Action Line D2.3 of the Swiss National Open Research Data Action Plan:

Incentivise, Support, and Fund Research Data Protection Officers (RDPO) at HEIs

Project founded by swissuniversities
from January 1st, 2024 to December 31st, 2024

Les passages en allemand du présent document ont été rédigés à l'aide du logiciel de traduction DeepL.
Die deutschen Textpassagen dieses Dokuments wurden unter Zuhilfenahme der Übersetzungssoftware DeepL erstellt.

FAQ – recherche et données personnelles

Ce document a pour but d'aborder les principales questions relatives à l'*Open Research Data* (ORD) en rapport avec la protection des données. Il a pour intention de servir d'outil de travail aux *Data Protection Officers* (DPO) et à toute personne impliquée dans la protection des données et l'ORD dans les hautes écoles suisses (*data stewards*, service juridique, service IT, etc.) ainsi qu'aux chercheurs et aux chercheuses de ces hautes écoles.

Les questions et les réponses ont été collectées, consolidées et analysées par les huit hautes écoles partenaires mentionnées en page de couverture dans le cadre du projet "DPO & ORD" (ligne d'action D2.3 du Plan d'action national ORD) financé par swissuniversities et mené par Switch. Les questions et les réponses ont été revues par Mes Sylvain Métille et Marie-Laure Percassi (Etude HDC à Lausanne). Leur rôle a été uniquement consultatif et ils ne sont pas responsables de la version finale du document.

Les réponses aux Question / Frage 70 et Question / Frage 92 ont en outre été données par privatim, la Conférence des Préposé·e·s suisses à la protection des données.

Le présent document n'a pas la prétention d'être complet ou exact. Il reflète uniquement les points de vue juridiques des partenaires du projet impliqués et de HDC au moment de sa rédaction et de sa finalisation (du 1er janvier 2024 au 31 janvier 2025). Les réponses sont générales et il est recommandé de les vérifier dans chaque cas en fonction du droit applicable. Bien que les partenaires du projet et l'Etude HDC aient consacré un travail rigoureux et méticuleux à la collecte des questions et à la consolidation des résultats formulés, ils ne peuvent garantir l'exactitude absolue de ces informations et déclinent toute responsabilité à cet égard.

Le document est classé par thèmes. La table des matières, qui reprend les questions, permet d'accéder aux réponses directement en cliquant sur les liens.

FAQ – zu Forschung und Personendaten

Dieses Dokument soll die wichtigsten Fragen im Zusammenhang mit *Open Research Data* (ORD) in Bezug auf den Datenschutz erörtern. Es dient Datenschutzbeauftragten (DPOs) und allen anderen Personen, die an Schweizer Hochschulen mit Datenschutz und ORD zu tun haben (Data Stewards, Rechtsabteilung, IT-Abteilung usw.), sowie Forschern und Forscherinnen an diesen Hochschulen als Arbeitshilfe.

Die Fragen und Antworten wurden von den acht auf der Titelseite genannten Projektpartnern im Rahmen des von swissuniversities finanzierten und von Switch geleiteten Projekts „DPO & ORD" (Aktionslinie D2.3 des Nationalen Aktionsplans zu ORD) gesammelt, konsolidiert und analysiert. Anschliessend wurden die Fragen und Antworten von den Rechtsanwälten Sylvain Métille und Marie-Laure Percassi (Kanzlei HDC in Lausanne) überprüft. Ihre Rolle war lediglich beratender Natur und sie sind nicht für die endgültige Version des Dokuments verantwortlich.

Die Antworten auf die Question / Frage 70 und Question / Frage 92 wurden ausserdem von privatim, der Konferenz der Schweizer Datenschutzbeauftragten, zur Verfügung gestellt.

Das vorliegende Dokument erhebt keinen Anspruch auf Vollständigkeit oder Richtigkeit. Es spiegelt lediglich die Rechtsauffassungen der beteiligten Projektpartner und der Kanzlei HDC zum Zeitpunkt seiner Ausarbeitung und Fertigstellung (1. Januar 2024 bis 31. Januar 2025) wider. Hierbei sind die Antworten allgemein gehalten und müssen in jedem Fall anhand des geltenden Rechts überprüft werden. Obwohl die Projektpartner und die Kanzlei HDC bei der Zusammenstellung der Fragen und der Erarbeitung der Ergebnisse ein Höchstmass an Gründlichkeit und Sorgfältig angewendet haben, kann bezüglich der Richtigkeit keine Haftung übernommen werden.

Das Dokument ist nach Themen gegliedert. Über das nachfolgende Inhaltverzeichnis, das die Fragen wiedergibt, können die verlinkten Antworten aufgerufen werden.

