

Frédéric Erard / Mathilde Heusghem / Clément Parisato

## **Biomedical Research and Open Data**

### **Prospects in Swiss law**

---

Policies for open access to research and research data are becoming increasingly widespread in our society. Some include health data used in the context of biomedical research. The purpose of this article is to analyse the interactions between open access policy on the one hand and legal constraints on the other, with regard to biomedical research data. It also proposes a list of elements to consider before any biomedical research data is made available.

---

Category of articles: Scientific Articles  
Field of Law: Health Law, Data Protection

Citation: Frédéric Erard / Mathilde Heusghem / Clément Parisato, Biomedical Research and Open Data, in: Jusletter 30 January 2023

## Contents

1. Introduction
2. Background and definitions
  - 2.1. Open Science, Open Data and Open Research Data
  - 2.2. Swiss context
  - 2.3. Open Data and biomedical research
3. Personal data protection constraints
  - 3.1. Applicable legal framework and scope
  - 3.2. Opening data through anonymisation?
  - 3.3. Reuse of personal data, in particular for human research purposes
    - 3.3.1. HRA Regime
    - 3.3.2. Non-HRA Regime
  - 3.4. Need to adopt a contractual framework when sharing personal data
  - 3.5. Use of Privacy Enhancing Technologies (PETs)
  - 3.6. Excursus: European Health Data Space project in Europe
  - 3.7. Interim observations and brief considerations on the legal architecture of the reuse of data for research purposes
4. Opening up data
  - 4.1. Constraints related to opening up data
    - 4.1.1. Applicable legal regimes
    - 4.1.2. Examples of constraints
  - 4.2. Putting data into circulation: licence & waiver
5. Practical application and check-list
6. Conclusion

## 1. Introduction<sup>1</sup>

[1] The paradigm of science and open data is undeniably a development factor for today's societies in that it aims both to increase confidence in the results of the research generated and to allow the development of new knowledge. The COVID-19 pandemic has once again demonstrated the need to develop solutions for the secure collection and exchange of information related to health data. Access to and reuse of this scientific data has made it possible to facilitate the development of vaccines, but also to adapt the measures taken by governments in response to the evolution of the pandemic.

[2] The philosophy of open access is based on a relatively simple principle, namely «as open as possible, as closed as necessary». In practice, however, it is not easy to determine to what extent the rules imposed by the various legal regimes applicable to research data and their possible overlapping can make it possible to consider their open access, in accordance with Open Data standards. While the general topic of framework conditions and incentives for sharing health data in Switzerland is the subject of regular studies in various disciplines, particularly in medical ethics<sup>2</sup>, it has still given rise to few legal contributions in Switzerland.

---

<sup>1</sup> All internet links in this article were last consulted on 15 December 2022 (for the publication of this article in French), except for footnote 25 and for those whose content is quoted and/or for which an English version of the source was available. Since the original text was written in French, references to sources are kept in the Swiss French format.

<sup>2</sup> See e.g. ANDREA MARTANI *et al.*, *Evolution or Revolution? Recommendations to improve the Swiss Health Data Framework*, *Front. Public Health*, 31 May 2021, available here: <https://doi.org/10.3389/fpubh.2021.668386>; LESTER DARRYL GENEVIÈVE *et al.*, *Individual notions of fair data sharing from the perspectives of Swiss stakeholders*, *BMC Health Services Research*, 23 September 2021, available here: <https://bmchealthservres.biomedcentral.com/articles/10.1186/s12913-021-06906-2>.

[3] After a brief presentation of the concept of open access (2) we will examine the constraints to opening biomedical data, in particular from the point of view of the protection of personal data (3), in order to determine the extent to which biomedical data can be made available in accordance with the principles advocated by Open Data (4). We will finish with a brief proposal for a checklist of aspects that need to be taken into account when considering «opening» data for research purposes. Some issues will lead us to examine the approaches developed and the solutions adopted, particularly at European level, but the following reflections will be carried out essentially under Swiss law.

## 2. Background and definitions

### 2.1. Open Science, Open Data and Open Research Data

[4] The paradigm of Open Data is a concept that is part of the more global movement of Open Science, which is based on the idea that academic knowledge must be freely accessible to the public without restriction. Although the concept is not strictly defined in positive law, it is the subject of definitions in various statements and initiatives aimed at promoting it.

[5] Thus, in its recommendation for open science, UNESCO defines Open Science as «[...] an inclusive construct that combines various movements and practices aiming to make multilingual scientific knowledge openly available, accessible and reusable for everyone, to increase scientific collaborations and sharing of information for the benefits of science and society, and to open the processes of scientific knowledge creation, evaluation and communication to societal actors beyond the traditional scientific community».<sup>3</sup>

[6] The Budapest Open Access Initiative<sup>4</sup> and the Berlin Declaration<sup>5</sup> are two major initiatives that establish the Open Science movement. While the Budapest Initiative promotes open access to research publications, the Berlin Declaration broadens this field by offering open access to the world's scientific literature, that is to say both to research results and to the tools used to collect the data. It states that the authors and copyright owners of open access contributions grant all users a free, irrevocable, worldwide right of access to the work, as well as a licence thereto. This covers the original results of scientific research, raw data and meta data, source documents, digital representations of pictorial and graphic documents, and multimedia scientific documents.<sup>6</sup>

[7] It can therefore be noted that Open Science presupposes free access and reuse of research results available on the Internet in order to promote their widespread dissemination. This concept promotes the transfer of knowledge, as well as its access and visibility to both the scientific community and the general public.

---

<sup>3</sup> UNESCO recommendation on Open Science, 23 November 2021, p. 7 (see <https://unesdoc.unesco.org/ark:/48223/pf0000379949.locale=en>).

<sup>4</sup> Budapest Open Access Initiative (BOAI) of 14 February 2002 (see <https://www.budapestopenaccessinitiative.org/>).

<sup>5</sup> Berlin Declaration on Open Access to Knowledge in the Sciences and Humanities of 22 October 2003 (see [https://openaccess.mpg.de/68042/BerlinDeclaration\\_wsis\\_fr.pdf](https://openaccess.mpg.de/68042/BerlinDeclaration_wsis_fr.pdf)). This declaration was ratified by 768 institutions (<https://openaccess.mpg.de/319790/Signatories>).

<sup>6</sup> See Berlin Declaration.

[8] Open Data is a sub-category of Open Science (alongside, for example, Open Source software [free software]) and involves opening up, thus making free the use, reuse, storage and redistribution of data, in a usable and readable format for humans and machines. Texts encouraging Open Data often refer to the FAIR (Findable, Accessible, Interoperable, Reusable) principles. Developed by researchers to guide the implementation of Open Data strategies,<sup>7</sup> they are now widely recognised and serve regularly as a reference for large-scale research institutions, projects and initiatives, both at Swiss<sup>8</sup> and international level.<sup>9</sup> The process of opening research data, which is part of the Open Data paradigm, is referred to as Open Research Data.<sup>10</sup>

## 2.2. Swiss context

[9] Aware of the importance of these challenges, Switzerland in 2021 adopted a National Strategy for Open Research Data (ORD)<sup>11</sup>, jointly developed by swissuniversities<sup>12</sup>, the ETH Domain, the Swiss National Science Foundation (SNSF) and the Swiss Academies of Arts and Sciences.<sup>13</sup>

[10] The National Strategy for ORD aims to facilitate access to research data and its reuse. This vision must be reflected in the development of practices based on the sharing of research data in Switzerland, in particular by regulating the services and infrastructure supporting researchers for this purpose.<sup>14</sup> The FAIR principles must be applied when dealing with publicly funded research data.<sup>15</sup> In particular, the National Strategy for ORD recognises that the generation, access and use of such data presents many legal, ethical and social challenges. Some are linked to the federalised structure of Switzerland, which results in cantonal, federal and sometimes international legal bases coexisting. These legal provisions govern both the processes involving data (from acquisition to reuse), as well as the different levels of responsibility incumbent on the people and entities involved.<sup>16</sup>

[11] Open Data policies are often implemented through incentive instruments. This is the case in Switzerland, in particular, of the funding rules of the Swiss National Science Foundation (SNSF), which provide that the recipients of subsidies undertake to ensure that the research results supported by SNSF resources will be made available to the public in an appropriate manner.<sup>17</sup> The

---

<sup>7</sup> MARK D. WILKINSON *et al.*, *The FAIR Guiding Principles for Scientific Data Management and Stewardship*, *Sci Data* 3, 160018 (2016), available here: <https://www.nature.com/articles/sdata201618>.

<sup>8</sup> The Swiss National Open Research Data strategy, which will be discussed in the following section, specifically refers to it (see fn 11).

<sup>9</sup> This is the case for the European Open Science Cloud and Horizon Europe projects.

<sup>10</sup> For a definition (at Swiss level), see below 2.2 and fn 11.

<sup>11</sup> Swiss National Strategy for Open Research Data of 23 April 2021, available here: [https://www.swissuniversities.ch/fileadmin/swissuniversities/Dokumente/Hochschulpolitik/ORD/Swiss\\_National\\_ORD\\_Strategy\\_fr.pdf](https://www.swissuniversities.ch/fileadmin/swissuniversities/Dokumente/Hochschulpolitik/ORD/Swiss_National_ORD_Strategy_fr.pdf). The concept of Open Research Data (ORD) is explained there as follows (p. 4): «By facilitating access to and reuse of research data, ORD promotes better, more efficient and powerful research for the benefit of society as a whole.»

<sup>12</sup> swissuniversities is the umbrella organisation for Swiss higher education institutions.

<sup>13</sup> See: <https://www.swissuniversities.ch/fr/themes/digitalisation/open-research-data/strategie-nationale-et-plan-daction>.

<sup>14</sup> Swiss National Strategy for Open Research Data, p. 4.

<sup>15</sup> See: <https://www.swissuniversities.ch/fr/themes/digitalisation/open-research-data/strategie-nationale-et-plan-daction>.

<sup>16</sup> Swiss National Strategy for Open Research Data, p. 10.

<sup>17</sup> Regulation of the Swiss National Science Foundation on research grant, Art. 47.

SNSF favours a bottom-up approach that consists of providing best practice guidelines and allows each scientific community to define and apply its own standards with great flexibility.<sup>18</sup> However, this approach has its limitations, since the binding nature of these strategies is limited and can be applied in a very different way within the Swiss scientific community.

[12] As an extension of the National Strategy for ORD, in August 2022, the Council of States' Science, Education and Culture Committee tabled a motion for the Federal Council to set up, in a framework law, the necessary bases to ensure that specific infrastructures for the reuse of data in strategic areas (including health and research) are rapidly developed and put in place.<sup>19</sup> The Federal Council noted the importance of the reuse of data, while recalling that it was not always easy to reconcile with the conditions set out in the Federal Data Protection Act (FDPA)<sup>20</sup> for data collection (determined and recognisable purposes for the data subject). Indeed, it is often difficult, if not impossible, to predict the usefulness that data could have if it were used for other purposes, at the time of its collection. The Federal Council therefore proposed to accept the motion and specify that it would focus in particular on the areas in which secondary use of the data would be relevant and proportionate, as well as the infrastructure and other prerequisites that would be necessary to exploit reliable and interoperable data spaces. The Swiss legal framework should therefore evolve in the future and have regulations on the reuse of data, particularly health data.

[13] In parallel with political developments, the Swiss scientific community is advancing data sharing nationwide and implementing projects that achieve the objectives of the National Strategy for ORD. In the field of biology, for example, one of the most ambitious projects is certainly the SwissBiodata ecosystem (SBDe), which currently involves a total of fifty-three platforms, facilities and research groups affiliated with eighteen Swiss institutions.<sup>21</sup> The SBDe project is based on the observation that Swiss universities and research institutes have largely developed their local data generation and data processing platforms and adopted the principles of open research data (ORD). However, the development of a national ORD strategy in Switzerland requires more effective data sharing and reuse. It is therefore essential to adopt common quality and operating standards and to establish close collaboration between the Swiss institutions and their experts. SBDe is considering a decentralised infrastructure that aims to address these challenges, thereby strengthening Switzerland's ability to convert research data into knowledge and innovation, with the aim of (i) increasing the quality, standardisation and efficiency of the data value chain (from data production to knowledge generation), by the federation of platforms; (ii) providing state-of-the-art support to the Swiss scientific community in making its data, methods, and software tools compliant with FAIR principles; and (iii) establishing new resources that will enhance Switzerland's international competitiveness and its position in the data infrastructure for life sciences.<sup>22</sup>

---

<sup>18</sup> See: <https://www.snf.ch/fr/FAiWVH4WvpKvohw9/dossier/points-de-vue-politique-de-recherche>.

