Established in 1871

Swiss Medical Weekly

Formerly: Schweizerische Medizinische Wochenschrift

An open access, online journal • www.smw.ch

Review article: Biomedical intelligence | Published 01 September 2020 | doi:10.4414/smw.2020.20332
Cite this as: Swiss Med Wkly. 2020;150:w20332

Data protection and biomedical research in Switzerland: setting the record straight

Martani Andrea[a], Egli Philipp[b], Widmer Michael[b], Elger Bernice[ac]

[a] Institute for Biomedical Ethics, University of Basel, Switzerland
[b] School of Management and Law – Centre for Social Law, Zurich University of Applied Sciences, Winterthur, Switzerland
[c] University Centre of Legal Medicine, University of Geneva, Switzerland

Summary

Ensuring the protection of privacy and the compliance with data protection rules have become central issues for researchers active in the biomedical field. Data protection law is often perceived as very complex and difficult to interpret, which can hinder the efficacious planning and implementation of new research projects. Indeed, the sophisticated legal architecture that governs data processing activities in general and biomedical research in particular might feel overwhelming for both legal practitioners and researchers.

The objective of this article is to review the interaction of data protection law and biomedical research with a predominant focus on the Swiss context. In order to facilitate a better understanding of this issue, we discuss three crucial nodes that shape the interplay of law and data processing in research First, we explore the meaning of "personal" data, the requirements to classify data as "personal", "non-personal", "pseudonymised" or "anonymised" and the implications of such classifications from a legal perspective. We then consider the relationship between sector-specific data processing regulations for research and other laws on data protection. Finally, we examine the role of consent for data processing in the research field and its significance from a data protection perspective. In conclusion, this review underlines the importance of fostering reciprocal collaboration of data protection experts and biomedical researchers to facilitate the development of new projects in the future.

Keywords: *biomedical research, data protection, personal data, bioethics, consent*

Correspondence:
Andrea Martani, Institute of Biomedical Ethics, University of Basel, Bernoullistrasse 28, CH-4056 Basel, andrea.martani[at]unibas.ch

Introduction

In the last few years, concerns about the protection of personal data have become an increasingly important subject of discussion in biomedical research. Although it could be argued that data in general, and personal data in particular, have always been a central component of research, it is only recently that discussions about the appropriate data processing standards in this field have intensified. Arguably, this could be due to two intertwined factors, one related to the research world and one to legal developments. On the one hand, due to the progressive digitalisation of healthcare, clinics, laboratories and other medical research institutions have become data-driven environments, where the processing of large amounts data has grown exponentially. Fuelled by innovative projects in fields like genomics (e.g., the human genome project [1]), neuroscience (e.g., the human brain project [2]) and by the development of precision medicine [3], the urge to accumulate vast amounts of personal data of different types has skyrocketed. This has been further intensified by the open science and open data movements in their different forms [4]. On the other hand, the law is taking an active interest in the regulation of data processing across all industries and particularly for research purposes. In the recent General Data Protection Regulation (GDPR) [5] by the European Union, for example, it is reasserted that research undoubtedly falls under the scope of data protection law and the law creates a specific "research exemption" for the processing of data for research purposes, especially in case of secondary processing [6] (see also the section "The relevance of consent for data processing in research"). In preamble[1] 159, it is firmly asserted that: "Where personal data are processed for scientific research purposes, this Regulation should also apply […]. For the purposes of this Regulation, 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."

The increasing importance of considering data protection aspects in biomedical research also holds true for Switzerland, where several projects have been put in place to facilitate the legal and ethical use of data for research. For example, fostering more comprehensive, coordinated and efficient processing of data in healthcare was one of the main objectives of the National Research Program 74 launched in 2015 by the Swiss National Science Foundation [7]. In the same spirit, the Swiss Personalised Health Network (SPHN) was recently started as a nationwide initiative with the specific mandate to leverage the potential of health-related data [8] with respect to the research sector [9]. Or else, in 2016, the Swiss Biobanking Platform was initiated to facilitate the harmonisation of biobanks and

their research work with biological material and personal data [10]. All these initiatives are designed with particular attention paid to the legal ramifications of data protection, especially in reference to Switzerland's specific legislation for processing personal data in the research sector (the Human Research Act - HRA [11], see below). Issues related to the legal ramifications of data protection in relation to scientific research are also likely to remain a central concern for the scientific community in the future, since a revised version of the Federal Act on Data Protection (FADP [12]) is currently being discussed [13] (for the relationship between FADP and HRA, see below).

Within this context of biomedical research and data protection law, the latter is often perceived as a potential hindrance from the perspective of researchers. In international reports on the status quo of the health-data framework of Switzerland and other developed countries, it is often referenced to as "legal barriers" (e.g., [14]). Indeed, even in interviews with national stakeholders conducted for our ongoing research on the health-data framework in Switzerland[2] [15], a common complaint from researchers was that navigating data protection rules is demanding. *Prima facie*, such observation appears to have some factual basis. In Switzerland alone there are 26 different data protection regulations (the FADP and 25 cantonal data protection laws – the cantons of Jura and Neuchatel have a common data protection bill [16]), a law on biomedical research, several other sectorial regulations containing norms about personal data processing, and even additional rules related to data processing in the criminal code (see below). It is understandable that researchers in the biomedical field might feel overwhelmed by such a complex regulatory architecture. In fact, even for legal experts, the coordination of data protection rules and research poses many uncertainties [17]. In this respect, addressing difficulties concerning how to combine the potential of data-rich research projects with adequate privacy protections for participants (data subjects) necessitate open dialogue between the research and the legal fields.

The objective of this article is to offer an overview of the current debate in the legal field around three nodes of data protection law that concern biomedical research. It provides a critical review, according to the classification by Grant and Booth [18], since it aims to go beyond mere description of the reviewed literature and case law and includes a certain degree of conceptual innovation. Given space constraints, our focus is on three nodes that are considered of primary importance in the literature. Other relevant issues in the legal debate (e.g., the concepts of purpose limitation or data minimisation) are only indirectly addressed insofar as it is relevant to the other topics of the review. We start by tackling the meaning of personal data, since this is the primary criterion that determines whether any data protection rules apply – including in biomedical research. Then, we discuss specific data-protection rules concerning the processing of personal data for research purposes. Finally, we turn to the topic of consent and clarify its role in data processing in general and data processing for research in particular. This review draws mainly on legal literature and legal sources (both judicial decisions and legal texts), but our intent is to address the medical and research community. Moreover, although the focus is on Switzerland and its legal framework, this review is also of interest for a non-Swiss readership, since the three nodes under discussion are central to the relationship between data protection and research across borders. To help link the content of this review with the legal texts, we provide a conversion table (table 1) of the legal terminology discussed, to facilitate reference to original legislative acts not written in English.