Liste des thèmes / Themenübersicht

Données publiques / Öffentlich zugängliche Daten 18

Application du RGPD / Anwendbarkeit der DSGVO 21

Responsabilité / Verantwortung 24

Transfert de données personnelles à l'étranger / Übermittlung von Personendaten ins Ausland 30

Obligations légales / Gesetzliche Verpflichtungen 34

Open research data (ORD) et dépôt / Open Research Data (ORD) und Repositorien 38

Partage et réutilisation de données / Teilen und Weiterverwendung von Daten 56

Consentement / Einwilligung 58

Personnes ayant accès aux données / Personen mit Zugang zu Daten 64

Anonymisation et pseudonymisation / Anonymisierung und Pseudonymisierung 68

Secret de fonction / Amtsgeheimnis 79

Archives / Archivierung 80

Durée de conservation et destruction des données / Speicherdauer und Datenvernichtung 82

Autres / Weitere 88

Table des matières / Inhaltsverzeichnis

I. Données publiques / Öffentlich zugängliche Daten 18

Question / Frage 1 18

Puis-je librement collecter et traiter des données personnelles d'une personnalité publique telle qu'un·e politicien·ne ? 18

Dürfen Personendaten einer öffentlichen Person, wie z. B. eines Politikers, frei gesammelt und bearbeitet werden? 18

Question / Frage 2 18

Utilisation des données personnelles archivées : est-ce que je peux utiliser des données personnelles issues d'archives publiques ? 18

Zur Verwendung von archivierten Personendaten: Können Personendaten aus öffentlichen Archiven verwendet werden? 19

Question / Frage 3 19

Est-ce que je peux, dans le cadre de mes recherches, utiliser puis publier/diffuser des données personnelles (personnes en vie) qui sont accessibles publiquement par exemple sur des sites internet, des bases de données accessibles en ligne ? 19

Darf ich im Rahmen meiner Forschung Personendaten (von lebenden Personen), die öffentlich zugänglich sind, z. B. auf Websites, in online zugänglichen Datenbanken verwenden und dann veröffentlichen/verbreiten? 19

II. Application du RGPD / Anwendbarkeit der DSGVO 21

Question / Frage 4 21

Si je mène depuis la Suisse (affiliation à une haute école suisse) des recherches sur des citoyen·ne·s européen·ne·s qui impliquent le traitement de leurs données personnelles, quelle loi sur la protection des données prévaut ? Est-ce que la situation est différente si je mène ces recherches depuis le territoire européen avec affiliation à une haute école suisse ? 21

Wenn ich von der Schweiz aus (mit Zugehörigkeit zu einer Schweizer Hochschule) Forschung über EU-Bürger betreibe und dabei deren Personendaten bearbeite, welches Datenschutzgesetz gilt dann? Ist die Situation anders, wenn ich diese Forschung von europäischem Territorium aus betreibe und (trotzdem) einer Schweizer Hochschule angehöre? 21

Question / Frage 5 22

À quel moment le RGPD s'applique-t-il et avec quelles conséquences sur l'ORD : (1) si les données de recherche traitées contiennent des données personnelles de citoyen·ne·s européen·ne·s ? (2) si des données de recherche contenant des données personnelles sont stockées voire traitées dans un pays de l'UE ? 22

In welchen Fällen muss eine Hochschule die DSGVO anwenden und welche Einschränkungen bestehen ggf. bei der Veröffentlichung von Daten? (1) wenn die bearbeiteten Forschungsdaten Personendaten von EU-Bürgern enthalten? (2) wenn Forschungsdaten, die Personendaten enthalten, in einem EU-Land gespeichert oder bearbeitet werden? 23

III. Responsabilité / Verantwortung 24

Question / Frage 6 24

Si l'anonymisation d'un jeu de données est incomplète, et que le jeu de données est mis à disposition publiquement, qui a la responsabilité finale ? 24

Wenn die Anonymisierung des Datensatzes unvollständig ist und der Datensatz öffentlich zugänglich gemacht wird, wer trägt dann die endgültige Verantwortung? 24

Question / Frage 7 24

Comment déterminer le ou la propriétaire des données ? 24

Wie bestimmt man den Dateneigentümer? 24

Question / Frage 8 25

Qui est responsable de la sécurité de l'information et de la protection des données en clair (c'est-à-dire lisibles ou non chiffrées) ? 25

Wer ist verantwortlich für die Informationssicherheit und den Schutz von Daten im Klartext (d. h. lesbar oder unverschlüsselt)? 25

Question / Frage 9 25

Qui est le·la responsable de traitement pour les données ORD : la plateforme, le chercheur ou la chercheuse, la haute école ? Est-ce que cette responsabilité peut être transférée ? 25

Wer ist der/die Verantwortliche für die Bearbeitung von ORD-Daten: die Plattform, der*die Forscher*in oder die Hochschule? Kann diese Verantwortung übertragen werden? 26

Question / Frage 10 26

Qui est responsable de la conformité et du caractère non frauduleux des données ? C'est en principe le ou la chercheuse qui dépose. Mais qu'en est-il quand le chercheur ou la chercheuse est accompagné par des data stewards et qu'une autre personne dépose effectivement ses données avec son accord ? Que se passe-t-il en cas de révocation du consentement ? 26