<sup>19</sup> Motion 22.3890 of 28 August 2022 of the Council of States' Science, Education and Culture Committee, Development of a framework law on the reuse of data. Available here: <https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaefte?AffairId=20223890>.

<sup>20</sup> Federal Data Protection Act of 19 June 1992 (FDPA; RS 235.1).

<sup>21</sup> See: [https://www.sib.swiss/about/news/10943-the-swissbiodata-ecosystem-gains-further-traction?utm\\_source=LinkedIn&utm\\_medium=social&utm\\_campaign=organic&utm\\_content=SwissBioData-newpartners](https://www.sib.swiss/about/news/10943-the-swissbiodata-ecosystem-gains-further-traction?utm_source=LinkedIn&utm_medium=social&utm_campaign=organic&utm_content=SwissBioData-newpartners).

<sup>22</sup> See: <https://www.sib.swiss/pages/10890-swissbiodata-ecosystem-boosting-switzerland-s-data-intensive-research-in-life-sciences>.

### 2.3. Open Data and biomedical research

[14] Biomedical research, on which this article focuses, is directly confronted with incentives for Open Science and Open Data. This discipline encompasses the study of life processes, disease prevention and treatment, as well as environmental genetic factors related to disease and health.<sup>23</sup> It is in this field of research that medical informatics<sup>24</sup> and personalised medicine<sup>25</sup> have emerged, offering many prospects for the development of treatments.

[15] In 2017, the State Secretariat for Education, Research, and Innovation (SERI) launched the national incentive initiative for personalised medicine over a four-year period, which was renewed for another four years in 2021.<sup>26</sup> In this context, the SERI and the Federal Office of Public Health (FOPH) have entrusted the Swiss Academy of Medical Sciences (SAMS) and the SIB (Swiss Institute of Bioinformatics) to implement a Swiss Personalised Health Network (SPHN). The SPHN initiative contributes in particular to the development, implementation and validation of coordinated infrastructure to make health data for research in Switzerland interoperable.<sup>27</sup> It has also made it possible to establish a secure IT environment for the analysis and sharing of sensitive data guaranteeing data protection (BioMedIT infrastructure), which is made available to researchers throughout Switzerland.<sup>28</sup> The second incentive period for the SPHN initiative, initiated in 2021, focuses on consolidating this infrastructure.<sup>29</sup>

[16] From another perspective, the Federal Council Council in May 2022 published a long-awaited and important report entitled: «*Mieux utiliser les données médicales pour assurer l'efficacité et la qualité des soins*» (Humbel Report).<sup>30</sup> This report focuses on three main questions, namely (i) the potential for the reuse and exploitation of medical data, (ii) identifying the conditions to be met so that medical data can be reused by different groups of users and (iii) exploring the technical, organisational and legal developments to be initiated to enable the reuse of health data. The report proposes the establishment of a «data space» in the health sector, which must take into account technical, legal or semantic aspects, but also the development of a common culture of data

---

<sup>23</sup> See: <https://statesforbiomed.org/education/background-on-biomedical-research/biomedical-research-definitions/>.

<sup>24</sup> «Medical informatics» is the science of the systematic development, management, storage, processing and provision of data, information and knowledge in the field of medicine and the health system, through the use of computer theories, methods, procedures and techniques. SAMS Bulletin 2/15, p. 1, available here: [https://www.samw.ch/dam/jcr:bl69468a-9bcb-42c3-bf0d-853fda9eb67b/bulletin\\_assm\\_15\\_2.pdf](https://www.samw.ch/dam/jcr:bl69468a-9bcb-42c3-bf0d-853fda9eb67b/bulletin_assm_15_2.pdf).

<sup>25</sup> Personalised medicine is defined by the EU Health Ministers in their Council conclusions on personalized medicine for patients as follows: «A medical model using characterization of individuals' phenotypes and genotypes (e.g. molecular profiling, medical imaging, lifestyle data) for tailoring the right therapeutic strategy for the right person at the right time, and/or to determine the predisposition to disease and/or to deliver timely and targeted prevention» (see : [https://health.ec.europa.eu/medicinal-products/personalised-medicine\\_en](https://health.ec.europa.eu/medicinal-products/personalised-medicine_en)). See also Swiss Academies Communications, Vol. 14, no 6, 2019, Ch. 1 (available here: [https://www.samw.ch/dam/jcr:b4aad9d0-c7d9-4c2f-b998-7f3c4727e539/assm\\_2019\\_medecine\\_personnalisee\\_chapitre\\_1.pdf](https://www.samw.ch/dam/jcr:b4aad9d0-c7d9-4c2f-b998-7f3c4727e539/assm_2019_medecine_personnalisee_chapitre_1.pdf)).

<sup>26</sup> See: <https://www.sbf.admin.ch/sbf/fr/home/recherche-et-innovation/la-recherche-et-linnovation-en-suisse/initiative-nationale-dencouragement-de-la-medecine-personnalisee.html>.

<sup>27</sup> See: <https://sphn.ch/fr/home/>.

<sup>28</sup> See: [www.biomedit.ch](http://www.biomedit.ch).

<sup>29</sup> See: <https://www.sbf.admin.ch/sbf/fr/home/services/publications/base-de-donnees-des-publications/s-n-2021-2/s-n-2021-2h.html>.

<sup>30</sup> Report of the Federal Council following up on Humbel postulate 15.4225 of 18 December 2015, *Mieux utiliser les données médicales pour assurer l'efficacité et la qualité des soins* (free translation : «Better use of medical data to ensure efficiency and quality of care»), 4 May 2022, available here: <https://www.admin.ch/gov/fr/accueil/documentation/communiqués.msg-id-88631.html> (Humbel Report of 4 May 2022). For a summary, see: FRÉDÉRIC ERARD, Towards a new model for reusing medical data in Switzerland?, 2 July 2022, in: [www.swissprivacy.law/156](http://www.swissprivacy.law/156).

reuse. In particular, it underlines the need to clarify the data ownership regime, which could potentially be considered as a collective good if the data subjects consent.<sup>31</sup> The importance of complying with the FAIR principles is also highlighted.<sup>32</sup> At the end of the report, the Federal Council stresses the need to adapt the legal framework to establish a framework of trust and legal certainty allowing the reuse of data for various purposes.<sup>33</sup> The report, however, remains fairly vague on the legal aspects.

[17] Biomedical research uses different types of data, including personal data, whether or not related to health. The spectrum of data covered by biomedical research is very broad and includes, in particular in the context of personalised medicine, so-called «-omics» data, in reference to the suffix common to some of this data. For example, this term includes genomic data (resulting from techniques for studying the whole genome), transcriptomics (resulting from techniques for analysing mRNA<sup>34</sup> and the level of gene expression in a tissue), proteomics (relating to the composition of proteins in a tissue), and metabolomics (relating to metabolic products).<sup>35</sup>

[18] In general, it is important to stress that the encouragement of Open Science, in particular Open Data, does not therefore amount to imposing open access to research data on an unconditional basis. On the contrary, Open Research Data coexists with several legal regimes that aim, among other things, to protect the interests of the people whose data is being used. More broadly still, the Federal Council observes, as part of the Open Government Data Strategy in Switzerland, that «the publication of open access data must comply with the provisions on data protection, information security, copyright and professional secrecy».<sup>36</sup> The encounter between biomedical research, the legal framework in which it operates and encouraging Open Data can therefore create tensions.

### 3. Personal data protection constraints

[19] The fundamental right to the protection of privacy in the field of health is a widely recognised right, both by international conventions<sup>37</sup> or ethics<sup>38</sup> and by Swiss constitutional law.<sup>39</sup> In the field of health and research, the protection of the privacy of data subjects aims, in particular, to

---

<sup>31</sup> Humbel Report of 4 May 2022 (fn 30), p. 26.

<sup>32</sup> Humbel Report of 4 May 2022 (fn 30), p. 26 et seq.

<sup>33</sup> Humbel Report of 4 May 2022 (fn 30), p. 43.

<sup>34</sup> Acronym of Messenger Ribonucleic Acid. For a definition, see: [https://sciencesnaturelles.ch/covid19-vaccination-explained/mrna\\_vaccines/was\\_ist\\_eine\\_mrna\\_und\\_welche\\_funktion\\_hat\\_sie\\_](https://sciencesnaturelles.ch/covid19-vaccination-explained/mrna_vaccines/was_ist_eine_mrna_und_welche_funktion_hat_sie_).

<sup>35</sup> For more information, see the website of the Swiss Academy of Natural Sciences: [https://sciencesnaturelles.ch/personalized-health-explained/welche\\_methoden\\_werden\\_eingesetzt\\_/omcis](https://sciencesnaturelles.ch/personalized-health-explained/welche_methoden_werden_eingesetzt_/omcis).

<sup>36</sup> Open Government Data Strategy in Switzerland for the years 2019 to 2023, adopted by the Federal Council on 30 November 2018, p. 858 (free translation), (see: <https://www.bfs.admin.ch/bfs/en/home/services/ogd/strategy.html>).

<sup>37</sup> In particular: Art. 8 European Convention for the Protection of Human Rights and Fundamental Freedoms of 4 November 1950 (ECHR; RS 0.101); Art. 1 Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine of 4 April 1997 (Convention on Human Rights and Biomedicine; RS 0.810.2); Council of Europe Convention for the Protection of Individuals with regard to the Automated Processing of Personal Data of 28 January 1981 (ETS Convention 108; RS 0.235.1).

<sup>38</sup> e.g. World Medical Association (WMA) Declaration on Ethical Considerations regarding Health Databases and Biobanks, October 2016 (commonly referred to as the «Declaration of Taipei»).

<sup>39</sup> Art. 13 para. 2 of the Federal Constitution of the Swiss Confederation of 18 April 1999 (Cst.; RS 101), according to which everyone has the right to be protected against the misuse of their data.

protect them against misuse of their (sensitive) data, which could lead to forms of discrimination, for example. The need to regulate the processing of personal data relating to patients or research subjects also serves to preserve the public's confidence in science.

[20] The protection of the privacy of research subjects may conflict with the interests of biomedical research, the progress of which often depends on access to the personal data of research subjects. More generally, biomedical research has evolved over the past two decades marked by the increasing sharing of data. This is due in particular to technical advances, investments in infrastructure allowing data sharing, as well as the requirements of funding agencies in terms of Open Science.<sup>40</sup>

[21] However, the increase in research data sharing is not without consequences from the point of view of personal data protection. To ensure effective data sharing and reuse, it is, for example, necessary to establish systems for matching data. Data matching (record linkage) consists of linking or merging, using one or more matching variables, individual data on the same person from at least two sets of data.<sup>41</sup> The matching then generates the creation of new data sets offering more information about the data subject.

[22] This section provides a summary overview of the rules that may apply in the event of the provision of personal data for biomedical research purposes, with a view to Open Science.

### 3.1. Applicable legal framework and scope

[23] The processing of «personal data» triggers the application of relevant legislation regarding the protection of personal data. In Switzerland, the processing of data related to human research is subject to a fragmented legislative framework, consisting of general laws and special laws. From a general perspective, the Federal Data Protection Act, the full revision of which will take effect on 1 September 2023 (nFDPA)<sup>42</sup>, governs the processing of personal data by private persons (e.g., private foundations or laboratories) and federal bodies (e.g. the EPFL and ETHZ).<sup>43</sup> Conversely, the processing of personal data carried out by public cantonal bodies (e.g. university hospitals) is primarily governed by the various cantonal data protection laws.

[24] The main purpose of the general data protection laws is to protect the fundamental rights of data subjects by imposing obligations on data controllers (e.g., duty to comply with general principles, duty to inform, obligations to take technical or organisational security measures) or by recognising specific rights of data subjects (e.g. right to access their data, right to object to certain data processing operations).

[25] In parallel with the general data protection laws, so-called «special» legislation may impose specific rules related to certain types of personal data processing. According to the adage *lex specialis derogat legi generali*, special legal provisions in principle take precedence over so-called «general» laws. In terms of personal data protection, this is at least the case if the special regu-

---

<sup>40</sup> JANE KAYE, *The Tension Between Data Sharing and the Protection of Privacy in Genomics Research*, Annual Review of Genomics and Human Genetics 2012, p. 415 et seq., p. 417.

<sup>41</sup> On this subject and for a description of the different matching methods, see: Humbel Report of 4 May 2022 (fn 30), p. 12 et seq.

<sup>42</sup> FF 2020 7397 et seq.