Three "nodes" at the crossroad between biomedical research and data protection law

The meaning of *personal* data

Data protection law is not relevant for the processing of data *in general*, but rather it is specifically applied to the processing of *personal* data. This is a common trait of virtually every piece of legislation on data protection. In Switzerland, for example, this is clearly established by the FADP (art. 3.a [12]), the HRA (art. 2 para. 1.e [11]) and most of the cantonal data protection regulations[3]. For the field of biomedical research, this implies that data protection rules apply only if researchers are using *personal* data. Biomedical research with *non-personal* (or *anonymised*, see below) data falls outside the scope of data protection rules (for more details, see [19] p. 109) and thus does not require, amongst other things, approval from ethics committees. The staggering difference in the regulatory regime between *personal* and *non-personal* data, clearly begs the question of how to distinguish between these two categories.

In the legal literature, the exact meaning of what constitutes *personal* data is extensively debated and the exact borders of this category are highly contested [17], especially after recent developments in the field of data science [20]. In regulations, *personal* data are usually defined as information relating to an identified or identifiable person. For example, the FADP states that *personal* data are "all information relating to an identified or identifiable person" (art 3.a [12]). Virtually every other cantonal data protection law contains a similar definition and even for the EU level, the GDPR (art. 4 (1) [5]) uses very similar words, although

Table 1: Cross-language comparison for Switzerland of the legal terminology discussed as part of the first node.

Term in English discussed in this review	Corresponding term in German	Corresponding term in French	Corresponding term in Italian
"Personal data"	"Personendaten" or "Personenbezogene Daten"	"Données personnelles"	"Dati personali"
"Relating to"	"sich beziehen auf"*	"se rapporter a"†	"relative a"‡
"Identified or identifiable"	"Bestimmt oder bestimmbar"	"identifiée ou identifiable"	"identificata o identificabile"

* As in article 3.a. of the FADP "Personendaten (Daten): alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen". † As in article 3.a. of the FADP "données personnelles (données), toutes les informations qui se rapportent à une personne identifiée ou identifiable" ‡ As in article 3.a. of the FADP "dati personali (dati): tutte le informazioni relative a una persona identificata o identificabile"

it refers only to *natural* persons. Along the same line, the HRA defines (health related) *personal* data as "information concerning the health or disease of a specific or identifiable person" (art. 3.f [11]). All these definitions are relatively open-ended and leave room for interpretation by legal doctrine and by courts. In practice, to understand within a specific biomedical research project whether the data being processed are *personal*, two[4] elements are of primary importance. First, it must be determined whether data are *relating to* a person. Secondly, it must be determined whether this person is *identified or identifiable*. If both conditions are satisfied, data must be considered *personal* and data protection rules will apply.

In the context of biomedical research, it will often be clear that data *relate to* a person, since most of the data used are *about* people. However, in order to be *personal*, data must not only be *relating to* a person, but the person must also be *identified or identifiable*. With respect to this requirement, it is difficult from a legal point of view to give clear-cut answers. Cases where the data relate to an *identified* person, i.e., when the identity of the person is evident from the data ([22] p. 34), are easy to recognise. If, for example, the database of a research project contains the names or the addresses of the people whose data are processed, such data will obviously relate to an *identified* person and thus be *personal* data ([19], p. 516). Cases where data relate to an *identifiable* person, i.e., when the identity of the person does not emerge directly from the data(set) itself but can be derived from the context or the combination with other data, are more difficult ([22] p. 34). Whether such data can still be considered *personal* data depends on several factors, since the legal concept of *identifiability* – at least in Switzerland – is relative and not absolute ([22] p. 34). Traditionally, legal doctrine has argued that both an objective (the existence of means to re-identify) and a subjective factor (a sufficient interest by the data-processor to re-identify) need to be present in order for data to be considered *identifiable* [23]. The relativity of the concept of *identifiability* and its dependency on context and intentions of the data-processors are also confirmed by case law. In a recent decision of the Swiss Federal Supreme Court [24], for example, the judges ruled that images of people on Google Street View are *identifiable* (and thus *personal* data) since the identity of the person can often be derived by the context (e.g. dress, location, etc.), notably this applies even if faces are blurred. In another decision by the same court [25], it was established that IP-addresses are data relating to an *identifiable* person, if the data-processor in the specific case has the concrete possibility to access additional information that can lead to (re-)identification of the person using the IP-address. Therefore, the relative nature of the concept of *identifiability* entails that even the same data that might be considered *non-personal* in a certain context may be deemed *personal* if the circumstances change.

In the biomedical research context, *anonymisation* represents the procedure through which data cease to be *identifiable* and thus *personal*. Indeed, rather than speaking of *non-personal* data, the term *anonymised* data is often heard in this context. From a legal perspective, *anonymisation* is defined as the procedure through which *personal* data are processed so that re-identifying the person becomes either impossible or disproportionately difficult ([19] p. 512). Article 25 of the Human Research Ordinance (HRO [26]) explains that "for the anonymisation of […] health-related personal data, all items which, when combined, would enable the data subject to be identified without disproportionate effort, must be irreversibly masked or deleted. In particular, the name, address, date of birth and unique identification numbers must be masked or deleted." Since the law provides a non-exhaustive list of elements that must be deleted in order to anonymise personal data, this leaves some room for interpreting what actual processes can be considered relevant to match the legal definition of anonymisation. Due to current advances in big data analytics, there are concerns that the legal concept of anonymisation is bound to become ever more elusive ([22] p. 34), but in current practice anonymisation can be treated as the flipside of identifiability (see previous paragraph). In order to determine whether data are truly *anonymised* (and thus *non-personal*), both the material chances of re-identification and the interest in re-identifying must be evaluated on a case-by-case fashion ([19] p. 513). This means, in turn, that the problems of relativity described above with respect to *identifiability* also apply to *anonymisation*. Therefore, the classification of a certain dataset as *anonymised* might not be definitive: if the circumstances change and the links to identities of individuals are re-established ([19] pp. 515ss), this would turn *anonymised* data back into being classifiable as *personal*. This generates more legal uncertainty when compared to the legal situation in the US, where health data are considered definitively de-identified (i.e., *anonymised*) once a precise and exhaustive list of 18 personal identifiers are removed [27]. The porous differentiation between *personal* data and *anonymised* data in Switzerland also implies that even for research projects processing data that they deem *anonymised*, it could still be convenient to adhere to the rules of personal data processing (e.g., in terms of data security).