Wer ist dafür verantwortlich, dass Daten korrekt und nicht manipuliert sind? Im Prinzip ist es der*die Forscher*in, welche*r die Daten ablegt. Aber was passiert, wenn der*die Forscher*in von Data Stewards unterstützt wird und eine andere Person die Daten im Auftrag des*der Forschers*in ablegt? Was passiert im Falle eines Widerrufs? 26

Question / Frage 11 27

Dans quelle mesure la responsabilité d'une université ou haute école peut-elle être engagée en cas de conflit vis-à-vis des données de recherche ? Notamment en ce qui concerne : (1) La production de données frauduleuses ; (2) La rétractation d'un article ; (3) Un leak de données sensibles ; (4) La publication de données personnelles, sensibles ou soumises au secret sans consentement effectif sur une plateforme de partage de données (par exemple, SwissUBase) (que l'erreur provienne soit du chercheur ou de la chercheuse, des data stewards, de la curation de la haute école, de la curation des partenaires) 27

Inwieweit kann eine Universität oder Hochschule im Falle eines Problems im Zusammenhang mit Forschungsdaten verantwortlich gemacht werden? Insbesondere im Hinblick auf: (1) eine Fälschung von Daten? (2) einen Rückzug eines Artikels? (3) en Bekanntwerden von besonders schützenswerten Daten? (4) eine Veröffentlichung von persönlichen, sensiblen oder geheimhaltungsbedürftigen Daten auf einer Datensharing-Plattform (z.B. SwissUBase) ohne wirksame Einwilligung (unabhängig davon, ob der Fehler von den Forschenden, den Data Stewards, einem Hochschul-Vertreter oder einem Partner erfolgte) 27

Question / Frage 12 28

Si un chercheur ou une chercheuse quitte la haute école à laquelle il·elle est affilié·e (départ à la retraite, fin de contrat ou encore changement de poste au sein de l'institution), qui s'occupe des droits de la personne concernée si les données n'ont pas encore été rendues anonymes (ne peuvent pas être rendues anonymes) ? 28

Wenn ein*e Forscher*in die Hochschule, der er*sie angehört, verlässt (Pensionierung, Vertragsende oder Stellenwechsel innerhalb der Institution), wer kümmert sich dann um die Rechte der betroffenen Person, wenn die Daten noch nicht anonymisiert wurden (nicht anonymisiert werden können)? 28

Question / Frage 13 28

Qui est responsable du partage des données personnelles collectées dans le cadre d'un projet de recherche d'une haute école ? 28

Wer ist für die Bekanntgabe von Personendaten verantwortlich, die im Rahmen eines Forschungsprojekts an einer Hochschule gesammelt wurden? 28

Question / Frage 14 29

Quels sont les risques si les exigences de sécurité des répertoires ne sont pas suffisantes ? 29

Was passiert, wenn Repositorien den Schutzanforderungen nicht genügen? 29

Question / Frage 15 29

Qui est responsable des données transmises aux archives de l'État ? 29

Wer ist verantwortlich für Daten, die an das Staatsarchiv übergeben werden? 29

IV. Transfert de données personnelles à l'étranger / Übermittlung von Personendaten ins Ausland 30

Question / Frage 16 30

Quelles conditions dois-je respecter pour transférer des données personnelles hors de la Suisse (par exemple sur la plateforme autrichienne Pangaea pour les géosciences), et surtout hors de l'UE ? 30

Welche Bedingungen müssen erfüllt sein, um Personendaten ausserhalb der Schweiz (bspw. auf die österreichische Plattform Pangaea für Geowissenschaften) und vor allem ausserhalb der EU zu übermitteln? 30

Question / Frage 17 31

Quels sont les risques juridiques qu'encourt un chercheur ou une chercheuse s'il·elle dépose son jeu de données (avec restrictions d'accès), sur une plateforme (data repository) américaine ? 31

Welche rechtlichen Risiken bestehen für Forschende, wenn sie einen Datensatz (mit Zugangsbeschränkungen) auf einer amerikanischen Plattform (Datenrepositorium) ablegen? 31

Question / Frage 18 31

Les solutions américaines de stockage telles que OneDrive, Teams sont-elles fiables pour stocker les données personnelles collectées dans le cadre de mes recherches ? 31

Sind amerikanische Speicherlösungen wie OneDrive, MS Teams sicher, um Personendaten zu speichern, die im Rahmen einer Forschungsarbeit gesammelt werden? 31

Question / Frage 19 32

Peut-on conseiller le dépôt de données de recherche suisse dans des dépôts étrangers ? 32

Kann die Ablage von Schweizer Forschungsdaten in ausländischen Repositorien empfohlen werden?..... 32

Question / Frage 20 32

À quelles conditions et avec quelles mesures de protection les données ORD (en particulier contenant des données personnelles) peuvent-elles être stockées voire traitées par des sous-traitants domiciliés dans un État dont la législation ne garantit pas un niveau de protection adéquat des données ?..... 32