<sup>43</sup> Art. 2 para. 1 let. b FDPA; Art. 2 para. 1 let. b nFDPA.

lation aims to specifically regulate data protection itself or if it offers at least equivalent protection.<sup>44</sup> In the context of biomedical research, the main special legislation is the Federal Human Research Act (HRA).<sup>45</sup> The provisions of the HRA are specified by two implementing orders, the Federal Human Research Act (HRO)<sup>46</sup> and the Clinical Trials Ordinance (ClinO).<sup>47</sup>

[26] The HRA establishes, among other things, special rules on the processing and reuse of data for the purposes of human research (see below 3.2). The provisions of the HRA apply, however, only to the extent that the activities concerned fall within its scope (Art. 2 HRA). The scope of the HRA is primarily limited to research, i.e. «methodological research aimed at obtaining generalisable knowledge»<sup>48</sup>, on human diseases and on the structure and functioning of the human body.<sup>49</sup> When data is involved, the scope of the HRA is furthermore limited to research carried out on «personal health-related data», with the exception of health-related data that has been collected anonymously or which is anonymised.<sup>50</sup> The act of anonymising data itself constitutes data processing, the performance of which may be subject to rules imposed by the HRA, such as the anonymisation of genetic data for research purposes.<sup>51</sup>

[27] It is also essential to ensure that the envisaged data sharing complies with the requirements imposed in terms of medical or research ethics. Research projects involving the reuse of personal health-related data are subject to the approval of an ethics committee (Art. 45 al. 1 HRA). The ethics committee must ensure, when evaluating a research project, that the ethical, legal and scientific requirements provided for by the HRA are met (Art. 45 para. 2 HRA). In terms of the provision and sharing of data, the reference text is certainly the 2016 World Medical Association (WMA) Declaration on ethical considerations regarding health databases and biobanks (often referred to as the «Declaration of Taipei»). Its purpose is to set out ethical principles for the collection, storage and use of identifiable data beyond the care provided to patients, in particular through its use in databases and biobanks. In particular, the Declaration of Taipei reiterates the need to preserve the principle of confidentiality necessary to maintain trust in databases (§ 10), as well as the need to ensure that the collection, storage and use of data are voluntary for those able to consent (§ 11). It lists the information that must be communicated to data subjects who consent to the reuse of their data for multiple and indefinite uses (§ 12). The ethical texts adopted at Swiss level include the Ethical Framework for Responsible Data Processing in Personalized Health Research, developed as part of the SPHN initiative.<sup>52</sup>

---

<sup>44</sup> DAVID ROSENTHAL, *Die rechtlichen und gefühlten Grenzen der Zweitnutzung von Personendaten*, sic! 2021 p. 168 et seq., p. 169.

<sup>45</sup> Federal Human Research Act of 30 September 2011 (HRA; RS 810.30).

<sup>46</sup> Human Research Ordinance of 20 September 2013 (HRO; RS 810.301).

<sup>47</sup> Clinical Trials Ordinance of 20 September 2013 (ClinO; RS 810.305).

<sup>48</sup> Art. 3 let. a HRA.

<sup>49</sup> Art. 3 let. b HRA defines «disease research» as «research on the causes, prevention, diagnosis, treatment and epidemiology of impairments of physical and mental health in human beings». Art. 3 let. c HRA defines «research on the structure and functioning of the human body» as «basic research, in particular on human anatomy, physiology and genetics, and non-disease-related research concerning interventions and impacts on the human body».

<sup>50</sup> Art. 2 para. 1 let. e and Art. 2 para. 2 let c. HRA.

<sup>51</sup> Art. 32 para. 3 HRA, which authorises the anonymisation of genetic data for research purposes only on the condition that the data subject or, if applicable, their legal representative or relatives, have not objected to it, after being informed.

<sup>52</sup> Available here: <https://sphn.ch/document/ethical-framework/>.

### 3.2. Opening data through anonymisation?

[28] The question of what does or does not constitute personal data is central since non-personal data processing operations fall outside the scope of the HRA and the general data protection laws. From an open data perspective, this means that research data that is not personal (i.e. anonymous in accordance with applicable law) can be made available to other researchers without regard to the constraints imposed by these laws, it being understood, however, that other rights are likely to prevent the free use of such data (exclusive rights, business secrets, etc.). In practice, the determination of the personal or non-personal nature of research data often leads to debate.

[29] Personal health data is defined by the HRA as «information relating to a specific or determinable person which relates to their state of health or disease, including genetic data».<sup>53</sup> Except for the fact that data must necessarily relate to health<sup>54</sup> to fall within the scope of the HRA, the definition of personal data within the meaning of the HRA is similar to that of the FDPA (even though the FDPA uses the terminology «identified/identifiable» instead of «determined/determinable»<sup>55</sup>). A person is determined when their identity is directly apparent from the information; they are determinable when the circumstances or context allow the person to be identified by correlation of information.<sup>56</sup>

[30] Unlike personal data, anonymous or anonymised data is data that cannot be linked to a specific person, or only at the cost of efforts considered disproportionate.<sup>57</sup> Art. 35 HRO specifies that anonymisation involves making permanently unrecognisable or destroying all information which, when combined, allows the identity of the person to be reestablished without disproportionate effort. The same provision states that at least the names, addresses, dates of birth and identifying identification numbers must be made unrecognisable or destroyed. The HRA and its orders do not define in more detail the indirect identifiers that should be taken into account to re-identify a person, nor do they provide for numerical thresholds below which re-identification is considered probable or admitted (e.g. 20 patients sharing the same characteristics)<sup>58</sup>. It is therefore appropriate to focus the analysis of the identifiable character of data on the efforts necessary to re-identify the person, which should not be considered disproportionate. Cost, time and work investment is expected to be taken into account.<sup>59</sup> In general, caution is recommended when health-related data is involved<sup>60</sup>, especially genetic data. Due to the particularly close link between this data and the data subject, the ever-increasing number of external sources with which

---

<sup>53</sup> Art. 3 let. f HRA.

<sup>54</sup> According to the Federal Council, the concept of health data is identical to that of Art. 3 let. c FDPA, see Federal Council Message of October 2019 on the Federal Human Research Act, FF 2009 7259 et seq. (HRA Message), p. 7310.

<sup>55</sup> Art. 3 let. a FDPA; Art. 5 let. a nFDPA. HRA Message (fn 54), 7311; HFG-VAN-SPYK/RUDIN/SPRECHER/POLEDNA, Art. 3 N 43, in: Bernhard Rütsche (publisher), *Humanforschungsgesetz (HFG)*, Bern 2015 (cit. SHK HFG-AUTHOR).

<sup>56</sup> Federal Council Message of 15 September 2017 regarding the federal law on the complete revision of the Federal Data Protection Act and on the amendment of other federal laws, FF 2017 6565 et seq. (cit. nFDPA Message), p. 6639. ATF 138 II 346 c. 6.1, JdT 2013 I 71. FRÉDÉRIC ERARD, *Les données codées dans le contexte de la recherche : personnelles ou anonymes?*, AJP/PJA 2021 p. 606 et seq., p. 608; ALEXANDRE JOTTERAND, *Personal Data or Anonymous Data: where to draw the lines (and why)?*, in: Jusletter, 15 August 2022, N 14 et seq.

<sup>57</sup> Art. 3, let. i. HRA.

<sup>58</sup> VALÉRIE JUNOD/BERNICE ELGER, *Données codées, non-codées ou anonymes : des choix compliqués dans la recherche médicale rétrospective*, in: Jusletter, 10 December 2018, N 16.

<sup>59</sup> HRA Message (fn 54), p. 7311.

<sup>60</sup> On the difficulties associated with the anonymisation of health data, see e.g. ROLF H. WEBER/DOMINIC OERTLY, *Aushöhlung des Datenschutzes durch De-Anonymisierung bei Big Data Analytics?*, in: Jusletter IT, 21 May 2015.

this data can be cross-referenced and ever more efficient technical and IT resources, the risks of re-identification are increased, in particular in states with small populations like Switzerland.

[31] In the context of biomedical research, personal data is also frequently processed in «pseudonymised» form or, to use the terminology of the HRA, in «coded» form. This form of processing is explained not only by compliance with the principle of data minimisation and security, but also because the HRA facilitates the reuse of data which is in coded form (see below 3.3.1) and, above all, pseudonymisation makes it possible to go back to the research subject concerned, which may often be useful in carrying out additional investigations. From a legal point of view, pseudonymisation and coding within the meaning of the HRA are synonyms. Data is considered to be coded if it can only be linked to a specific person by means of a key.<sup>61</sup> To be properly coded, the data must appear as anonymised from the point of view of a person who does not have the key to match the original data.<sup>62</sup>

[32] The question of whether coded or pseudonymised personal data still constitutes personal data with regard to the recipient who does not have the match key has given rise to considerable doctrinal debate in Switzerland and Europe.<sup>63</sup> From a dogmatic point of view, the authors of doctrine generally have a tendency to contrast the absolute and relative approaches. According to the absolute approach, it suffices that a single actor in the communication (provider or recipient) be able to re-identify the data subject for the data to be considered personal with regard to all. Conversely, according to the relative approach, pseudonymised or coded data is personal data only with respect to those who are able to re-identify the person, i.e. in principle, the persons in possession of the match key if the data has been correctly pseudonymised.

[33] From the perspective of general data protection laws, Swiss doctrine<sup>64</sup> and certain cantonal courts<sup>65</sup> now tend to favour the relative approach. It is also the position of the Federal Council in its message relating to the future Federal Data Protection Act.<sup>66</sup> While this approach can be convincing for ordinary processing of personal data, it must be rejected for processing of data falling within the scope of the HRA. The HRA establishes a legal regime allowing the easier reuse of personal data for research purposes (Arts. 32 to 34 HRA, see 3.3.1 below). However, this regime directly regulates the processing of coded data, in particular by limiting the purpose for which such data may be processed (a research project or for research purposes in general and not for other purposes). In this context, accepting that coded research data would be anonymous

---

<sup>61</sup> Art. 3 let. h HRA.

<sup>62</sup> Art. 26 para. 1 HRO.

<sup>63</sup> On this subject: JOTTERAND (fn 56), N 17 et seq. and the references cited.

<sup>64</sup> e.g. DAVID ROSENTHAL/SAMIRA STUDER/ALEXANDRE LOMBARD (for the translation), *La nouvelle loi sur la protection des données*, in: Jusletter 16 November 2020, N 20; DAVID ROSENTHAL/YVONNE JÖHRI, *Handkommentar zum Datenschutzgesetz*, Zurich 2008, Art. 3 let. a N 36; BEAT RUDIN, in: Bruno Baeriswyl/Kurt Pärli (publisher), *Datenschutzgesetz (DSG)*, Bern 2015, Art. 3 N 14; CÉLIAN HIRSCH/EMILIE JACOT-GUILLARMOD, *Les données bancaires pseudonymisées – Du secret bancaire à la protection des données*, *Revue suisse de droit des affaires et du marché financier (RSDA)* 2020 p. 151 et seq., p. 160–161.

<sup>65</sup> Zurich Handelsgericht, HGer ZH, HG150170, 30 March 2017, c. 5.3.5 (in a case relating to the communication of bank data to the US tax authorities). According to the decision, however, it was up to the bank sending the data to prove that it had taken sufficient measures against re-identification, which it failed to do in this case. Moreover, the decision underlined that the technologies available (in particular big data) left little room for irreversible anonymisation.

<sup>66</sup> nFDPA Message (fn 56), p. 6640: «The law does not apply to data that has been anonymised if re-identification by a third party is impossible (the data has been completely or definitively anonymised) or only seems possible at the cost of such efforts that no interested party will attempt it. The latter rule also applies to pseudonymised data» (free translation).

from the point of view of the recipients would have the inadmissible effect of excluding them from the scope of the HRA (since the HRA does not apply to anonymous or anonymised data processing). The recipients of the data would no longer be bound by the requirements imposed by the HRA and could, for example, avoid adopting the technical and organisational measures for the storage of research data imposed by Art. 43 HRA.<sup>67</sup> It should therefore be considered that the coded data remains personal data with regard to the recipients if the activities concerned fall within the scope of the HRA<sup>68</sup>.

[34] Interestingly, some authors suggest moving away from the purely binary approach of absolute and relative theories. According to JOTTERAND, the central element of the analysis of the personal nature or not of data would mainly be based on the (dynamic) environment of the data holder.<sup>69</sup> Data would therefore be personal if the data holder has the additional data to re-identify the data or, if it does not have it, if it exists and it is likely to be able and willing to obtain it in order to re-identify the data subject. Conversely, if the additional data required for re-identification does not exist, or the data exists, but it seems unlikely that the holder of the data will attempt to obtain it to re-identify the individual, then the data should not be considered personal from the latter's point of view. In this system, it is the responsibility of the data controller who transfers pseudonymised data to take all necessary measures, in particular contractual measures, to ensure that what is not authorised for the data controller does not become permissible because it has communicated the data to a third party who does not have the re-identification key, i.e. a third party for whom the data is anonymous.<sup>70</sup> With regard to the specific context of the HRA, JOTTERAND notes that the approach chosen should not lead to circumventing the protective rules of the HRA. He nevertheless rejects a purely absolute approach and argues that an approach based on the analysis of the environment of the data processor (in particular the recipient) is also transposable to the HRA regime. Therefore, according to this author, a researcher who receives coded data is directly subject to the HRA and can only conduct their research if all of the conditions imposed by the HRA are met. However, if the researcher can reasonably consider that the data received is completely anonymised, they can conduct their research without any further formalities.<sup>71</sup> This approach is sound in itself, but its practical implication seems limited, at least if the data come from a Swiss research institution. Indeed, the institution making available the research data (in coded form) should do so only if all the legal conditions for reuse are met, in particular the approval of the project by an ethics committee (Art. 45 al. 1 HRA). However, this approval can only be obtained by submitting a research protocol that describes precisely how the data will be processed, in particular if it will be coded. In this configuration, it seems unlikely that the researcher will come into possession of coded data while believing in good faith that it is completely anonymised.