Pseudonymisation or *coding* are also often described as procedures through which data can somehow be made "less" *personal*. From a legal point of view, *coding* (and equally *pseudonymising*) is regarded as the process through which the elements that link data to the identity of a person are *reversibly* removed ([19] p. 512). For example, if a research project aims at studying mortality rates after one type of surgery based on retrospective analysis of routinely collected data from two different hospitals, researchers might merge data from the two hospitals in a unified database, remove the original case-IDs of each single patient and substitute them with newly developed codenames. If it is possible to reverse such process and go back from the codenames to the original case-IDs of the two hospital, these data might be considered as *pseudonymised* from a legal point of view. In contrast to *anonymising*, which irreversibly prevents data from being connected to an identifiable person and thus renders the data *non-personal*, *coding/pseudonymising* simply represents a way to better protect personal data and to benefit, under certain circumstances, from better conditions concerning the reuse of data for research purposes (see also last section). To refer back to the terminology of the previous sections, if data are simply *coded* or *pseudonymised*, they will still be *relating to* an *identifiable* person (and thus still be *personal* data), although only indirectly by means of a key.[5] If, on the contrary, data are *anonymised*, the key to link them

back to an identifiable person either does not exist or it has been eliminated. The exact boundary between these two categories can often be blurry, especially when the key exists, but it is not directly and easily accessible to the researchers and it is not their intent to re-identify patients.[6] Moreover, it has been argued that, aside from the legal requirements, the actual practices for producing anonymisation are far from uniform in Switzerland [29].

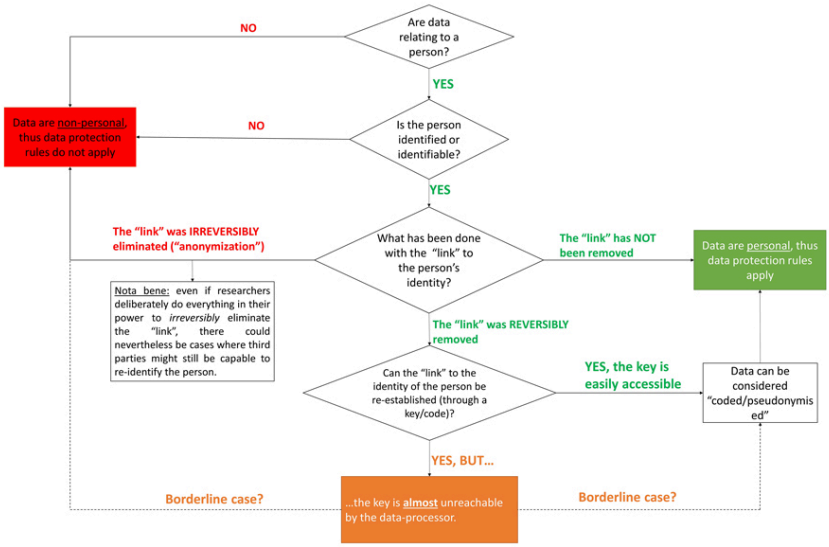
To help researchers navigate these different aspects, we summarised this section in a decision-tree (fig. 1.) that can be used to reflect whether data used in a research project are indicatively *personal* or *non-personal*.

Sector-specific data protection rules for research

If they ascertain that the data in their project are *personal* and thus data protection rules apply, researchers still need to determine which specific regulatory framework they need to follow. Traditionally in Europe, data protection rules are contained in legislative acts that regulate the processing of personal data across sectors. In Switzerland, for example, the FADP contains general rules on the processing of personal data by federal bodies (e.g. federal universities) and private persons (e.g. pharmaceutical companies), while cantonal data protection regulations set the norms for the processing of data relating to or deriving from cantonal bodies (e.g. cantonal hospitals and cantonal universities). On top of these general regulations, a number of additional data protection rules are scattered across several sectorial legislative acts (fig. 2). The principal ones in the field of interest for this article are the HRA [11], the law on electronic patient record (LEPR [30]), the Law on Health insurance (LHI [31]), the Epidemic Law (EL [32]), the Law on Cancer Registration (LCR [33]), the Federal Statistic Act (FSA [34]) and the Federal Act on Human Genetic Testing (HGTA [35]). The HRA covers the collection and analysis of data in the field of human research. The LEPR concerns the "processing of data in the electronic patient record" (art. 1 [30]), which hospitals and nursing homes have the duty to offer [36]. The LHI contains some data protection rules concerning duties of healthcare providers and healthcare payees to transfer data to federal offices with monitoring (art. 23 and art 59a [31]) or quality control purposes (art 58b and 58c [31]). The EL has some sectorial rules applicable to "process personal data, including data concerning health, for the purpose of identifying people who are ill, potentially ill, infected, potentially infected or that expel pathogen elements with respect to public health provisions, in particular to single out and surveil contagious illness and fight against them" (art. 58 [32]). The LCR regulates the "collection, recording and analysis of data concerning cancer illnesses" (Art. 1 [33]) for monitoring, prevention, quality development and research purposes (art. 2 [33]). The FSA delineates some data protection rules for the processing of data by the Federal Office of Statistics. The HGTA focuses on the regulation of genetic testing for the medical, employment, insurance and liability contexts and it contains some rules on the protection of genetic data. Lastly, the processing of data by healthcare professionals and researchers is also covered by the rules on confidentiality in the Criminal Code (art. 321 and art. 321bis Criminal Code [37]).