Unter welchen Bedingungen und mit welchen Datenschutzmassnahmen können ORD-Daten (insbesondere Personendaten) von Subunternehmen mit Sitz in einem Staat, dessen Gesetze kein angemessenes Datenschutzniveau gewährleisten, gespeichert oder bearbeitet werden? 32

Question / Frage 21 33

Comment permettre et faciliter le partage voire l'ouverture de données personnelles dans des projets de recherche réunissant des hautes écoles soumises à différentes législations (cantonales, suisse, européenne) en matière de protection des données personnelles ? Quid si certains partenaires de recherche ne sont pas situés dans un État garantissant un niveau adéquat de protection des données personnelles ?..... 33

Wie können der Austausch und die Offenlegung von Personendaten in Forschungsprojekten ermöglicht und erleichtert werden, wenn die teilnehmenden Hochschulen unterschiedlichen Rechtsvorschriften (kantonal, schweizerisch, europäisch) betreffend den Schutz von Personendaten unterliegen? Was, wenn einige Forschungspartner nicht in einem Staat ansässig sind, der ein angemessenes Datenschutzniveau gewährleistet? 33

V. Obligations légales / Gesetzliche Verpflichtungen 34

Question / Frage 22 34

Qui a l'obligation de tenir un registre des activités de traitement (données personnelles) ?..... 34

Wer ist verpflichtet, ein Register der Bearbeitungstätigkeiten (zu Personendaten) zu führen?..... 34

Question / Frage 23 34

Dans quel cas un chercheur ou une chercheuse doit-il·elle mener une analyse d'impact en matière de protection des données (AIPD) ?..... 34

In welchen Fällen müssen Forschende eine Datenschutz-Folgenabschätzung (Risikoanalyse) durchführen? 34

Question / Frage 24 35

Quels critères permettent de déterminer s'il y a traitement de données personnelles à risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée dans le cadre de recherches académiques ? Des exemples concrets pourraient être utiles 35

Anhand welcher Kriterien lässt sich feststellen, ob bei Forschungsarbeiten die Bearbeitung von Personendaten ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann? Konkrete Beispiele könnten hilfreich sein..... 35

Question / Frage 25 36

Quelles sont les obligations concrètes des hautes écoles en matière de sécurité des données ? Quels sont les moyens à mettre en œuvre ? Quels sont les résultats/objectifs à atteindre ?..... 36

Welche konkreten Pflichten haben Hochschulen im Hinblick auf den Datenschutz? Welche Mittel sind einzusetzen? Welche Ergebnisse/Ziele sind zu erreichen?..... 36

Question / Frage 26 36

Une université ou haute école peut-elle et doit-elle imposer ses standards à ses partenaires recevant des données de sa part ? Si oui, quels sont les critères concrets permettant d'évaluer la capacité des infrastructures partenaires à respecter ces standards ? 36

Kann und soll eine Universität oder Hochschule ihren Partnern, die Daten von ihr erhalten, ihre Standards vorschreiben? Wenn ja, anhand welcher konkreten Kriterien lässt sich beurteilen, ob die Partnerinfrastrukturen in der Lage sind, diese Standards einzuhalten? 37

VI. Open research data (ORD) et dépôt / Open Research Data (ORD) und Repositorien....38

Question / Frage 27 38

Peut-on déposer sur une plateforme des données personnelles en ORD pour leur réutilisation ? 38

Kann man in einem Repositorium Personendaten als ORD zur Weiternutzung ablegen? 38

Question / Frage 28 39

Quelles sont les conditions à remplir pour que des données personnelles ou confidentielles puissent être partagées dans des dépôts ? 39

Welche Voraussetzungen müssen eingehalten werden, damit Personendaten oder vertrauliche Daten mittels Repositorien geteilt werden können? 40

Question / Frage 29 41

Dans le cadre de recherches académiques, peut-on réutiliser des données personnelles de santé sans le consentement des personnes concernées ? 41

Können im Rahmen der Forschung erhobene Gesundheitsdaten ohne die Einwilligung der betroffenen Personen weiterverwendet werden? 42

Question / Frage 30 42

Puis-je partager mes données dans n'importe quel dépôt ? 42

Kann ich meine Daten in jedem Repositorium zugänglich machen? 43

Question / Frage 31 43

Comment préparer les données (en particulier leur désignation) pour les partager dans un dépôt en étant conforme aux exigences légales ? 43

Wie bereitet man Daten (insbesondere ihre Bezeichnung) für die Freigabe in einem Repositorium auf und erfüllt dabei die rechtlichen Anforderungen? 43

Question / Frage 32 43

Existe-t-il des règles ou des recommandations sur le moment où les données doivent être déposées (par exemple par rapport au déroulement d'un projet ou d'une thèse) ? 43

Gibt es Regeln oder Empfehlungen, wann Daten (in einem Repositorium) abgelegt werden sollten (z. B. in Bezug auf den Verlauf eines Projekts oder einer Dissertation)? 43