[35] In summary, the anonymisation of personal data can, of course, be a way to remove the constraints imposed by data protection legislation, but it must be handled with great caution, in particular due to the close link of this data with the data subjects. The precautionary recommendation is especially true for pseudonymised/coded data in the context of human research,

---

<sup>67</sup> For a more substantiated argument in this regard: ERARD (fn 56), p. 613 et seq.

<sup>68</sup> In a similar direction: ROSENTHAL (fn 44), p. 169.

<sup>69</sup> JOTTERAND (fn 56), N 46.

<sup>70</sup> JOTTERAND (fn 56), N 61.

<sup>71</sup> JOTTERAND (fn 56), N 78.

which should continue to be considered as personal data when the HRA applies. Finally, the action of anonymising data may also be subject to specific rules (e.g. prior information and non-objection of the data subject for the anonymisation of genetic data for research purposes according to Art. 32 para. 3 HRA).

### 3.3. Reuse of personal data, in particular for human research purposes

#### 3.3.1. HRA Regime

[36] The concept of «reuse» of data is at the heart of the concept of Open Data. However, when personal data is involved, reuse of data may undermine the general principle of purpose. According to this principle, processing complies with the purpose principle when the data subject is informed of it, when the processing is provided for by law or when it is clear from the circumstances.<sup>72</sup> During each «reuse» of personal data,<sup>73</sup> it is therefore necessary to ensure that the reuse complies with the applicable legal requirements, so as to comply with the general principle of lawfulness. For the reuse of data for research purposes, it is necessary to distinguish between uses that fall within the scope of the HRA (Art. 2 HRA) from other uses for research purposes.

[37] In the event that the reuse of personal health-related data is envisaged for the purpose of human research, Articles 32 to 34 HRA provide for easier reuse conditions. The system is, however, established according to rules that are complex to say the least, which depend on the type of data (genetic or non-genetic) and its form (non-coded, coded or anonymised).<sup>74</sup> These reuse rules, which also govern the reuse of biological material, presuppose that the data has already been collected, for example in a healthcare context. The data may also have been collected in a preliminary research project, in the event that the envisaged reuse exceeds the consent initially given by the data subject.<sup>75</sup>

[38] Without going into details, the systematics established by the HRA require that specific consent for a particular research is necessary when the reuse involves non-coded genetic data (Art. 32 para. 1 HRA).<sup>76</sup> A so-called «general» consent for research purposes – i.e. not limited to any particular research – is allowed under Swiss law for the reuse of coded genetic data (Art. 32 para. 2 HRA) and non-genetic non-coded data (Art. 33 para. 1 HRA). With regard to the reuse of coded non-genetic data, the HRA acknowledges that a right to object after information is sufficient (Art. 33 para. 2 HRA). However, for ethical reasons, hospitals that provide general consent waive the application of separate rules for non-genetic data solely because it is coded or non-coded.<sup>77</sup> In practice, reuse of coded non-genetic data is therefore also subject to prior general consent. Finally, Art. 34 HRA still provides for an exception regime in situations where the requirements of Arts. 32 and 33 HRA are not met and several conditions are met, namely the impossibility or the

---

<sup>72</sup> nFDPA Message (fn 56), p. 6640.

<sup>73</sup> Art. 24 HRO defines reuse as: «any handling, for research purposes, of biological material already sampled or data already collected». On the concept of reuse in the context of the HRA: SHK HFG-RUDIN (fn 55), Vorbemerkungen Art. 32–35, N 4 et seq.

<sup>74</sup> For a review of the system: VALÉRIE JUNOD/BERNICE ELGER (fn 58), N 16 et seq.

<sup>75</sup> SHK HFG-RUDIN (fn 55), Vorbemerkungen Art. 32–35, N 4.

<sup>76</sup> Consent may also be valid for several specific projects: SHK HFG-RUDIN (fn 55), Art. 32, N 6.

<sup>77</sup> See e.g. the general consent form template proposed by swissethics: <https://swissethics.ch/en/templates/studieninformationen-und-einwilligungen>.

disproportionate difficulties in obtaining the data subject's consent, the absence of a document attesting to the data subject's refusal and the preponderance of the interest of science over that of the data subject in deciding whether to reuse their data.<sup>78</sup>

[39] If the processing of anonymous data falls in principle outside the scope of the HRA, Art. 32 para. 3 HRA nevertheless provides for a special regime for the anonymisation of genetic data for research purposes. Provided that the envisaged anonymisation is technically possible for the genetic data concerned, anonymisation for research purposes is only allowed if the data subject (or their representative) has not objected to it after having been informed.<sup>79</sup>

[40] General consent is an interesting tool from the point of view of data sharing and reuse by third parties. The law allows data subjects to consent to the use of their data in the strict context of human research, but without knowing in advance what specific research their data will be used for. By authorising the use of general consent, the HRA reduces the obligation to strictly comply with the purpose principle. Insofar as this is «consent», it can also be revoked. Where appropriate, Art. 10 HRO provides that personal health-related data «must be anonymised after having been analysed». However, anonymisation is not necessary if the data subject expressly waives it or if it is evident from the start of the research project that anonymisation is not possible and the person has been sufficiently informed at the time of participating in the project.

[41] Although general consent as such is now widely accepted in Switzerland, it is not exempt from criticism. First of all, the wording of general consent may vary from hospital to hospital, which is likely to create uncertainties in research projects using data collected from different hospitals. TALANOVA/SPRECHER, for their part, make several criticisms of the wording currently used, which would, among other things, weaken the rights of research subjects.<sup>80</sup>

[42] While recognising the need to obtain the free consent of data subjects to reuse their data for research purposes, the Federal Council recently considered that general consent should be upgraded to improve the potential for reuse and exploitation of health data.<sup>81</sup> According to a first option,<sup>82</sup> the data subjects could electronically consent to the primary use of their data and would be informed of the possible reuse of their data during the initial collection. They will then receive electronic information on the envisaged reuses and would be offered the possibility to object to such reuses on a case-by-case basis (opt out system). According to a second option,<sup>83</sup> presented as an alternative, the data subjects could voluntarily give their newly collected data for unspecified free reuse, provided that no commercial interest is pursued. The use of the data would be authorised for purposes that would exceed the strictly limited framework of human research. It should be noted that, in the context of current law, «dynamic» consent, i.e. allowing

---

<sup>78</sup> On this exception clause, see in particular: DOMINIQUE SPRUMONT/VLADISLAVA TALANOVA, *La recherche sans consentement : l'exceptionnelle exception*, in: Evelyne Clerc/Jean-Philippe Dunand/Dominique Sprumont (publisher), *Alea jacta est: Santé! Mélanges en l'honneur d'Olivier Guilloid*, Basel 2021, p. 235 et seq.; SUSANNE DRIESSEN/ANDRI CHRISTEN/PIETRO GERVASONI, *Humanforschung, Weiterverwendung und informierte Einwilligung. Analyse zur Weiterverwendung von gesundheitsbezogenen Personendaten und biologischem Material sowie Anwendung von Artikel 34 HFG*, in: Jusletter 1 February 2021.

<sup>79</sup> The information that must be given in this case is described in Art. 30 HRO.

<sup>80</sup> VLADISLAVA TALANOVA/Franziska Sprecher, *Le consentement général : points à améliorer*, *Bulletin des médecins suisses*, 16 September 2020, available here: <https://bullmed.ch/article/doi/bms.2020.19143>.

<sup>81</sup> Humbel Report of 4 May 2022 (fn 30), p. 34.

<sup>82</sup> Humbel Report of 4 May 2022 (fn 30), p. 39.

<sup>83</sup> Humbel Report of 4 May 2022 (fn 30), p. 40.

data subjects to be offered research projects and to decide on a case-by-case basis whether they intend to make their data available, is in principle already admissible.<sup>84</sup>

[43] An update of general consent may certainly be considered with a view to improving open data. Nevertheless, caution should be exercised. Following its introduction in 2014, general consent is now the subject of a high acceptance rate in patients<sup>85</sup> and has the advantage of respecting the wishes of people who refuse to have their data used for research purposes, in accordance with the constitutional principle that a research project can in principle only be carried out if the person participating in it has consented to it (Art. 118b al. 2 let. a Cst.).<sup>86</sup> In the event of a review or modernisation of general consent, it will be essential to ensure that the consent of its substance is not empty and that consent is consistent with international ethical standards, in particular the rules imposed by the Declaration of Taipei.

[44] Finally, it should be noted that personal data that has been collected for research purposes or that has been reused within the meaning of the HRA cannot then be communicated for other purposes except under specific conditions. According to Art. 41 HRA, such communication is only admissible if a legal basis provides for it or if the data subject has given informed consent «in the particular case». In light of this provision, general consent cannot therefore cover other purposes than those of the research.

### 3.3.2. Non-HRA Regime

[45] The reuse of biomedical data may involve purposes other than human research within the meaning of the HRA, in which case the HRA does not apply. This applies, for example, to the reuse of data for quality assurance purposes, such as the evaluation of a process applied in the treatment of post-partum haemorrhages (introduced on the basis of a study) or the safety assessment of a national guideline based on published studies.<sup>87</sup> In such cases, it is necessary to identify the applicable legal rules, starting with the general laws on the protection of personal data.

[46] In light of the new FDPA, for example,<sup>88</sup> reuse of data is in principle acceptable if it is compatible with the purposes for which the data was collected. However, there are no criteria in this Act to be used. According to the Federal Council, further processing is incompatible with the purposes of collection if the data subject can legitimately consider it to be «unexpected, inappropriate or questionable».<sup>89</sup> If we refer to Art. 5 para. 4 let. b of the international Convention for the Protection of Individuals with regard to the Processing of Personal Data (Convention 108+) and in particular its explanatory report, it is necessary to carry out a compatibility test of the

---

<sup>84</sup> SHK HFG-RUDIN (fn 55), Art. 32, N 19. For a detailed analysis of the issue: JULIAN MAUSBACH, *Dynamische Einwilligung. Gedanken und Fragen zu einem neuen Einwilligungskonzept für die Forschung am Menschen*, in: Jusletter 27 January 2020.

<sup>85</sup> SPRUMONT/TALANOVA, (fn 78), p. 249.

<sup>86</sup> In this regard, with a discussion taking into account the ethical principles governing the practice of human research: SPRUMONT/TALANOVA, (fn 78).

<sup>87</sup> On the issue of the distinction between quality assurance and research subject to authorisation, see the guidelines issued by swissethics, available here: <https://swissethics.ch/en/news/2020/02/04/qualitaetssicherung-oder-bewilligungspflichtige-forschung>.

<sup>88</sup> Art. 6 para. 3 nFDPA.

<sup>89</sup> nFDPA Message (fn 56), p. 6645.

purposes.<sup>90</sup> The compatibility test must, among other things, take into account the links between the initial purpose and the subsequent purpose of the processing, the context of the collection and the reasonable expectations of the data subjects, the nature of the data, the consequences of further processing for the data subject or the existence of appropriate safeguards. The test must be conducted in the light of all the circumstances of the case. It should be noted, however, that health-related data is sensitive data and that secondary processing of such data may easily be inconsistent with the reasonable expectations of the data subjects. In this context, it is therefore necessary to be careful when carrying out the compatibility test.