For researchers, this framework of data protection rules involving several legislative acts might look quite difficult to navigate. Indeed, even from a legal point of view, determining exactly which rules concerning data protection have to be followed in a single research project can be a challenge. There are, however, some general indications that can be given. One general principle of law is that *lex specialis derogat legi generali*, i.e., when two pieces of law cover the same subject matter the specific legislation derogates the more general one. In the case of data protection rules, the more general legislations are the FADP and the other cantonal data protection acts, since they regulate the processing of data across sectors. This means that their framework can be derogated if a specific legislation covering the processing of personal data in particular sector exists. This is the case for the field of biomedical research, where the passing of the HRA in 2011 created sector-spe-

Figure 1: Ascertaining whether the data in a research-project are personal or not. A supportive decision-tree. This decision-tree has merely indicative and instructive (rather than prescriptive) purposes, since every schematisation involves some degree of simplification and approximation. Specificities of each single case (such as linking possibilities) might lead to different outcomes.

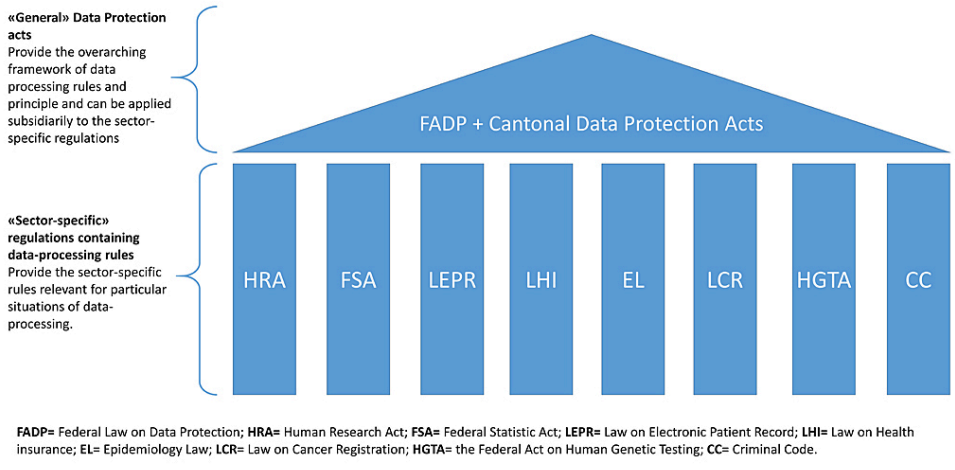


cific data protection rules that apply to the processing of personal data for biomedical research. As noted, the HRA created a proper "data protection regime" for the field of biomedical research ([19] p. 808). Data protection rules contained in the FADP and other general cantonal data protection regulations have thus a *subsidiary* function, i.e., they can be considered to supplement the rules of the HRA. In other words, the general data protection regulations remain applicable in cases where the provisions of the HRA are not exhaustive enough (see also [19] pp. 809ss).

The presence of a sector-specific regulation containing data protection rules for the field of biomedical research has both advantages and disadvantages. A considerable advantage is that the processing of data for biomedical research purposes has its own peculiar needs and features – for example, compared to data processing for marketing purposes, or for other types of research. In this respect, having data protection rules tailored to the field of biomedical research (rather than the more general rules contained in the FADP [12]) was perceived as particularly important by the regulator [38]. Another advantage is that the presence of a specific regulation for the field of research does, to some extent, allow for the harmonisation of rules throughout a country [39]. Other European countries, such as Germany, do not have a general regulation that comprehensively covers biomedical research [40], and data protection rules for this sector are scattered amongst several other laws [41]. Having a sector-specific regulation, however, also entails disadvantages. These include factors such as the coordination and the interplay with other existing regulations containing rules on data processing. We will turn to these two issues consecutively.

To determine whether a research project can benefit from the sector-specific data protection rules of the HRA, it must be determined if the project falls within the scope of this act. Art. 2 para. 1 [11] defines the scope of the HRA and states that the act "applies to research concerning human diseases and concerning the structure and function of the human body". As it has been clarified ([19] p. 103), the scope of application of the HRA is based on the aim, and not directly on the type/design of the research, which is in contrast to an earlier draft of the HRA [42]. The scope of the HRA is thus quite broad: as long as a methodology recognised by the scientific community is used to produce knowledge with the (distant?) objective of improving medical standards or better understanding the human body (and its subparts), the HRA will apply [19, 38]. For the HRA to apply, another important fact to consider is whether the project is using *health related* personal data. Although a very general definition of this concept is provided in art. 3.f [11] of the HRA, the exact meaning of *health related* personal data is bound to be influenced by technological advances and by the context in which data are processed [43]. No relevant rulings by Swiss Federal courts are present to help guide practice. Legal doctrine in Switzerland traditionally interprets the *concept of health data* very broadly, including all personal data that have a direct or indirect connection with the physical or psychological health of a person ([22] p. 39; [44] p. 56). Moreover, as recently highlighted [43], it is increasingly difficult to distinguish from "traditional" health data and new forms of data (especially those collected digitally) that can be used to infer knowledge about the health status of a person. Since health data are universally considered as particularly sensitive[7], the blurred edges of their definition are particularly problematic. In fact, determining whether or not the personal data being processed is health-related, not only determines the applicability of the HRA, but triggers specific (and usually more stringent) requirements for data processing. This is because health data – together with other types of data, such as those about religion or political orientation – are considered particularly sensitive and thus deserving special protection (on the notion of *particularly sensitive data*, see e.g., [22] pp. 37ss). For example, the FADP (Art. 4 para 5) stipulates that when personal data are processed based on consent, that consent must be explicit when particularly sensitive data such as health data are processed.

Figure 2: An overview of parts of the legislative framework concerning data processing in Switzerland. The image does not aim to be exhaustive, but merely indicative of the relationship between different legislative acts concerning data protection and data processing in the healthcare sector.



FADP= Federal Law on Data Protection; **HRA=** Human Research Act; **FSA=** Federal Statistic Act; **LEPR=** Law on Electronic Patient Record; **LHI=** Law on Health insurance; **EL=** Epidemiology Law; **LCR=** Law on Cancer Registration; **HGTA=** the Federal Act on Human Genetic Testing; **CC=** Criminal Code.