Question / Frage 33 43

À quoi les chercheurs et chercheuses doivent-ils faire attention lors du choix des dépôts, en particulier s'ils veulent déposer des données personnelles (sensibles) ? 43

Worauf sollten Forschende bei der Wahl von Repositorien achten, insbesondere, wenn sie (besonders schützenswerte) Personendaten ablegen wollen? 43

Question / Frage 34 44

À quoi peut ressembler une grille d'évaluation pour déterminer si une mise à disposition du public est appropriée ? 44

Wie kann ein Beurteilungsraster aussehen, zur Feststellung der Eignung für eine öffentlichen Zugänglichmachung? 44

Question / Frage 35 44

Comment s'assurer que les jeux de données prévus pour l'ORD soient préparés de manière à être facilement réutilisables ? Ce faisant, ils ne devraient pas être modifiés par des exigences légales de manière à réduire ou à fausser leur contenu informatif. 44

Wie kann man sicherstellen, dass für ORD vorgesehene Datensätze so aufbereitet werden, dass sie leicht wiederverwendbar sind? Dabei sollten sie nicht durch rechtliche Vorgaben so verändert werden, dass ihr Informationsgehalt reduziert oder verfälscht wird. 45

Question / Frage 36 45

À quelles données précises se réfère l'expression « données de recherche ouvertes » ? En d'autres termes, quelles données de recherche doivent être rendues publiques ? 45

Welche Daten sind vom Verständnis «offene Forschungsdaten» umfasst? Mit anderen Worten: Welche Forschungsdaten sollen offengelegt werden? 45

Question / Frage 37 46

Comment les données personnelles doivent-elles être traitées dans le cadre de l'ORD si ces données personnelles ne peuvent pas être anonymisées, par exemple parce qu'il s'agit d'une interview d'expert·e ? 46

Wie wird mit Personendaten im Zusammenhang mit ORD umgegangen, wenn diese Personendaten nicht anonymisiert werden können, bspw. weil es sich um ein Experteninterview handelt? 46

Question / Frage 38 47

Qui est responsable, au sens d'une loi sur la protection des données, de la fourniture de données (en particulier de données claires) dans le contexte ORD, si plusieurs chercheurs et chercheuses les utilisent ? S'agit-il d'un chercheur ou d'une chercheuse en personne (c'est lui·elle qui les a recueillies dans un but précis) ou est-ce les universités qui les emploient ? Comment peut-on le régler ? 47

Wer ist im Sinne eines Datenschutzgesetzes verantwortlich bei Datenbereitstellung (insbesondere von Klardaten) im Kontext mit ORD, wenn diverse Forscher diese Daten nutzen? Ist es der*die Forscher*in persönlich (nachdem er*sie die Daten zu einem definierten Zweck erhoben hat) oder sind es die Hochschulen, bei denen der*die Forscher*in angestellt ist? Wie kann man dies regeln? 47

Question / Frage 39 48

Sur la base de quels critères l'accès aux données doit-il être accordé à des tiers ? Peut-on déterminer/imposer ce que les utilisateurs et les utilisatrices ultérieurs sont autorisés à faire ? Et si oui, comment ? 48

Nach welchen Kriterien ist der Zugang zu Forschungsdaten zu gewähren? Kann bestimmt / vorgeschrieben werden, was spätere Nutzer machen dürfen? Und wenn ja: wie? 48

Question / Frage 40 49

Les accords d'utilisation d'ORD peuvent-ils être conclus pour une durée limitée ? À quoi ressemblent-ils ? Les données peuvent-elles être supprimées à la fin de la période d'utilisation ? 49

Können Nutzungsvereinbarungen für ORD für einen begrenzten Zeitraum getroffen werden? Wie sehen diese aus? Kann am Ende der Nutzungslaufzeit eine Datenlöschung vereinbart werden? 49

Question / Frage 41 49

Dans quelle mesure est-ce que les chercheurs et chercheuses doivent ouvrir leurs données soit sous la pression du FNS, soit sous la pression des éditeurs ? 49

Inwieweit sollten Forschende ihre Daten veröffentlichen, sei es auf Druck des SNF oder auf Druck eines Verlags? 50

Question / Frage 42 50

Un bailleur de fonds exige la conservation à long terme des données de recherche sur un dépôt de données « FAIR ». Quelles données devraient être conservées tout en respectant le cadre légal et éthique ? 50

Ein Geldgeber verlangt die langfristige Aufbewahrung von Forschungsdaten in einem „FAIR“-Datendepot. Welche Daten sollten unter Einhaltung der rechtlichen und ethischen Rahmenbedingungen aufbewahrt werden? 51

Question / Frage 43 51

Dans quelles circonstances les chercheurs et chercheuses peuvent-ils·elles déposer des données génomiques (données personnelles sensibles qui requièrent une protection particulière) dans un repository / dans une archive ? 51

Unter welchen Umständen dürfen Forschende genomische Daten (besonders schützenswerte Personendaten, die einen besonderen Schutz erfordern) in einem Repositorium / in einem Archiv abgelegt werden? 52

