met?
- Would the application of any right from with there is a derogation seriously compromise the purpose and the use of the derogations are necessary and proportional for achieving the purpose?
- Check if there are further requirements/derogations in EU or national law?
- Is the process and reasoning documented?

## 5.9 Conclusion

The GDPR requires that entities processing personal data define the personal data they wish to process as well as the purpose of the data processing operation. Processing of personal data is subject to lawfulness and entities processing data must meet compliance obligations. Entities processing personal data must facilitate the fulfilment of data subject's rights. Operating on this baseline, the processing of personal data for research purposes requires specific safeguards to ensure compliance with the GDPR. As outlined above, the secondary or further use of personal data for research is possible under certain circumstances set out in the GDPR. In this respect, it is important to reflect on the growing scale and complexity of systems applied in research and compare this to compliance aspects. The underlying regulatory ideal is to scale compliance to ensure that potential externalities created by the processing of personal data are internalized by the entities conducting these processing operations.[38]

[38] Baldwin et al. [13], p. 18.

## References


1. Frischhut M. "EU": short for "ethical" union?: the role of ethics in European Union Law. Heidelberg J Int Law. 2015;75(3):531–77.
2. Wilkinson MD, et al. The FAIR guiding principles for scientific data management and stewardship. Sci Data. 2016;3:160018. https://doi.org/10.1038/sdata.2016.18.
3. Wilkinson MD, Sansone S, Schultes E, Doorn P, Bonino da Silva Santos LO, Dumontier M. A design framework and exemplar metrics for FAIRness. Sci Data. 2018;5:180118. https://doi.org/10.1038/sdata.2018.118.
4. Lynskey O. The foundations of EU data protection law. Oxford: OUP; 2015.
5. Mostert M, Bredenoord AL, van der Slootb B, van Delden JJM. From privacy to data protection in the: implications for big data health research. Eur J Health Law. 2017;25:43–55. https://doi.org/10.1163/15718093-12460346.
6. Schwartz PM, Peifer KN. Transatlantic data privacy (November 7, 2017). 106 Georgetown Law J. 2017;115. UC Berkeley Public Law Research Paper. Available at SSRN: https://ssrn.com/abstract=3066971.
7. Spindler G, Schmechel P. Personal data and encryption in the European general data protection regulation. JIPITEC. 2016;7:163.
8. Kosta E. Consent in European data protection law. Leiden: Martinus Nijhoff Publishers; 2013.
9. Chassang G. The impact of the EU general data protection regulation on scientific research. ecancer. 2017;11:709.
10. Portmeister K. Genetic data and the research exemption: is the GDPR going too far? IDPL. 2017;2:137.
11. Hallinan D, Freidewald M. Open consent, biobanking and data protection law: can open consent be 'informed' under the forthcoming data protection regulation? Life Sci Soc Policy. 2015;11:1. https://doi.org/10.1186/s40504-014-0020-9.
12. Rumbold JMM, Pierscionek B. The effect of the general data protection regulation on medical research. J Med Internet Res. 2017;19(2):e47. https://doi.org/10.2196/jmir.7108.
13. Baldwin R, Cave M, Lodge M. Understanding regulation. Theory, strategy, and practice. 2nd ed. Oxford: OUP; 2012.