However, even if the scope of sector-specific regulation like the HRA is clarified, some additional questions might emerge for researchers. What happens with "borderline" research projects, which may rely on innovative methodologies (e.g. mining of electronic health records), or make use of large datasets generated during clinical routine and are not aimed at singling out individual cases (e.g. retrospective registry-based studies)? What if a research project processes data from multiple sources and which were originally collected according to different data-protection regimes (e.g. combining data from insurance providers, cantonal hospitals and the Federal Office of Statistics)? How do the data processing rules of these different regimes interact? Unfortunately, such questions do not have one-size-fits-all answers from a legal perspective. Innovative healthcare service research that relies on data routinely collected is relatively underdeveloped in Switzerland ([45] p. 28) and has only been recently encouraged by the scientific community (e.g. through the aforementioned NRP 74 [7]). How to combine existing rules on data protection and data processing with this type of research will require the effort of both the research and the legal field to develop efficient and accepted practices. The latter should help, for example, to simplify the combination of different sectorial legal regimes and of the federal and cantonal data protection law (see e.g., [46], and, to better clarify the distinction between processing of data for research and for quality improvement purposes, see [47, 48]). Moreover, a balance should be found between easing the requirements for the processing of data for research (through the creation of a "research exemption" [6]) and the retention of ethical requirements, especially with respect to health data [49]. Lastly, particular attention should be given to the topic of consent, which we address in the next section.

The relevance of consent for data processing in research

Consent, especially in the field of biomedical research, has considerable importance, since it has traditionally been one of the key requirements to legitimately enrol patients in clinical studies and it is one of the cornerstones of research ethics. This is due to the fact that consent has become a fundamental precondition to justify the intrusion upon the *physical* integrity of both patients and research participants [50]. When data processing techniques evolved so that more research could be undertaken without any physical contact with participants, but rather through the processing of their data, consent continued to remain a pivotal requirement, especially because of its ethical significance. Participants' protection rules like the requirement of consent were upheld, in the conviction that data processing for research entails an *intangible* (rather than physical) invasion of personal integrity [51]. Consent, thus, remained one of the central paradigms of data processing for research purposes to such an extent that, even when processing happens without traditional informed consent, it is often spoken of *presumed consent* solutions (e.g., for the collection of data in registries and the performance of epidemiological research with them in Denmark [52] and [53]).

From the legal perspective, however, the role of consent for data processing is quite different. While consent remains a fundamental instrument to protect informational self-determination[8] especially when it comes to health data (e.g., [56].), the concept may come into play at different levels. Where the law, such as the GDPR at the EU-level, requires a lawful basis for any data processing, the long list of grounds that permit data processing includes not only consent, but also several alternatives, such as the necessity to perform a contract, the pursuance of a legal obligation or the protection of a vital interest of a natural person (art. 6 GDPR [5]).

In Switzerland, one has to distinguish whether personal data are being processed by a federal or cantonal body or by private persons. If personal data are processed *by private entities*, the FADP [12] does not necessarily require consent to be obtained. If processing does not comply with general data protection principles, which could lead to a potential violation of the data subject's personality rights, it may be possible to justify such processing by several means: by obtaining consent ([21] p. 350; [22] p. 165) a specific legislative act authorising such data processing, or by the presence of an overriding private (e.g., the execution of a contract) or public interest (e.g., the compilation of statistics) - Art. 13 FADP ([12]; [22] p. 172). If personal data are processed *by federal public bodies*, a formal legislative act authorising the processing is necessary to use personal data, consent of the person being of minor relevance ([22] pp. 220ss). In both contexts (processing by private persons or by federal public bodies), data processing for research, planning and statistics is privileged (art. 13 sec. 2 lit. e and art. 22 FADP) by the presence of less rigid conditions ([22] pp. 184ss and 290ss; [44] pp. 124ss), which partly resemble the "research exemption" present at the EU level [6]. These considerations show that, from a legal perspective, the right question researchers should formulate when they design the data protection framework of a project is not "Do we have consent?", but rather "Do we need consent?".

To better understand what this means in practice, it is helpful to consider a case study offered by the rules of the HRA. As specified in the previous section, the HRA represents a sector-specific set of data processing rules for biomedical research. In articles 32-35 [11], this act sets some specific conditions for the "further processing" (or secondary processing) of personal data. Further processing refers to those cases where data are collected for a specific aim (e.g. during the provision of care) but can then potentially be re-used for research purposes. A classic example is the further processing for research purposes of routinely collected data from hospitals, which has received much attention and prompted both application (e.g., [57].) and implementation (e.g., [58]) projects. In such cases, the HRA offers multiple requirements and possibilities for further data processing (for more details see e.g., [59]). For genetic data and for non-genetic health data in an identified form (i.e. non-coded/non-pseudonymised), the requirement for further data processing is having the consent of the data-subject, in some cases even of a "general" nature (art. 32.1, 32.2 and 33.1 HRA ([11]; [19] p. 484). For the further processing of non-genetic health data in a coded form or for the anonymisation of genetic data, the requirement is for the provision of information and the acknowledgment of the right to dissent (but explicit consent is not necessary [19] p. 499). However, when provision of consent (first case) or provision of information (second case) is not pos-

sible, an alternative strategy for undertaking further data processing is to receive an *exceptional* exemption by the competent Research Ethics Committee (Art. 34 HRA [11]; see also [19] pp. 501ss). The latter needs to ascertain that: (1) providing consent (first case) or information (second case) is impossible or disproportionately difficult; (2) no documented refusal by the subject whose data are used is available; and (3) the interests of the research project outweigh the interests of the person concerned (art. 34 HRA [11]). Since this contingency is defined in theory as *exceptional*, it is disputed whether the application of this alternative route for (further) data processing should be regularly used [19, 60]. In any case, this example shows how, from a purely legal perspective, consent often remains a very relevant aspect of lawful data processing, but it is not necessarily the only one. Other alternative requirements for data processing is a matter for the law to settle. How (and how often) they are used within the legal limitations, is a matter for practice to develop. In this context, it should also be kept in mind that, as mentioned above, data protection rules contained in more general regulations (such as the FADP for Switzerland) may continue to apply in a *subsidiary* function.