[47] Reuse of personal data incompatible with the initial processing is not prohibited, but results in a personality infringement of the data subjects and must therefore be based on a justified reason.<sup>91</sup> The latter may in any case rest on a legal basis authorising the reuse of data. In principle, the derogation from the general principle of purpose may also be justified by the consent of the person or, in cases where the processing is carried out by a private person subject to the FDPA, by an overriding private or public interest.<sup>92</sup>

[48] The FDPA and the nFDPA<sup>93</sup> contain provisions that facilitate, under certain conditions, the processing of personal data for purposes that do not relate to one or more individuals as such, but to a group of individuals (processing of personal data for research, statistical or planning purposes).<sup>94</sup> In such situations, personal data is processed without any relation to the data subject.<sup>95</sup> The legal requirements for this type of reuse vary according to the applicable law and the type of data controller (private person or public body). For example, Art. 31 para. 2 let. e nFDPA requires private data controllers who wish to rely on this reason to ensure that the data is anonymised as soon as possible, that the data is communicated to third parties only in a form that does not allow the data subject to be identified (or, if not possible, that measures are taken to ensure that the recipient processes the data only for purposes not related to individuals) and that the results are published in a form that does not allow the data subjects to be re-identified. Anonymity must be preserved not only at the time of communication or publication, but also as long as it can reasonably be assumed that third parties would have an interest in re-identifying the data subjects and that they would have or could acquire the means to do so.<sup>96</sup> A federal public body may, for its part, process data for purposes not relating to individuals under the conditions laid down by Art. 39 nFDPA, it being understood that the envisaged processing should in principle be based on a legal basis under the principle of lawfulness (Art. 34 nFDPA). However, Art. 39 para. 2 nFDPA waives the requirement of the formal nature of the legal basis in the situations covered by Art. 34 para. 2 nFDPA, especially when processing sensitive data is involved. It should be noted that most of the cantonal data protection laws, applicable to public cantonal bodies, also

---

<sup>90</sup> Council of Europe, Convention 108 + Convention for the Protection of Individuals with regard to the Processing of Personal Data, Explanatory Report, 2018 N 49.

<sup>91</sup> Art. 12 para. 2 let. a *cum* Art. 13 FDPA; Art. 30 al. 2 let. a *cum* 31 nFDPA. ROSENTHAL (fn 44), p. 173.

<sup>92</sup> Art. 13 FDPA; Art. 31 nFDPA.

<sup>93</sup> Art. 13 para. 2 let. e and Art. 22 FDPA; Art. 31 para. 2 let. e and 39 nFDPA.

<sup>94</sup> According to the Federal Council Message on the nFDPA, the scope of this justification does not appear to be limited to processing activities related to research, planning or statistics, but extends to any type of processing of personal data for purposes not related to individuals. nFDPA Message (fn 56), p. 6692.

<sup>95</sup> DAVID ROSENTHAL/SAMIRA STUDER/ALEXANDRE LOMBARD (fn 64), N 42; ROSENTHAL (fn 44), p. 173.

<sup>96</sup> ROSENTHAL (fn 44), p. 173.

contain provisions for similar purposes, but their content and conditions vary from one canton to another.<sup>97</sup>

[49] From an Open Data perspective, we believe that the legal provisions allowing data processing for purposes not related to individuals may be an interesting avenue for research not related to data subjects, for example for quality assurance purposes. For this reuse regime to apply, it is nevertheless essential that the reuse does not fall within the scope of the HRA (which would then apply as a special law). In addition, the application of this data reuse regime faces several constraints when data is involved:

- The provisions authorising the reuse of data for purposes not related to individuals do not make it possible to derogate from the special legal obligations of confidentiality, such as professional secrecy (Art. 321 Swiss Criminal Code). In other words, a doctor must be limited to communicating data in the situations provided for by Art. 321 Swiss Criminal Code (consent, legal provision specifically derogating from professional secrecy or lifting of confidentiality by the competent cantonal authority). They cannot therefore rely on the general provisions for reusing data for purposes not related to individuals to communicate personal data covered by secrecy to third parties. Such communication is nevertheless possible if the data is anonymous (or correctly pseudonymised, since the HRA would not apply, see above 3.2), so that the recipient is not able to re-identify the data subject.<sup>98</sup>
- Genetic data from an analysis falling within the scope of the Federal Act on Human Genetic Testing (HGTA)<sup>99</sup> may only be used for a purpose other than the purpose of the initial analysis if the data subject has freely and expressly consented to the proposed reuse, even if the data is in coded form (Art. 12 para. 1 HGTA). Use for another purpose in anonymised form is only possible if the data subject has been informed of this and has not objected to it (Art. 12 para. 2 HGTA). As a special provision, Art. 12 HGTA takes precedence over the provisions authorising the reuse of data for purposes not related to individuals.

[50] Finally, since the reuse or the provision of personal data for processing not related to individuals constitutes in principle a form of data processing activity, the data controller is generally obliged to provide sufficient information to the data subjects, in accordance with its obligation to respect the principle of transparency.<sup>100</sup> Determining whether information is necessary and the extent of this information are issues that need to be analysed on a case-by-case basis.

### 3.4. Need to adopt a contractual framework when sharing personal data

[51] A data controller who intends to share personal data with a third party who would like to use it for biomedical research purposes cannot limit itself to verifying that the legal conditions allowing such sharing are met. As the data provider is also required to comply with obligations imposed by law regarding the protection of personal data, particularly with regard to research

---

<sup>97</sup> e.g. Art. 24 Vaud Law on the Protection of Personal Data, RS VD 172.65; Art. 41 Geneva Law on Public Information, Access to Documents and Protection of Personal Data, RS GE A 2 08.

<sup>98</sup> FRÉDÉRIC ERARD, *Le secret médical. Etude des obligations de confidentialité des soignants en droit suisse*, Zurich 2021, N 465.

<sup>99</sup> Federal Act on Human Genetic Testing of 8 October 2004 (HGTA; RS 810.12).

<sup>100</sup> Art. 14 FDPA; Art. 19 nFDPA.

subjects, it must take all necessary measures to continue to be able to fulfil its obligations after sharing the data with a third party. For example, if the provider of personal data is only authorised to process the data for specific purposes, it must ensure that the data recipient will not use it for any other purpose unless permitted by applicable law. This is usually done by entering into a contract between the data provider and the data recipient. The relevant contractual clauses may then be included in a specific data sharing contract (e.g. Data Transfer and Use Agreement, Data Transfer Agreement) or be incorporated into larger contracts (e.g. Consortium Agreement, Research Agreement). In Switzerland, the SPHN has developed contract templates to facilitate the sharing of research data.<sup>101</sup>

[52] The establishment of the clauses necessary for the sharing of data in the context of human research depends on various factors, such as the status of the parties (controller or processor) or their function (data collector, data provider, data recipient, data owner).<sup>102</sup> A detailed review of issues related to establishing the contractual framework for sharing research data can be found in a contribution from JOTTERAND/ERARD,<sup>103</sup> to which we refer. We are limiting ourselves here to briefly and non-exhaustively mentioning some themes that should be agreed on by the parties:

- Scope of processing<sup>104</sup>: the parties should clearly determine the purposes of the processing by the recipient, so as to ensure that the data will not be used for unlawful purposes (e.g. processing for insurance purposes whereas the data is to be reused for research purposes in accordance with Arts. 32 to 34 HRA).
- Data guarantees: in order to limit its legal risks, the data recipient must ensure that the data it receives has been collected and is shared in accordance with all applicable legal provisions. This is reflected by guarantees from the data provider.
- Distribution of obligations imposed by data protection law<sup>105</sup>: data controllers are required to comply with a series of obligations under data protection law, whether in obtaining consents or authorisations, reporting a security breach to the authority or ensuring the exercise of the rights of data subjects (e.g. the right to access their data). It is essential that the parties to data sharing agree on the sharing of these responsibilities.
- Security measures<sup>106</sup>: since the data provider is in principle directly responsible for data processing with regard to data subjects, it has every interest in contractually imposing security or minimisation measures on the data recipient, in such a way as to limit the risks of negligent processing.

[53] The need for the parties (both the provider and the recipient) to adopt a contractual framework for the sharing of personal data and to continue to ensure respect for the rights of data subjects after data sharing has the effect of limiting the free sharing of personal data. It is in fact necessary to maintain a link between the data subject and the end user of the personal data, for

---

<sup>101</sup> Available here: <https://sphn.ch/services/dtua>. See also: ALEXANDRE JOTTERAND/FRÉDÉRIC ERARD, Recherche sur l'être humain et données personnelles. Gestion des échanges et répartition des responsabilités, in: Jusletter 30 August 2021, N 90.

<sup>102</sup> JOTTERAND/ERARD (fn 101), N 92.

<sup>103</sup> JOTTERAND/ERARD (fn 101).

<sup>104</sup> JOTTERAND/ERARD (fn 101), N 94.

<sup>105</sup> JOTTERAND/ERARD (fn 101), N 95.

<sup>106</sup> JOTTERAND/ERARD (fn 101), N 97.

example to ensure that the withdrawal of a general consent actually results in the exclusion of the provision of the data concerned in accordance with legal requirements.<sup>107</sup> In other words, data protection requirements do not combine well with «chain» reuses of personal data, which make it particularly difficult to exercise the rights of data subjects. Therefore, if personal data is to be shared for open science purposes, it should preferably be shared from a single access point ensuring controlled access.

### 3.5. Use of Privacy Enhancing Technologies (PETs)

[54] Without being limited to the field of biomedical research, the constraints currently imposed by data protection legislation have led research environments, particularly those related to computer technology and cryptography, to develop and propose models and technologies that should allow personal data to be processed and/or shared in a more privacy-friendly manner. These technologies are generally referred to as Privacy Enhancing Technologies (PETs).

[55] Since the question of sharing sensitive data on a large scale is a central issue in the biomedical research sector and the application of regulatory constraints can have the negative consequences of complicating or delaying the completion of research projects, special efforts have been made in recent years to propose privacy-friendly sharing solutions in this specific sector. The following methods, with their benefits and risks, are described, for example, by SCHEIBNER *et al.*<sup>108</sup>:

- *k-anonymity*: an anonymisation method aimed at reducing the possibilities of re-identification by establishing a model that guarantees that for each combination of identifiers, there are at least a certain number (k) of individuals who share the same attributes.<sup>109</sup> However, the efficacy of this method is limited.
- Decentralised analysis model: research data does not leave the sites (e.g. hospitals) and statistical analyses are carried out in a decentralised manner. Only the results are sent to the central institution, which gathers them and carries out a meta-analysis.<sup>110</sup>
- Federated analysis and learning model: this is an evolution of the decentralised model, in which the sites that make the data available train a common (global) learning model made available by the central research site on their own data. Sites then send updated versions of their model to the central research site, which then updates the global model. Once reconfigured, the global model is sent back to the sites and the process is repeated until the global model converges.<sup>111</sup>

---

<sup>107</sup> Art. 10 HRO.

<sup>108</sup> JAMES SCHEIBNER *et al.*, *Revolutionizing Medical Data Sharing Using Advanced Privacy-Enhancing Technologies: Technical, Legal, and Ethical Synthesis*, *Journal of Medical Internet Research*, Vol. 23/2 (2021), 25 February 2021, available here: <https://www.jmir.org/2021/2/e25120/>.

<sup>109</sup> SCHEIBNER *et al.* (fn 108), p. 3.

<sup>110</sup> SCHEIBNER *et al.* (fn 108), p. 3–4.

<sup>111</sup> SCHEIBNER *et al.* (fn 108), p. 4.

- Homomorphic encryption: this particular type of encryption allows for calculations directly on encrypted data, without having to decrypt it.<sup>112</sup> Although it only allows for a limited number of calculations, this type of encryption can now be used in real situations.<sup>113</sup>

[56] Technological developments in computing and cryptography can offer particularly attractive prospects for facilitating and enabling data sharing (or sometimes of analysis results). However, the use of such methods or models does not exempt data controllers from ensuring that they meet all the applicable legal requirements.

### 3.6. Excursus: European Health Data Space project in Europe

[57] While this contribution focuses primarily on Swiss law, the topic in question requires a slight deviation towards the European Union, which counts among its many regulatory projects related to data a project which should precisely facilitate the use of health data: the European Health Data Space (EHDS) project.<sup>114</sup> It has two main objectives. First of all, the aim will be to improve the use of data, i.e. digital access to and control over electronic personal health data, while facilitating its free movement (primary use). Secondly, the aim of the project is to implement a coherent, reliable and effective mechanism for the use of health data for research, innovation, and policy and regulatory development (secondary use).<sup>115</sup>

[58] The EHDS is part of the European Data Strategy, which aims to create a single market for data which must guarantee global competitiveness and data sovereignty.<sup>116</sup> It follows on from the General Data Protection Regulation (GDPR)<sup>117</sup>, the Data Governance Act<sup>118</sup>, the draft Data Act<sup>119</sup> and the Directive on the Security of Networks and Information Systems.<sup>120</sup> A proposal for a European regulation on health data, which has already been the subject of an impact assessment and an open public consultation, is currently under discussion at the Council of the European Union.<sup>121</sup>

[59] Chapter IV of the proposed regulation concerns the reuse of health data. Art. 33 compiles a list of electronic health data that holders make available for secondary use. It is specified in Art. 33 para. 4 that electronic health data including protected intellectual property rights and

---

<sup>112</sup> SCHEIBNER *et al.* (fn 108), p. 5.