Question / Frage 44 52

Des outils appropriés seront-ils mis à disposition ou devront-ils être développés pour une préparation uniforme des données de recherche selon FAIR, si nécessaire ? 52

Werden für eine ggf. erforderliche einheitliche Aufbereitung von Forschungsdaten nach FAIR entsprechende Werkzeuge zur Verfügung stehen bzw. sollen diese entwickelt werden? 52

Question / Frage 45 52

Comment stocker / conserver les données vidéo à long terme en conformité avec la protection des données et l'ORD ? 52

Wie sollen Videodaten in Übereinstimmung mit dem Datenschutz und der DSGVO langfristig gespeichert/aufbewahrt werden? 52

Question / Frage 46 53

Comment préparer des enregistrements sonores ou vidéo en vue d'une réutilisation ultérieure qui respecte la protection des données et les principes de l'ORD ? 53

Wie bereitet man Ton- oder Videoaufnahmen für eine spätere Weiterverwendung auf, die dem Datenschutz und den Grundsätzen der DSGVO entspricht? 53

Question / Frage 47 54

Comment traiter les données qualitatives (par exemple, les entretiens personnels non structurés) ? A quoi faut-il faire attention ? 54

Wie ist mit qualitativen Datensätzen (bspw. unstrukturierte persönliche Interviews) umzugehen? Was gilt es zu beachten? 54

Question / Frage 48 54

Est-il possible d'informer de manière générale les participant·e·s à une recherche que leurs données personnelles seront communiquées pour des « projets de recherche nationaux et internationaux, dans les secteurs public et privé » (à l'instar de ce qui se fait pour le consentement général selon la LRH) ? 54

Ist es möglich, Teilnehmende eines Forschungsprojekts allgemein darüber zu informieren, dass ihre Personendaten für «nationale und internationale Forschungsprojekte im öffentlichen und privaten Sektor» bekanntgegeben werden (nach dem Vorbild der allgemeinen Einwilligung nach HFG)?..... 55

VII. Partage et réutilisation de données / Teilen und Weiterverwendung von Daten 56

Question / Frage 49 56

Quel est le statut des données pour le chercheur ou la chercheuse qui réutilise des données de tiers? Dans quel cas faut-il prévoir un contrat pour cette réutilisation ? 56

Wie sind Daten rechtlich einzuordnen, wenn Forschende diese von Dritten weiterverwenden? In welchem Fall ist ein Vertrag für die Weiterverwendung erforderlich? 56

Question / Frage 50 56

Que faut-il prendre en compte lors du partage de données de recherche entre institutions en ce qui concerne les données personnelles ? 56

Was muss beim Austausch von Forschungsdaten zwischen Institutionen in Bezug auf Personendaten beachtet werden? 57

VIII. Consentement / Einwilligung 58

Question / Frage 51 58

D'un point de vue juridique et pratique, que signifie pour une recherche le retrait du consentement pour l'utilisation et pour le partage des données personnelles ? Quelle est la situation si les données personnelles ont déjà été publiées ? 58

Was bedeutet es aus rechtlicher und praktischer Sicht für ein Forschungsprojekt, wenn die Einwilligung zur Verwendung und Bekanntgabe von Personendaten widerrufen wird? Wie sieht die Situation aus, wenn die Personendaten bereits veröffentlicht sind? 58

Question / Frage 52 58

Quelles sont les bonnes pratiques pour stocker et conserver des consentements pendant et après le projet ? Comment gérer pratiquement les consentements lors du dépôt et du partage de données ? Sur quel support la conservation est-elle préconisée et peut-on passer d'un format papier à un format numérique ? Qu'en est-il du cycle de vie de ce consentement ? 58

Welche bewährten Verfahren gibt es für die Speicherung und Aufbewahrung von Einwilligungserklärungen während und nach dem Projekt? Wie können Einwilligungen im Rahmen der Ablage und Bekanntgabe von Daten verwaltet werden? Auf welchem Medium wird die Aufbewahrung empfohlen und kann von Papier auf digitale Formate umgestellt werden? Wie sieht es mit dem Lebenszyklus der Einwilligung aus? 59

Question / Frage 53 59

Quel devrait être le contenu d'une déclaration de consentement pour le dépôt de données en ORD et leur réutilisation ? Cette déclaration est-elle différente si les données sont personnelles, sensibles, soumises à la LRH ou pseudonymisées ? Si oui, comment ? Est-il possible de construire un consentement général comme il est proposé dans la LRH ? 59

Welchen Inhalt sollte eine Einwilligungserklärung mit Blick auf die Ablage und die Weiterverwendung von Personendaten als ORD haben? Ist diese Erklärung anders, wenn die Daten personenbezogen, besonders schützenswert, dem Humanforschungsgesetz unterliegend oder pseudonymisiert sind? Wenn ja, wie? Ist es möglich, eine generelle Einwilligung zu formulieren, wie sie im HFG vorgesehen ist? 60