Conclusion

In this article, we explored three intersections of data protection law and biomedical research. We first focused on the concept of personal data, which represents the most important criterion to determine whether data protection rules apply at all. We then analysed the sector-specific data protection rules for research and their interaction with more general data protection norms. Finally, we reflected on the topic of consent for data processing from a legal perspective. Our aim was to help bridge the gap between the legal and biomedical sectors by providing an overview of the legal debate regarding several important elements of data processing relevant for the biomedical sector. Given the complexity of such elements, we explained why there cannot be an expectation to find the exact and exhaustive rules for correct data processing in one single document, be it a legislative act, a guideline or a policy statement. This is also due to the fact that data protection and privacy are important values, but they are not absolute and, especially with respect to research, have to be balanced with other important legal and ethical principles. Therefore, the establishment of such balance will require collaboration between biomedical research professionals and legal experts. This cooperative effort will be crucial for addressing the pivotal question of how to ensure adequate data protection while promoting important research in the future.

Currently, there is a discussion [61] ongoing in the legal doctrine about a renewed definition of anonymisation of data for research purposes, one that is sufficiently nuanced and comprehensive and that takes into consideration the specific features of the research context. The proponents for developing a new definition argue that once personal identifiers are eliminated from a dataset, researchers often[9] have no *subjective* motivations to re-identify subjects, even when re-identification remains technically (i.e., *objectively)* possible (by e.g., combining data from different datasets). In a similar fashion, also Voekinger et al. [27] propose a further category of data, namely pseudo-anonymised, to define all those data where every effort has been made to anonymise them, but re-identification cannot be excluded. These legal proposals should also be considered by the research community so that solutions for finding a definition of anonymisation that is both legally solid and research friendly. A good starting point for this collaboration between the legal and the research worlds is the creation of courses on data protection for the research community (see e.g., the initiative of the SPHN [62]). Another possibility for productive exchange between the research and legal community is a partnership between researchers and cantonal data protection officers, who could offer assistance for the interpretation and application of the law if they are evenly organised and properly funded [63].

Footnotes

[1] In European Law, preambles are claims attached to any approved law to indicate the motivations of the legislator in enacting such law and to indicate how it ought to be interpreted. They are not, however, legally binding.

[2] Manuscripts in preparation.

[3] Some cantons, like Zürich (Gesetz über die Information und den Datenschutz) and Basel-Stadt (Informations- und Datenschutzgesetz), have regulations that deal with the principle of transparency for public bodies and "information" more generally, but most of the rules are in reference to personal data. Additionally, there are some other federal regulations that contain rules concerning non-personal data (e.g., the LIH).

[4] A third element sometimes considered is that of defining what *information* means (see e.g,, [21], pp. 25ss), which is normally interpreted extremely quite broadly as to include information in any form and on any support (e.g., digital, analogue).

[5] The key can be, for example, a conversion table where every code-name is associated with the original ID, or another technical device that can recover the original ID starting from the codename.

[6] See, for example, Baeriswyl and Parli ([22] pp. 35–36) where it is argued that in such cases data can be considered anonymized (non-personal) from the perspective of the researchers. The same stance is argued in [28].

[7] This holds true also in Switzerland, where the FADP and each cantonal regulation on data protection considers data concerning health as worth of additional protection.

[8] The right to informational self-determination (informationelle Selbstbestimmung) is not directly present in the law in Switzerland, but it has been introduced into case law and has been recognised by the doctrine (e.g., [54]), although sometimes in a critical fashion [55].

[9] But not always: for example, when they could return clinically relevant incidental findings.

Acknowledgements
AM would like to thank Georg Starke for reading one version of the manuscript and discussing the topic. Moreover, AM would like to thank the kind staff of the café in Szczecin who put up with him for several days whilst one of the drafts of the manuscript was written.

Financial disclosure
AM and BE acknowledge the financial support provided by the Swiss National Science Foundation (SNF NRP-74 Smarter Health Care,

grant number 407440_167356). The funder had no role in the drafting of this manuscript and the views expressed therein are those of the authors and not necessarily those of the funder.

Competing interests

The authors have no conflict of interest to declare.

References

1 Collins FS, Morgan M, Patrinos A. The Human Genome Project: lessons from large-scale biology. Science. 2003;300(5617):286–90. doi: http://dx.doi.org/10.1126/science.1084564. PubMed.

2 Amunts K, Ebell C, Muller J, Telefont M, Knoll A, Lippert T. The Human Brain Project: Creating a European Research Infrastructure to Decode the Human Brain. Neuron. 2016;92(3):574–81. doi: http://dx.doi.org/10.1016/j.neuron.2016.10.046. PubMed.

3 Meier-Abt P, Lawrence AK, Selter L, Vayena E, Schwede T. The Swiss approach to precision medicine. Swiss Medical Weekly [Internet]. 2018 Jan 2 [cited 2020 April 16]. Available from: https://smw.ch/en/op-eds/post/the-swiss-approach-to-precision-medicine/.

4 Fecher B, Friesike S. (2014). Open science: one term, five schools of thought. In: Bartling S., Friesike S, editors. Opening science. Cham: Springer; 2014. p. 17–47. doi: http://dx.doi.org/10.1007/978-3-319-00026-8_2. .

5 General Data Protection Regulation (GDPR) [internet]. The European Parliament and The Council of the European Union [cited 2020 March 30]. Available from: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32016R0679.

6 Staunton C, Slokenberga S, Mascalzoni D. The GDPR and the research exemption: considerations on the necessary safeguards for research biobanks. Eur J Hum Genet. 2019;27(8):1159–67. doi: http://dx.doi.org/10.1038/s41431-019-0386-5. PubMed.

7 Swiss National Science Foundation (SNF) [internet]. Smarter Health Care National research program. Call for proposals. 2015. [cited 2020 March 30]. Available from: http://www.nfp74.ch/SiteCollectionDocuments/Call_SmarterHealthCare_en.pdf.

8 Swiss Personalised health Network (SPHN) [internet]. Vision, Mission, and Mandate. available from: https://sphn.ch/organization/about-sphn/.

9 Meier-Abt P, Egli F. Kräfte bündeln: «Swiss Personalized Health Network. Bulletin SAMW. 2016;1:1–5. Available at: https://www.samw.ch/dam/jcr:65a852a6-5c43-4186-8992-bc37595238fd/bulletin_samw_16_1.pdf.

10 Swiss Biobanking Platform (SBP) [Internet]. Annual Report 2019. [cited 2020 March 30]. Available from https://swissbiobanking.ch/annualreport2019.