<sup>113</sup> For examples of applications using this encryption method: MedCo system (<https://medco.epfl.ch/>) and Tune Insight (<https://tuneinsight.com/>).

<sup>114</sup> EHDS is the acronym for the European Health Data Space.

<sup>115</sup> [https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space\\_en](https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en).

<sup>116</sup> <https://digital-strategy.ec.europa.eu/en/policies/strategy-data>.

<sup>117</sup> 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, GDPR).

<sup>118</sup> Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European Data Governance and amending Regulation (EU) 2018/1724.

<sup>119</sup> Procedure 2022/0047/COD, Proposal for a regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act).

<sup>120</sup> Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to ensure a high common level of security of network and information systems within the Union.

<sup>121</sup> Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space of 3 May 2022, Procedure 2022/0140/COD.

business secrets of protected private companies are made available for secondary use and that all necessary measures are taken to safeguard these rights.

[60] Art. 34 of the proposed regulation determines the purposes for which electronic health data may be processed for secondary use. The list includes development and innovation activities for products or services contributing to public health or social security, or to ensuring a high level of quality and safety of health care, medicines or medical devices (Art. 34 para. 1 let. f), as well as the training, testing and evaluation of algorithms, among others in medical devices, artificial intelligence systems and digital health applications, contributing to public health or social security, or to ensuring a high level of quality and safety of health care, medicines or medical devices (Art. 34 para. 1 let. g).

[61] The proposed regulation therefore provides for an obligation to make health data available for reuse for purposes other than research. These two provisions were the subject of comments from the European Data Protection Board and the European Data Protection Supervisor in their joint opinion on the proposed regulation. They expressed some concern, considering that the purposes were not strictly enough defined.<sup>122</sup> Art. 35 of the proposed regulation introduces a ban on requesting access to and processing such data for certain purposes. The list of purposes covers the advertising, marketing and development of products or services that may harm people, such as illegal drugs, alcoholic beverages and tobacco products.

### **3.7. Interim observations and brief considerations on the legal architecture of the reuse of data for research purposes**

[62] Data protection and opening of data are not incompatible, but the requirements related to the protection of personal data subject the access and sharing of such data to compliance with conditions that are at the very least restrictive. Indeed, even though Swiss law offers conditions for easier reuse of data for the purposes of human research (Arts. 32 to 34 HRA), the sharing of such data must, for example, be based on the authorisation of a research ethics committee and be subject to a contractual agreement between the parties concerned. Anonymisation of data, if possible or authorised, would certainly exclude the processing and sharing of such data from the scope of the HRA and data protection laws, but such anonymisation is not always adequate to pursue the objectives of human research (need to get back to the patient if necessary), sometimes involves compliance with legal requirements (information and absence of refusal to reuse genetic data for research purposes) and may pose significant practical difficulties depending on the nature of the data (e.g. anonymisation of genetic data). As the legal provisions relating to human research (HRA) also regulate data processing in coded (or pseudonymised) form, they therefore have a particularly broad scope of application, which also applies to processing carried out by persons who do not have the key making it possible to trace the data subjects. As a result, personal data can be shared according to Open Data logic, but only within a framework that ensures strict control over the data concerned.

---

<sup>122</sup> EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space, of 12 July 2022, para. 85, available here: [https://edpb.europa.eu/system/files/2022-07/edpb\\_edps\\_jointopinion\\_202203\\_europeanhealthdataspace\\_en.pdf](https://edpb.europa.eu/system/files/2022-07/edpb_edps_jointopinion_202203_europeanhealthdataspace_en.pdf).

[63] The need to keep control over personal data can lead to significant complications in the opening of data in the context of the research. For example, the most recent genomics and precision medicine projects require large volumes of data and therefore require the cooperation of multiple «data provider» institutions. The data sets thus collected do not only derive their value from their volume, but also from the work that is carried out on this data (e.g. operations for making data interoperable, curation, interpretation) and therefore there is a strong interest in making them accessible for future purposes. These projects are usually multicentric in nature and are based on a «consortium» type contractual structure. However, in such configurations, the provision of data sets for reuse by third parties (sometimes called third use) can soon become complex if the data in question includes personal data. The challenge is, among other things, to maintain the link between the research subjects concerned and the end users of this data, which sometimes results in a series of data sharing contracts. The situation becomes even more complex when one of the links in the research disappears, for example when the multicentre research consortium that initially collected the data comes to an end.

[64] The above example demonstrates that, in practice, an approach based on the chain reuse of personal research data is not very viable, because it ultimately generates significant complications, particularly from a contractual point of view. To address these challenges, several options can be considered, starting with the use of privacy-friendly models or methods (see above 3.4). However, if we want to offer direct access to data, then it seems appropriate to favour a register-type approach. In other words, the aim is to allow data sets to be stored in a structure that can make data available to third parties.<sup>123</sup> The registry can then serve as a single point of contact for third parties wishing to access the data concerned with a view to reusing it for future research purposes. This approach allows data providers to keep direct control over the data and to ensure that the rights of research subjects are preserved, in accordance with the legal framework in force.

[65] The development of a data retention system is also one of the proposals made in the Humbel Report.<sup>124</sup> While excluding a solution in which the medical data available in Switzerland would be stored on a single medium, the report supports a decentralised data storage solution in which «the different data collections from the same organisation would be collected and stored in a local system» (free translation).<sup>125</sup> In our view, an approach tending towards a single register must indeed be rejected, in particular for reasons linked to the excessive security risks which would arise therefrom. Nevertheless, as part of his upcoming reflections on the subject, the legislator should be careful not to «impose» too restrictive a decentralisation, which would contribute to perpetuating the situation of data silos that currently exists. Biomedical research projects, particularly when conducted in a multicentric way, must be able to benefit from federated infrastructures in which they can deposit the data sets generated for the purpose of making them available for future research, while respecting the applicable law and the rights of research subjects.

---

<sup>123</sup> It should be noted that the storage or entry of data in a database already constitutes reuse within the meaning of the HRA, in accordance with Art. 24 let. c HRO. See also the example of biobanks: SHK HFG-RUDIN (fn 55), Vorbermerkungen Art. 32–35, N 7.

<sup>124</sup> Humbel Report of 4 May 2022 (fn 30), p. 41.

<sup>125</sup> Humbel Report of 4 May 2022 (fn 30), p. 41.

## 4. Opening up data

[66] As demonstrated by the analysis conducted in the previous section, the special rules applicable to the processing of personal data significantly limit the opening of personal data. The data processed in the context of biomedical research nevertheless covers a broader field than personal data and may also concern non-personal data, the access and use of which may be covered by other legal regimes.<sup>126</sup> While these generally offer more flexibility in terms of sharing, they can also raise certain constraints for Open Data. After examining these potential constraints (4.1), we will analyse certain contractual tools that promote the availability of data on an open access basis. However, we will not commit ourselves to a comprehensive approach (4.2).

[67] In order to avoid confusion, the terminology of research data will be used in this section to refer to both personal and non-personal data intended for use in biomedical research.

### 4.1. Constraints related to opening up data

#### 4.1.1. Applicable legal regimes

[68] Before examining the various legal tools promoting the reuse of research data in an Open Access context, it is first necessary to carry out a careful examination of the potential constraints likely to hinder their opening in open access.<sup>127</sup> In addition to the provisions applicable to the protection of personal data, particular attention must be paid to the applicable rules that may arise from other legal regimes, in particular those provided for by the federal Copyright Act<sup>128</sup> (CopA), the federal Act on Unfair Competition<sup>129</sup> (UCA) and contract law. Due to its multifaceted nature, research data is presented in multiple modes (medical imaging, tables, database, representation and structure of biomolecules) through the combination and linking of raw data (e.g., blood pressure measurements) and more complex information (multi-nucleotide variant annotation). It can therefore be covered by different legal regimes, the most important of which are briefly presented below from a practical point of view.

[69] The protection offered by copyright opens when the legal conditions are met, i.e. when we are in the presence of a literary or artistic intellectual creation of an individual character

---

<sup>126</sup> On the question of rights to access and reuse research data, see YANIV BENHAMOU, *Intelligence artificielle : licence libre et gouvernance collective des données à travers l'altruisme des données et des data trusts*, in: *Revue suisse de droit des affaires et du marché financier (RSDA)*, p. 419 et seq.; HÉLÈNE BRUDERER, *Les droits d'accès et de réutilisation des (bases de) données de recherche : de lege lata, de lege ferenda*, in: Jean-Philippe Dunand/Anne-Sylvie Dupont/Pascal Mahon (publisher), *Le droit face à la révolution 4.0*, Zurich 2019, p. 293 et seq. See also EVA CELLINA, *La commercialisation des données personnelles – Aspects de droit contractuel et de protection des données*, Geneva thesis, Geneva/Zurich/Basel 2020; Report of the Federal Institute of Intellectual Property, *Access to Non-Personal Data in the Private Sector*, 1 March 2021, available here: <https://www.ige.ch/en/intellectual-property/ip-and-society/data-processing-and-data-security>.

<sup>127</sup> Compliance with the principle «as open as possible, as closed as necessary» is not intangible and may suffer from certain exceptions. See e.g. Art. 39 para. 2 of Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing «Horizon Europe» the framework programme for research and innovation and defining its rules for participation and dissemination, and repealing Regulations (EU) no. 1290/2013 and (EU) no. 1291/2013.

<sup>128</sup> Federal Act on Copyright and Related Rights of 9 October 1992 (CopA; RS 231.1).

<sup>129</sup> Federal Act on Unfair Competition of 19 December 1986 (UCA; RS 241). On the study of the protection of databases by the UCA, PHILIPPE DUCOR, *Protection des bases de données et concurrence déloyale*, in : Alain Ragueneau (édit.), *Internet 2003 : travaux des journées d'étude organisées à l'Université de Lausanne les 21 mai et 26 novembre 2003*, CEDIDAC, Lausanne 2004, p. 153 et seq.

(Art. 2 para. 1 CopA). Research data can be expressed in various forms: tables, phylogenetic trees, various graphic representations or in the form of a database. It can be protected as a work with scientific content (Art. 2 para. 2 CopA), as a derivative work when it is the result of a reworking of a pre-existing work (Art. 3 para. 1 CopA) and finally, under collections when it is structured in the form of a database (Art. 4 para. 1 CopA). No formality is necessary for copyright protection to apply: it applies as soon as the work is created (Art. 29 para. 1 CopA), even at the simple project stage and for parts of works as soon as the conditions of protection are met (Art. 2 para. 4 CopA). Regardless of the classification chosen (work with scientific content, collection), the protection conferred by the CopA concerns only the structure and form of the presentation of the data and not the data itself.<sup>130</sup> No protection can be conferred on scientific ideas and facts, only the expression of the idea – i.e. its formatting – can be protected under copyright.<sup>131</sup> When the contingencies that govern the creation of a work are high, it is generally acknowledged that the individuality requirement is met as long as the authors have been able to make personal choices and it is not simple routine work. In the presence of an intellectual work of an individual character, its author is then vested with an exclusive right over it, conferring on them moral and patrimonial prerogatives.

[70] For all useful purposes, it should be remembered that Switzerland, unlike the European Union, has not introduced a *sui generis* right for databases which would prohibit any extraction and/or reuse of the content of a database that required substantial investment.<sup>132</sup> On the other hand, other protection mechanisms can protect a database, in particular the law on unfair competition (Art. 5 let. a and c and 6 UCA) or business secrecy (Art. 4 let. c and 6 UCA).<sup>133</sup> Contrary to intellectual property rights (e.g. CopA), these legal regimes do not confer any absolute subjective rights: they sanction behaviour indicating a certain disloyalty or improper access to secrecy, exploited or disclosed, by a third party.

[71] It should be noted that the methods of access to and the reuse of research data, regardless of the protection that may be conferred on it by copyright, may be the subject of a contract. It is thus possible to impose specific terms of use through a licence, or even other contractual obligations such as an obligation of confidentiality. It is therefore the principle of contractual freedom which prevails in this context, subject to compliance with any mandatory rules likely to apply (e.g. protection against excessive commitments) according to Art. 27 para. 2 of the Civil Code). Contrary to intellectual property rights, contracts shall, however, only have their effects between the parties and not with regard to third parties, on the basis of the principle of the relative effect of agreements.

---

<sup>130</sup> For a study of the protection of databases by copyright see NATHALIE TISSOT, *Bases de données et droit d'auteur*, in: Alain Ragueneau (publisher), *Internet 2003: travaux des journées d'étude organisées à l'université de Lausanne les 21 mai et 26 novembre 2003*, CEDIDAC, Lausanne 2004, p. 187 et seq. See also: AIPPI's Switzerland Group, sic! 2020, p. 655 et seq.