Question / Frage 54 60

Dans le cadre de recherches académiques, peut-on réutiliser des données personnelles de santé sans le consentement des personnes concernées ? 60

Dürfen im Rahmen der akademischen Forschung Gesundheitsdaten ohne die Einwilligung der betroffenen Personen weiterverwendet werden? 61

Question / Frage 55 62

Le consentement est-il le seul motif permettant d'ouvrir les données lorsque celle-ci sont encore personnelles ? 62

Bietet die Einwilligung die einzige Grundlage, um Personendaten mittels Repositorien zu teilen? 62

Question / Frage 56 62

Sur la base du « privilège de la recherche », l'obtention d'un consentement pour l'utilisation des données personnelles peut-elle être considérée comme un motif suffisant ? 62

Kann auf der Grundlage des «Forschungsprivilegs» die Einholung einer Einwilligung zur Verwendung von Personendaten als ausreichende Grundlage angesehen werden? 62

Question / Frage 57 62

Le consentement pour l'ouverture des données en ORD doit-il être obtenu séparément du consentement pour mener la recherche ? 62

Muss die Einwilligung zur Veröffentlichung von Personendaten als ORD getrennt von der Einwilligung zur Durchführung der Forschung eingeholt werden? 63

IX. Personnes ayant accès aux données / Personen mit Zugang zu Daten 64

Question / Frage 58 64

Qui peut être le porteur de code/clef après la fin d'un projet ? 64

Wer kann nach Abschluss eines Projekts Inhaber des Pseudonymisierungsschlüssels sein? 64

Question / Frage 59 64

Si un chercheur ou une chercheuse quitte la haute école à laquelle il·elle est affilié·e (départ à la retraite, fin de contrat ou encore changement de poste au sein de l'institution), qui a accès aux consentements éclairés relatifs au traitement de données personnelles que ce chercheur ou cette chercheuse a obtenus dans le cadre de ses recherches ? 64

Wenn ein Forscher die Hochschule, der er angehört, verlässt (Pensionierung, Vertragsende oder auch Wechsel der Position innerhalb der Institution), wer hat dann Zugang zu den Einwilligungserklärungen, die dieser Forscher im Rahmen seiner Forschung betreffend die Bearbeitung von Personendaten eingeholt hat? 65

Question / Frage 60 65

Si un chercheur ou une chercheuse quitte l'institution mais est encore dans un projet FNS, est-ce qu'il·elle a le droit de partir sans autre avec les données acquises dans le cadre du FNS ? Si les données ne sont pas anonymisées ou suffisamment codées, est-ce que l'institution a le droit de les laisser partir comme ça

hors de son périmètre ? Qu'en est-il de la responsabilité du chercheur ou de la chercheuse ? Un chercheur ou une chercheuse est-il·elle propriétaire des données collectées ? 65

Wenn ein Forscher eine Institution verlässt, aber noch in einem SNF-Projekt beteiligt ist, hat er dann das Recht, die im Rahmen des SNF-Projekts erworbenen Daten mitzunehmen? Wenn die Daten nicht anonymisiert oder ausreichend verschlüsselt sind, hat die Institution das Recht, sie aus ihrem Verantwortungsbereich entfernen zu lassen? Wie steht es mit der Verantwortung des Forschers? Ist ein Forscher Eigentümer der gesammelten Daten? 65

Question / Frage 61 66

Qui doit avoir accès aux données codées collectées dans le cadre du projet FNS ? Qui doit avoir accès aux données anonymes collectées dans le cadre du projet ? Qui doit avoir accès à la clé des données d'identification personnelle ? 66

Wer soll Zugang zu den im Rahmen eines SNF-Projekts erhobenen verschlüsselten Daten haben? Wer soll Zugang zu den im Rahmen des Projekts erhobenen anonymen Daten haben? Wer soll Zugang zum Schlüssel für die Identifikation haben? 66

X. Anonymisation et pseudonymisation / Anonymisierung und Pseudonymisierung.....68

Question / Frage 62 68

Afin de garantir une publication complète des données collectées, il est important de s'assurer, dès la collecte des données, qu'aucune donnée personnelle n'est disponible. Quelles conditions doivent être remplies pour garantir une collecte anonyme ? 68

Um eine vollständige Veröffentlichung der gesammelten Daten zu gewährleisten, kann es wichtig sein, bereits bei der Datenerhebung sicherzustellen, dass keine Personendaten vorhanden sind. Welche Bedingungen müssen erfüllt sein, um eine anonyme Sammlung von Daten zu gewährleisten? 68

Question / Frage 63 69

Pour préparer les données en vue d'une publication, les données personnelles éventuellement disponibles doivent être rendues anonymes. Quand des données personnelles sont-elles considérées comme pseudonymisées ? Quand sont-elles considérées comme anonymisées ? La réponse est-elle identique si les données sont soumises à la LRH ? 69

Um die Daten für eine Veröffentlichung vorzubereiten, müssen eventuell vorhandene Personendaten anonymisiert werden. Wann gelten Personendaten als pseudonymisiert? Wann gelten sie als anonymisiert? Ist die Antwort dieselbe, wenn die Daten dem Humanforschungsgesetz unterliegen? 69