11 Human Research Act (HRA) [Internet]. Federal Assembly of the Swiss Confederation. Status as of 1 January 2020 [cited 2020 March 30]. Available from: https://www.admin.ch/opc/en/classified-compilation/20061313/index.html.

12 Federal Act on Data Protection (FADP) [internet]. Federal Assembly of the Swiss Confederation. Status as of 1 March 2019 [cited 2020 March 30]. Available from: https://www.admin.ch/opc/en/classified-compilation/19920153/index.html.

13 Bundesamt für Justiz [Internet]. Stärkung des Datenschutzes. [cited 2020 March 30]. Available from: https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/datenschutzstaerkung.html. German.

14 OECD. Strengthening Health Information Infrastructure for Health Care Quality Governance: Good Practices, New Opportunities and Data Privacy Protection Challenges, OECD Health Policy Studies. Paris: OECD Publishing;2013. doi: http://dx.doi.org/10.1787/9789264193505-en. .

15 Elger B [Internet]. Promoting the merging of health data in Switzerland2016. [cited 2020 March 30]. Available from: http://www.nfp74.ch/en/projects/healthcare-across-sectors/project-elger.

16 Convention intercantonale relative à la protection des données et à la transparence dans les cantons du Jura et de Neuchâtel (CPDT-JUNE) [Internet]. La République et Canton du Jura et la République et Canton de Neuchâtel [cited 2020 March 30]. Available from: http://rsn.ne.ch/DATA/program/books/rsne/htm/15030.htm. French.

17 Thouvenin F. Datenschutz auf der Intensivstation. Digma. 2019;19(4):206–17. [German.].

18 Grant MJ, Booth A. A typology of reviews: an analysis of 14 review types and associated methodologies. Health Info Libr J. 2009;26(2):91–108. doi: http://dx.doi.org/10.1111/j.1471-1842.2009.00848.x. PubMed.

19 Rütsche B. Kommentar zum Humanforschungsgesetz. Bern: Stämpfli; 2015. German.

20 Roland M. Was bedeutet Big Data für die Qualifikation als besonders schützenswerte Personendaten? Jusletter IT. 21 May 2015. German.

21 Rosenthal D, Jöhri Y. Handkommentar zum Datenschutzgesetz. Zürich: Schulthess Juristische Medien AG; 2008. German.

22 Baeriswyl B, Parli K. Kommentar zum Datenschutzgesetz. Bern: Stämpfli; 2015. German.

23 Rosenthal D. Löschen und doch nicht löschen. Digma. 2019;19(4):190–8. [German.].

24 Ruling of the Swiss Federal Court [Internet]. BGE 138 II 346 S. 348. Available from: https://www.bger.ch/ext/eurospider/live/de/php/clir/http/index.php?highlight_docid=atf%3A%2F%2F138-II-346%3Ait&lang=de&zoom=&type=show_document. German.

25 Ruling of the Swiss Federal Court [Internet]. BGE 136 II 508 S. 509. Available from: https://www.bger.ch/ext/eurospider/live/de/php/clir/http/index.php?highlight_docid=atf%3A%2F%2F136-II-508%3Ait&lang=de&zoom=&type=show_document. German.

26 Human Research Ordinance (HRO) [Internet]. The Swiss Federal Council. Status as of 24 April 2018 [cited 2020 March 30]. Available from: https://www.admin.ch/opc/en/classified-compilation/20121177/index.html.

27 Vokinger KN, Stekhoven DJ, Krauthammer M. Lost in Anonymization - A Data Anonymization Reference Classification Merging Legal and Technical Considerations. J Law Med Ethics. 2020;48(1):228–31. doi: http://dx.doi.org/10.1177/1073110520917025. PubMed.

28 Peter C. DSGVO und E-DSG fordern Schweizer Spitäler, Praxen, Heime und Spitex, Jusletter. 26 Februar 2018. German.

29 Stürzer M, Günter K. Werden Patientendaten anonymisiert? Digma. 2017;17(3):176–9. [German.].

30 Law on the Electronic Patient Record (LEPR) [Internet]. The Federal Assembly of the Swiss Confederation. Status on the 17 April 2017 [cited 2020 March 30]. Available from: https://www.admin.ch/opc/de/classified-compilation/20111795/index.html. German.

31 Law on Health Insurance (LHI) [Internet]. The Federal Assembly of the Swiss Confederation. Status on the 1 January 2020 [cited 2020 March 30]. Available from: https://www.admin.ch/opc/de/classified-compilation/19940073/index.html. German.

32 Law E. (EL) [Internet]. The Federal Assembly of the Swiss Confederation. Status on the 1 January 2020 [cited 2020 March 30]. Available from: https://www.admin.ch/opc/de/classified-compilation/20071012/index.html. German.

33 Law on Cancer Registration (LCR) [Internet]. The Federal Assembly of the Swiss Confederation. Status on the 1 January 2020 [cited 2020 March 30]. Available from: https://www.admin.ch/opc/de/classified-compilation/20121618/index.html. German.

34 Federal Statistical Act (FSA) [Internet]. The Federal Assembly of the Swiss Confederation. Status on the 1 January 2020 [cited 2020 March 30]. Available from: https://www.admin.ch/opc/en/classified-compilation/19920252/index.html.

35 Federal Act on Human Genetic Testing (HGTA) [Internet]. The Federal Assembly of the Swiss Confederation. Status on the 1 January 2014 [cited 2020 March 30]. Available from: https://www.admin.ch/opc/en/classified-compilation/20011087/index.html.

36 De Pietro C, Francetic I. E-health in Switzerland: The laborious adoption of the federal law on electronic health records (EHR) and health information exchange (HIE) networks. Health Policy. 2018;122(2):69–74. doi: http://dx.doi.org/10.1016/j.healthpol.2017.11.005. PubMed.

37 Swiss Criminal Code (CC). Status as of 1 February 2020. Available at: https://www.admin.ch/opc/en/classified-compilation/19370083/index.html.

38 Botschaft zum Bundesgesetz über die Forschung am Menschen vom 21. Oktober 2009. BBI. 2009:8045–61. Available from: https://www.admin.ch/opc/de/federal-gazette/2009/8045.pdf. German.