<sup>131</sup> For a reminder of this principle, ATF 133 II 306 c. 3, JdT 1988 I 304. See BRUDERER (fn 126), p. 298–299 and the references cited.

<sup>132</sup> Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases.

<sup>133</sup> For a definition of business secrecy: judgment of the Federal Court of 8 June 2010 4A\_195/2010, c. 2.2. See also on this subject RALPH SCHLOSSER, *Les secrets économiques dans les relations de travail, les collaborations et les procès civils*, in: Jacques de Werra (publisher), *La protection des secrets d'affaires*, p. 65 et seq.

[72] A brief analysis of the different legal regimes applicable to research data thus shows that it is subject to relatively complete, albeit sparse, protection, making it possible to guarantee real control, or even «quasi-ownership».<sup>134</sup>

#### 4.1.2. Examples of constraints

[73] Following this brief overview of the legal regimes applicable to research data, we propose to further analyse three types of constraints that may arise in the context of opening up data for research purposes. They are the following potential constraints: (1) the existence of pre-existing content and/or knowledge belonging to third parties in the data to be disseminated openly, (2) the ownership of data generated as part of a research project, and (3) the competitive application of the different legal regimes applicable to the data.

[74] The first point of analysis consists of determining whether the research data newly generated as part of a research project, which can be classified as Output Data independently of its presentation method and the type of data in question, include pre-existing content and/or knowledge belonging to third parties, i.e. initial data (Input Data).<sup>135</sup> In the event that Output Data includes Input Data, it is necessary to establish whether its reuse is subject to specific contractual conditions such as an obligation to maintain secrecy or if it is subject to absolute subjective rights such as copyright. The distribution of Output Data knowingly incorporating content belonging to third parties without their authorisation is likely to constitute a breach of contract and/or obligations imposed by law. In the absence of a clear provision specifying the conditions for the reuse of content belonging to third parties and/or their explicit consent, it is prudent to ask them for a written authorisation validating the envisaged reuse.<sup>136</sup> Depending on the applicable operating procedures, Input Data aggregation activities may also involve observing specific rules, particularly in terms of citation. It is therefore essential to identify the contractual conditions governing access to and reuse of initial data belonging to third parties in order to assess the extent of the obligations imposed on the holders of Output Data with a view to opening up the data.

[75] The second aspect to be considered concerns the ownership of Output Data. During the course of a research project, Output Data is usually the result of collaborative work by several partners. In such a context, research data can, for example, be generated as follows: a first partner makes its Input Data expressed in different forms (databases, diagrams and various scientific representations), then a second partner is responsible for annotating and restructuring it according to a precise methodology. Finally, a third partner performs data matching operations to obtain the research data (Output Data). In such a constellation of successive contributions, and in the absence of agreement between the parties involved, the control of the data and its use may lead

---

<sup>134</sup> IPI Report (fn 126), section 5.1.3, p. 23.

<sup>135</sup> On the distinction between *Input Data* and *Output Data* and the issues raised in terms of intellectual property: YANIV BENHAMOU, *Big Data and the Law: a holistic analysis based on a three-step approach – Mapping property like rights, their exceptions and licensing practices*, *Revue suisse de droit des affaires et du marché financier (RSDA)* 2020 p. 393 et seq., p. 404–407; RICHARD KEMP, *Legal aspects of managing Big Data*, *Computer Law & Security Review: The International Journal of Technology Law and Practice* 2014, Vol. 30 p. 482 et seq., p. 489–490.

<sup>136</sup> FLORENT THOUVENIN, *Un droit de propriété sur les données en suisse ?*, in: Jacques de Werra (publisher), *Intellectual property in the Age of Big Data and Blockchain*, Zurich 2017, p. 113–114, rightly states that the data generation process is more likely to be the subject of similar creations, thus it is more difficult to claim an infringement of a pre-existing exclusive right. The author draws the conclusion that the copyright holder cannot prohibit a third party from using a work totally or largely identical to his own work if the latter is able to show that he has created his work completely independently.

to debates.<sup>137</sup> In addition, if CopA protection applies to Output Data, it is also necessary to determine whether a derivative work is present (Art. 3 para. 1 CopA) or a separate joint work (Art. 7 para. 1 CopA). In the first case, the use of the Output Data requires the consent of the holder of the initial data reused (Art. 3 para. 4 CopA), while in the second case, the holders are free to use it within the limits provided for in the CopA. The issue of the ownership of Output Data and the resulting consequences deserve special attention. The lack of prior agreement from the parties involved in the research project can quickly cause disagreements which will result in an impediment to the full use of the data, particularly from an Open Access perspective. Moreover, the determination of the ownership of Output Data is of significant practical interest, as only the holders of Output Data are authorised to delimit the scope of the usage rights conferred on future users and are responsible for the content published in open access. It is therefore recommended to pay particular attention to the drafting of the research plan by making sure to clearly define the objective and the results to be generated (Foreground IP) as well as the various contributors and/or processors, in particular by precisely identifying their respective contributions and the pre-existing knowledge they will make available (Background IP). The characteristic flexibility of contract law can therefore make it possible to develop suitable and original solutions to settle the claims of the participants involved in a research project with regard to Output Data, but also to define the methods for putting it into circulation.

[76] The third point of analysis consists of assessing the consequences related to the sometimes simultaneous application of various applicable legal regimes<sup>138</sup> with regard to Output Data. The implications will be significantly different depending on whether it is a question of reusing sensitive patient data or non-personal data, for example data linked to the genetic sequencing of a virus such as SARS-CoV-2. As rightly mentioned in the IPI Report<sup>139</sup>, a systematic review of the content of the data should be carried out prior to future use, in particular to determine whether re-identification of individuals is possible. In practice, however, the multifaceted nature of the data can make it difficult to examine its content and reveal the presence of mixed data protected by different legal instruments. In all cases, the applicable rules on the protection of personal data (e.g., FDPA, HRA) take precedence over other legislation applicable to data such as copyright.<sup>140</sup> Where possible and where useful for the dissemination of data, personal data should be isolated from non-personal data.

[77] In summary, the reuse of Input Data and the creation of Output Data can generate constraints that may have an impact from a perspective of opening up research results. In order to assess whether open access is possible and how it can be made available, it is therefore essential to properly assess the content of the data in question and to identify the various applicable legal regimes.

---

<sup>137</sup> On the issue of the ownership of digital goods in general and the applicable rules, YANIV BENHAMOU/LAURENT TRAN, *La circulation des biens numériques : de la commercialisation à la portabilité*, sic! 2006 p. 571 et seq., p. 582–583.

<sup>138</sup> On this subject, BENHAMOU (fn 135), p. 413–415; BRUDERER (fn 126), p. 295–298.

<sup>139</sup> IPI Report (fn 126), section 4.1, p. 20.

<sup>140</sup> In this sense, see BENHAMOU (fn 138), p. 429 who also proposes this approach when it is not possible to sort data.

## 4.2. Putting data into circulation: licence & waiver

[78] In Swiss law, there is no ownership right over data as such.<sup>141</sup> However, this does not exclude *per se* the possibility of regulating the terms of its access and use contractually, in particular through the use of licences or general terms and conditions. Given that research data can be expressed in different forms (databases, tables, images, diagrams) according to the different disciplines (genomics, transcriptomics, etc.), this section is limited to generally presenting legal tools compatible with the open access approach and highlighting certain issues relevant to practice.

[79] The free access movement aims to ensure that holders of research results retain their rights to research results and grant rights of use.<sup>142</sup> With a view to opening up data in Open Access, it is recommended to use the licensing mechanism. The practice of licensing is a conventional process of valuation of intangible assets carried out via the figure of a licence agreement covering both intangible assets protected by absolute subjective rights (e.g. copyright, protection of personal data), but also those that are not protected by a legal monopoly.<sup>143</sup> A licence is a *sui generis* innominate agreement by which the owner of an intangible asset (the licensor) grants to a third party (the licensee) the use and enjoyment of an intangible asset in return for the possible payment of a fee. The validity of this type of contract is not subject to compliance with any particular form requirement. It may be written, oral, or result from conclusive acts. The scope of the operating rights is determined by the type of licence<sup>144</sup> granted by the author: it may be simple or exclusive, paid or free, total or partial, for a fixed or indefinite period, geographically limited, with or without the ability to grant sub-licences, or even be granted for a specific purpose (e.g. for use for academic and/or commercial purposes). Subject to compliance with mandatory provisions (e.g. Art. 27 para. 2 CC, Art. 19 para. 1 CopA), it is therefore contractual freedom that prevails in this area. Under the relative effect of agreements, the licence agreement has no absolute effect (*erga omnes*), it only applies between the parties concerned (*inter partes*), i.e. between the licensor and the licensee.

[80] The opening up of open access research data can thus be formalised by establishing a licence agreement. To do so, it is possible to specify the conditions for access and reuse of data in a dedicated section, whether in a contract or in general terms and conditions, or to use free and standardised licence models such as Creative Commons<sup>145</sup> licences or licences developed by the Open Knowledge Foundation.<sup>146</sup> These two approaches are not exclusive and it is perfectly

---

<sup>141</sup> For an in-depth examination of this theme: THOUVENIN (fn 136), p. 61–62 and the references cited. The same approach is applied at European level: Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 establishing a framework for the free flow of non-personal data in the European Union, available here: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018R1807&from=FR>.

<sup>142</sup> See the Berlin Declaration, which explicitly states that: «Free access contributions must meet two conditions: 1. Their authors and the owners of the related rights grant to all users a free, irrevocable and worldwide right to access the work in question, as well as a licence authorising them to copy, use, distribute, transmit it and show it in public, and to make and distribute derivative works, on any digital medium whatsoever and for any responsible purpose whatsoever, provided that the author is duly mentioned [...]».

<sup>143</sup> THOMAS PROBST, *Der Lizenzvertrag: Grundlagen und Einzelfragen*, in: Jusletter 2 September 2013, N 10 et seq.; CELLINA (fn 126), p. 156 and the references cited.

<sup>144</sup> For a general overview of the different types of licence, PROBST (fn 143), N 25 et seq.

<sup>145</sup> For an overview of the various Creative Commons licences: MICHEL JACCARD/EVA CELLINA, *Les Creative Commons, avenir du droit d'auteur?*, SJ 2017 II p. 229 et seq., p. 235–239.

<sup>146</sup> See on this topic: <https://opendatacommons.org/licenses/>. Unlike Creative Commons licences, Open Data Commons licences only cover databases but not their content. The introduction of the three Open Data Commons licences states that: «Databases can contain a wide variety of types of content (images, audiovisual material, and sounds all in the same database, for example), and so this licence only governs the rights over the Database, and

possible to modify the provisions of Creative Commons licences.<sup>147</sup> When choosing one form of licence or another, it is nevertheless necessary to verify the existence of any internal rules specific to the research institution concerned and, where appropriate, to comply with them.

[81] In cases where research data is made available via a licence agreement, the scope of the licence granted must be precisely defined. In order to be consistent with the open access philosophy, the terms of the licence granted must, in our opinion, include the following characteristics: be non-exclusive, free of charge and allow all users to use, copy, modify and distribute the licensed content, including in derivative form. It is also useful and recommended to specify any applicable citation rules, to specify the use of Input Data or content belonging to third parties which falls outside the scope of the licence granted, to define the rules of liability applicable when reusing the content, to mention a point of contact, and also to specify the applicable law and the competent jurisdiction in the event of a dispute, as well as the conditions for termination.<sup>148</sup>

[82] If public licences are used, Creative Commons licenses should be preferred. They are an effective instrument to easily determine the extent of rights conferred on users in respect of a copyright-protected work.<sup>149</sup> These public licences enjoy a certain popularity and their use is recommended by several public institutions.<sup>150</sup> Rights holders can define how their content is exploited by choosing from six Creative Commons licence categories. Without going into the details of each licence, it is nevertheless possible to briefly present their respective characteristics. The most permissive licence is the attribution licence (BY). It offers each user the freedom to reuse the data provided, however, that they credit the original holders and indicate whether any changes have been made to the original content. The Share Alike (SA) licence requires citing the source and sharing newly created work from pre-existing work under the same CC BY-SA licence. The licence prohibiting commercial use (CC BY-NC) provides for the same rights as the attribution licence, but excludes any use for commercial purposes. The Non-derivative licence (CC BY-ND) allows commercial use, but prohibits any modification or creation of derivative works. Finally, it is worth mentioning the characteristics of the Creative Commons Zero (CC0) licence. It is not strictly speaking a licence since its application has the effect of placing the content in the public domain, with their creators thus renouncing the exercise of their copyright (waiver). Content released under a CC0 license can therefore be modified and reused freely without any restrictions. It is an effective instrument to remove any possible doubt about whether copyright protection applies or not, since the authors waive the exercise of their exclusive right with re-

---

not the contents of the Database individually». Therefore, it is entirely possible to apply both an Open Data Commons licence to a database and a CC BY licence to its content if it is copyrightable.