39 Rütsche B. Die Neuordnung des Schweizerischen Humanforschungsrechts: Normgenese als kritische Rezeption internationaler Vorgaben. Zeitung für Schweizerisches Recht. 2010;129-I(4):391–411. [German.].

40 Noack T, Hoffstadt A, Zotz N. Therapeutische und nicht-therapeutische Forschung. In: Lenk C, Duttge G, Fangerau H, editors. Handbuch Ethik und Recht der Forschung am Menschen. Berlin, Heidelberg: Springer; 2014. p. 273.276. doi: http://dx.doi.org/10.1007/978-3-642-35099-3_45. . German.

41 von Kielmansegg S. Datenschutz in der Forschung am Menschen. In: Lenk C, Duttge G, Fangerau H, editors. Handbuch Ethik und Recht der Forschung am Menschen. Berlin, Heidelberg: Springer; 2014. p. 121-128. doi: http://dx.doi.org/10.1007/978-3-642-35099-3_19. . German.

42 Eidgenössische Departement des Innern EDI. (2006) Erläuternder bericht vorentwurf HFG. Available at: https://www.admin.ch/ch/d/gg/pc/documents/1266/HFG_Erlaeuterungen_d.pdf. German.

43 Vokinger Kerstin N. Gesundheitsdaten im digitalen Zeitalter. Jusletter. 27 January 2020. German.

44 Rudin B, Baeriswyl B. Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Basel-Stadt (IDG). Zürich: Schulthess Verlag; 2014. German.

45 Schweizerische Akademie der Medizinischen Wissenschaften (SAMW) [Internet]. Stärkung der Versorgungsforschung in der Schweiz. Swiss Academies Reports, Basel 2014. [cited 2020 March 30]. Available from: http://www.akademien-schweiz.ch/dms/publikationen/09/report0901.pdf. German.

46 Rütsche B. Datenschutzaufsicht über Spitäler. Digma. 2012;12(4):176–81. [German.].

47 Szucs TD, Bräm C. Gesundheitsforschung mit Versicherungsdaten. Jusletter. 27 January 2020. German.

48 McLennan S, Maritz R, Shaw D, Elger B. The inconsistent ethical oversight of healthcare quality data in Switzerland. Swiss Med Wkly. 2018;148:w14637. doi: http://dx.doi.org/10.4414/smw.2018.14637. PubMed.

49 Vayena E. Ein ethischer Rahmen für den Austausch von Gesundheitsdaten. Schweiz Arzteztg. 2017;98(36):1138–40. doi: [German.]. http://dx.doi.org/10.4414/saez.2017.05941.

50 Miller FG. Research on medical records without informed consent. J Law Med Ethics. 2008;36(3):560–6. doi: http://dx.doi.org/10.1111/j.1748-720X.2008.304.x. PubMed.

51 Townend D. Privacy, health insurance, and medical research: tensions raised by European data protection law. New Genet Soc. 2010;29(4):477–93. doi: http://dx.doi.org/10.1080/14636778.2010.528194.

52 Ludvigsson JF, Håberg SE, Knudsen GP, Lafolie P, Zoega H, Sarkkola C, et al. Ethical aspects of registry-based research in the Nordic countries. Clin Epidemiol. 2015;7:491–508. doi: http://dx.doi.org/10.2147/CLEP.S90589. PubMed.

53 Nordfalk F, Hoeyer K. The rise and fall of an opt-out system. Scand J Public Health. Scand J Public Health. 2020;48(4):400–4. doi: http://dx.doi.org/10.1177/1403494817745189. PubMed.

54 Ehrenzeller B, Mastronardi P, Schweizer RJ, Vallender KA. Die Schweizerische Bundesverfassung. Kommentar. Zürich: Schulthess Verlag; 2002. German.

55 Gächter T, Egli P. Informationsaustausch im Umfeld der Sozialhilfe, Jusletter. 6 September 2010. German.

56 Sprecher F. Sozialpflichtigkeit von Gesundheitsdaten. Digma. 2019;19(4):184–9. [German.].

57 Roth JA, Goebel N, Sakoparnig T, Neubauer S, Kuenzel-Pawlik E, Gerber M, et al.; PATREC Study Group. Secondary use of routine data in hospitals: description of a scalable analytical platform based on a business intelligence system. JAMIA Open. 2018;1(2):172–7. doi: http://dx.doi.org/10.1093/jamiaopen/ooy039. PubMed.

58 Willers J. Development of a governance and quality management system for exchange of patient related data for research purpose. 2018. [cited 2020 March 30]. Available from: https://sphn.ch/wp-content/uploads/2019/11/2017DEV02_Willers_Lay_Summaries_20180117.pdf.

59 Martani A, Geneviève LD, Pauli-Magnus C, McLennan S, Elger BS. Regulating the Secondary Use of Data for Research: Arguments Against Genetic Exceptionalism. Front Genet. 2019;10:1254. doi: http://dx.doi.org/10.3389/fgene.2019.01254. PubMed.

60 Bundesamt für Gesundheit [Internet]. Humanforschungsgesetz (HFG): Ergebnisse der Evaluation und weiteres Vorgehen. Bern: 6 December 2019. [cited 2020 March 30]. Available from: https://www.bag.admin.ch/dam/bag/de/dokumente/biomed/forschung-am-menschen/evaluationhfg/evaluation-hfg-bericht-bag.pdf.download.pdf/Bericht_des_BAG_Ergebnisse_und_Empfehlungen_EvalHFG_d.pdf. German.

61 Thouvenin F. Forschung im Spannungsfeld von Big Data und Datenschutzrecht: eine Problemskizze. In: Boehme-Nessler V, Rehbinder M, editors. Big Data: Ende des Datenschutzes? Gedächtnisschrift für Martin Usteri. Bern: Stämpfli Verlag; 2017. P. 27-53. German.

62 SPHN/BioMedIT Data Privacy and IT Security Training [at the bottom of the page] [Internet]. BioMedIT Project [Cited 2020 Jul 6]. Available from: https://sphn.ch/network/projects/biomedit/.

63 Privatim. Resolution: Fehlende Ressourcen bei den Datenschutzbehörden [Internet]. [Cited 2020 Jul 6]. Available from: https://www.privatim.ch/de/resolution-fehlende-ressourcen-bei-den-datenschutzbehorden/. German.