<sup>147</sup> However, see the reservations mentioned in the FAQ for Creative Commons, <https://creativecommons.org/faq/#can-i-change-the-license-terms-or-conditions>.

<sup>148</sup> For example, access and use by third parties of the various scientific data available on the GISAID website are subject to a Data Access Agreement. Each user is granted a non-exclusive, worldwide, free and non-transferable licence to access and use the EpiFlu database. See for more details <https://gisaid.org/terms-of-use/>; for another similar example: <https://www.surechembl.org/terms/>.

See also the recommendations proposed by BENHAMOU (fn 138), p. 412–413.

<sup>149</sup> The disclaimer section of Creative Commons licences emphasises that they are intended for use «by authors and rights holders within the limits of applicable laws and regulations». See JACCARD/CELLINA (fn 145), p. 240.

<sup>150</sup> See e.g. the recommendations of the Open Access for Infrastructure for Research in Europe (OpenAIRE) infrastructure, available here: <https://zenodo.org/record/2574619>, which recommend the use of Creative Commons CC BY 4.0 licences where the material constitutes a work within the meaning of the CopA and CC0 for data and data sets that are not structured as a database.

spect to intangible assets covered by the licence within the limits of the law.<sup>151</sup> The CC0 licence also has the advantage of remedying the problem of attribution stacking, i.e. the need to credit a large number of reused data sets, each with its own citation requirements. The application of a CC0 licence therefore gives users the possibility to aggregate several data sets without having to worry about crediting their holders individually. Although the terms of the CC0 licence do not impose any obligation of citation concerning the reused content, it is still advisable to provide for a citation rule, as ethical considerations may apply, particularly in the academic community. Furthermore, publications in the research community are still a high-potential issue for people involved in biomedical research. It is important to carefully identify the content subject to Creative Commons licences and clearly highlight any elements that do not fall within the scope of the chosen licence.<sup>152</sup> It should be noted that Creative Commons licences are irrevocable and do not contain any specific clauses regarding the integration of personal data.<sup>153</sup>

[83] Creative Commons licences must not be used for the provision and sharing of personal data as they would result in a loss of control contrary to laws relating to the processing of personal data. This applies in the same way for the processing of data carried out in the context of human research and subject to the HRA: the free dissemination of coded personal data would not only prevent the research subjects from asserting their rights over their data, but would also result in it being impossible to guarantee that this data would only be reused for research purposes.<sup>154</sup> As previously stated (see section 3.4 below), it is necessary to use specific contractual instruments (e.g. *Data Sharing Agreement*) and to specify the scope of the licence granted for research data including sensitive personal data. In other words, Creative Commons licences may only be considered if the research data has been completely anonymised or if it does not contain any personal data.<sup>155</sup>

[84] In view of the above and provided that no contractual or legal constraints prevent an open access provision, the Creative Commons CC BY and CC0 public licences remain the most suitable legal tools for making content available in Open Access. The CC BY-SA licence is also compatible with the open access paradigm, but users who do not wish to suffer from the copyleft effect<sup>156</sup> will prefer not to reuse the content in question so as not to be forced to apply the terms of the CC BY-SA licence. The Non Derivative (CC BY-ND) and Non Commercial (CC BY-NC) licences appear less compatible with open access requirements. The Non Derivative condition prohibits any combination and aggregation with new data and the Non Commercial licence remains difficult to implement, as it is not always easy to determine what is or is not commercial use.<sup>157</sup>

---

<sup>151</sup> On the question of the waiver of copyright: DENIS BARRELET/WILLI EGLOFF, *Le nouveau droit d'auteur, Commentaire de la loi fédérale sur le droit d'auteur et les droits voisins*, 4<sup>th</sup> ed., Bern 2021, Art. 16 CopA, N 18–19.

<sup>152</sup> Under a CC-BY licence, copyrighted content may be freely reused, but licence terms require that reused content be identified (including in modified form) and that the authors of the original contribution be identified (Art. 3(a)(1)).

<sup>153</sup> See Art. 2(b)(1) of the Creative Commons CC BY licence, which states that: «Moral rights, such as the right to integrity, are not licensed under this Public Licence, nor are publicity, privacy, and/or similar personality rights; [...]».

<sup>154</sup> See also JANE KAYE (fn 40), p. 421–423.

<sup>155</sup> In the same direction, ANDREAS WIEBE/NILS DIETRICH, *Open Data Protection: Study on legal constraints to open data sharing – Data Protection and PSI*, Göttingen, Germany 2017, p. 199.

<sup>156</sup> The copyleft effect is associated with licences that allow any user to use, copy, modify, and distribute modified versions of a work provided that said work, including modified versions, is distributed under the same conditions.

<sup>157</sup> On this point, see JACCARD/CELLINA (fn 145), p. 247–249.

[85] In summary, waiver and licensing mechanisms are appropriate legal tools for releasing Open Access research data, provided it does not contain personal data. With regard to the licence agreement, it must be ensured that its terms are consistent with the open access philosophy. It will always be possible to draw on the contractual provisions mentioned in the Creative Commons CC0, CC BY and CC BY-SA licences to arrive at a similar or even identical scope of use. For the sake of clarity and so as not to unnecessarily hinder the reuse of open access content, it is more prudent not to modify the provisions of a Creative Commons licence, as this may cause confusion in the minds of the public about the scope of operation offered. In all cases, it is essential to specify the scope of the licence granted, as in the absence of specific mention on this subject, prudence recommends applying the rules laid down in the CopA, i.e. seeking permission from the content holders before any reuse. It should be noted that in a context whose main purpose is scientific research, users can also rely on the legal exception of text and data mining to reproduce available content without the prior authorisation of its authors.<sup>158</sup> However, if they wish to exploit such content in a way that goes beyond text or data mining, they must obtain prior authorisation from its authors.

## 5. Practical application and check-list

[86] The analyses conducted so far have shown that the provision, sharing and reuse of data for biomedical research purposes, with an Open Data perspective, could be subject to various limitations of a legal nature and/or involving the adoption of certain measures, particularly contractual measures. From a practical perspective, here we propose a check-list of the main issues to be resolved before data is opened for biomedical research purposes:

[87] Phase 1 – Assessment of the obligations related to the data concerned

- Is the provision of data imposed or encouraged by specific rules, e.g. rules imposed by a funder (e.g. SNSF) or internal rules of the institution holding the data? If so, what requirements are imposed?
- Does the data concerned contain personal data? If so, all applicable legal provisions must be identified (see above 3.1) and it must be determined if and under what conditions the data concerned can be made available to third parties. If the HRA is applicable and the sharing of personal data (coded or not) is envisaged, care will be taken, among other things, to determine whether the rules for reuse established by Arts. 32 to 34 HRA are met (in particular the validity of the consents) and to verify that the research project for which the data will be reused has been validated by an ethics committee (Art. 45 HRA). In any case, personal data cannot be freely distributed, it must remain in a controlled environment.
- Is the data concerned covered by other legal systems? For example, is the data subject to a specific obligation of confidentiality, licences granted by third parties, other types of contractual obligations that would prevent disclosure, a business or manufacturing secret?

---

<sup>158</sup> Art. 24d CopA. See also the Federal Council Message of 22 November 2017 relating to the amendment of copyright law, the approval of two World Intellectual Property Organisation treaties and their implementation, FF 2018 559 et seq., p. 594–595.

[88] Phase 1 should provide a comprehensive view of the rights and obligations related to the sharing of the data concerned and thus establish the minimum conditions under which the data can be made available to third parties. Phase 1 should also make it possible to determine whether specific actions should be taken.

[89] Phase 2 – Opening strategy

- Determine the type of licence to be applied for future reuses of data. The degree of openness of the data will depend on the content of the data, in particular whether or not it includes personal data.
- Opening involves sharing personal data:
  - If the funder imposes a general obligation to make data or results available to the public, submit a request for exemption if this is necessary to comply with the applicable legal obligations.
  - In the event that data is shared and reused by third parties, specific Data Transfer Agreement contractual instruments should be put in place to maintain control of the data, in particular by specifying the scope of use authorised by the data recipient, but also to ensure compliance with other specific obligations imposed by the applicable rules regarding the protection of personal data. The latter take precedence over considerations related to data opening.
- Opening does not imply the sharing of personal data, especially if the research data has been completely (and correctly) anonymised:
  - Ensure that there is no contractual obligation to maintain secrecy, for example because of filing a patent application. If special rules are imposed on Open Data by the funder or by the research institution concerned, ensure that they are complied with.
  - The licensor may make research data available using a proprietary license agreement or Creative Commons standard public licences. Use of the CC0 licence offers maximum reuse capability.
  - If appropriate, include specific contractual terms regarding the following: (a) description of the elements that do not fall within the scope of the licence and the rules applicable to the reuse of third-party materials, (b) citation rule, (c) applicable law and jurisdiction (d) any liability rules applicable in the case of reuse of the licensed content, (e) conditions for terminating access and reuse of data and (f) contact address (e.g. email address).
  - Evaluate the advisability of publishing and disseminating research data in a public directory (see in particular the [www.re3data.org/](http://www.re3data.org/) website, which lists the various public directories according to the disciplines concerned).

## 6. Conclusion

[90] Open Data, through the promotion of access to data and knowledge, has become an essential movement in the research sector. This phenomenon is observed both internationally and at Swiss level, where it is directly taken into account in the most recent strategies of the Federal Council on the reuse of medical data (Humbel Report), as well as in the funding conditions of the SNSF

for example. Nevertheless, the requirements set in terms of opening up data are not absolute and the texts on the subject usually reserve the existence of justifying reasons contrary to such opening up of data. The purpose of this contribution was to outline the limitations that Swiss law may impose on the opening of data for biomedical research purposes.

[91] At the end of our discussions, we come to the general conclusion that Open Data and the opening up of research data in the context of biomedical research are not incompatible with current law, in particular data protection, human research or intellectual property law. Depending on the context and the type of data involved, the implementation of Open Data must nevertheless be subject to significant adjustments.

[92] Unsurprisingly, the main constraint to take into account is the protection of any personal data. If such data is involved, the controller must carry out a sometimes complex assessment of the applicable legal rules and determine the conditions under which it may make the data concerned accessible. As a general rule, it is necessary to ensure that personal data remains under constant control and therefore «chain» reuses of such data should be avoided. Privacy-friendly technologies or models can contribute to overcoming the constraints imposed on the sharing of personal data, but a detailed analysis must be carried out on a case-by-case basis.

[93] When the question of personal data is cleared up and opening up of the data is possible, i.e. there are no other constraints preventing it (e.g. third party rights to the data), a thoughtful data opening strategy must be established. Such a strategy generally involves establishing or selecting appropriate licenses for the purposes pursued.

[94] Recently, the Federal Council gave the Federal Department of the Interior a mandate to develop a concrete strategy for the reuse of health data (Humbel Report) and a draft federal framework law on the reuse of (potentially health) data is also under consideration.<sup>159</sup> As discussed, such an approach is now subject to more concrete projects in Europe, with the European Health Data Space project. At Swiss level, these are important considerations that could lead to proposals for legislative changes, in line with the Federal Council's desire to modernise the institution of general consent. The solutions proposed must strike a delicate balance between promoting open science and protecting participants, while respecting constitutional and ethical guarantees.

---

FRÉDÉRIC ERARD, Dr. iur., Attorney-at-law, CIPP/E, Head, Legal and Technology Transfer Office at the SIB Swiss Institute of Bioinformatics.

MATHILDE HEUSGHEM, LL.M., Attorney-at-law, Legal Officer at the SIB Swiss Institute of Bioinformatics.

CLÉMENT PARISATO, M.Law, Senior Legal Officer at the SIB Swiss Institute of Bioinformatics.

The SIB Swiss Institute of Bioinformatics is responsible, in collaboration with the Swiss Association of Medical Sciences (SAMS), for the implementation of the SPHN initiative, which also includes the establishment of the BioMedIT network. The salaries of Frédéric Erard and Mathilde Heusghem are partly financed by SPHN funds. The SwissBiodata ecosystem (SBDe) project is co-directed by the University of Bern and the SIB Swiss Institute of Bioinformatics.

---

<sup>159</sup> See fn 19.

The analyses and reflections conducted in this contribution are based on the personal opinion of their authors and do not imply that of their employer, namely the SIB Swiss Institute of Bioinformatics, or that of other entities such as the SPHN.

The authors thank Mr Marc Fillietaz for his proofreading of the text and his valuable comments.

This article was originally published in French under the following reference: *Recherche biomédicale et Open Data – Perspectives en droit suisse*, in: Jusletter 30 January 2023.