Question / Frage 64 70

Lors de la publication de données de recherche, il faut s'assurer qu'elles sont anonymisées. Différentes catégories de données collectées peuvent permettre - sans que les catégories de données individuelles rendent une personne identifiable - une fois réunies, une identification. La question se pose de savoir quand la combinaison de données collectées permet d'identifier une personne ? 70

Bei der Veröffentlichung von Forschungsdaten muss sichergestellt werden, dass diese anonymisiert sind. Verschiedene Kategorien von gesammelten Daten können – ohne dass die einzelnen Datenkategorien eine Person identifizierbar machen - in ihrer Kombination eine Identifizierung ermöglichen. Es stellt sich die Frage, wann die Kombination an gesammelten Daten die Identifizierung einer Person ermöglicht? ... 71

Question / Frage 65 71

Pour les données agrégées, l'exigence est qu'il ne soit pas possible de remonter aux données originales. Comment cela est-il garanti (par défaut) ? Est-ce que chaque chercheur ou chercheuse le fait à sa guise ? 71

Bei zusammengefassten Daten besteht die Anforderung darin, dass diese nicht auf die Originaldaten zurückgeführt werden können dürfen. Wie wird dies (standardmässig) gewährleistet? Tut dies jeder Forscher nach eigenem Ermessen? 72

Question / Frage 66 73

Quelles sont les techniques d'anonymisation ? Peut-on mettre en place une démarche qui garantit que les données sont anonymes ? En particulier dans un contexte médical, quels sont les critères à vérifier / les mesures à prendre pour que des données personnelles soient réellement anonymisées, c'est-à-dire ne permettent pas de réidentifier des personnes concernées ? Comment garantir que les données (médicales et générales) restent anonymes dans le temps ? Qui a la responsabilité d'assurer cette garantie ? 73

Welche Anonymisierungstechniken gibt es? Kann ein Verfahren eingeführt werden, das garantiert, dass die Daten anonym sind? Welche Kriterien müssen insbesondere in einem medizinischen Kontext überprüft / welche Massnahmen ergriffen werden, damit Personendaten tatsächlich anonymisiert werden, d. h. keine Re-Identifizierung von betroffenen Personen möglich ist? Wie kann sichergestellt werden, dass (medizinische und allgemeine) Daten im Laufe der Zeit anonym bleiben? Wer ist dafür verantwortlich, die Anonymität zu gewährleisten? 73

Question / Frage 67 73

Des données pseudonymisées peuvent-elles être partagées si la clé de chiffrement est conservée dans l'université ou la haute école ayant mené la recherche initiale ? 73

Dürfen pseudonymisierte Daten bekanntgegeben werden, wenn der Verschlüsselungscode in der Universität oder Hochschule aufbewahrt wird, welche ursprünglich die Forschung durchgeführt hat? 74

Question / Frage 68 74

Si des données sont pseudonymisées, comment stocker les différentes parties (données anonymisées, table de correspondance et données brutes) ? Dans différents espaces de stockage ? 74

Wenn Daten pseudonymisiert werden, wie sollen die verschiedenen Teile (die anonymisierten Daten, die Zuordnungstabelle und die Rohdaten) gespeichert werden? In verschiedenen Speicherbereichen? 75

Question / Frage 69 75

Quel niveau précis d'anonymisation est-il attendu suivant chaque type de données ? La question se pose, par exemple, pour les données de la recherche en médecine où une radio ou un scanner peuvent permettre d'identifier la personne. 75

Welches Mass an Anonymisierung wird je nach Art der Daten erwartet? Diese Frage stellt sich zum Beispiel bei medizinischen Forschungsdaten, bei denen ein Röntgenbild oder ein CT-Scan die Person identifizieren kann. 76

Question / Frage 70 77

Si des données personnelles (voire sensibles) sont pseudonymisées et que la table de correspondance est conservée exclusivement au sein d'une haute école, peuvent-elles être considérées comme anonymisées lorsqu'elles sont transmises et traitées par d'autres hautes écoles ? 77

Wenn persönliche (oder sogar besonders schützenswerte) Daten pseudonymisiert werden und die Zuordnungstabelle ausschliesslich innerhalb einer Hochschule aufbewahrt wird, können diese Daten dann

als anonymisiert betrachtet werden, wenn sie an andere Hochschulen übermittelt und dort bearbeitet werden? ... 77

Question / Frage 71 ... 78

Est-ce que des données pseudonymisées, qui ont été traitées dans le cadre de recherches menées par une haute école suisse, sont considérées comme des données personnelles si elles sont partagées dans un data repository (par conséquent sans une clé d'identification) ? Si oui, qu'est-ce que cela signifie juridiquement ? La réponse est-elle identique si les données sont soumises à la LRH ? ... 78

Werden pseudonymisierte Daten, die im Rahmen von Forschungsarbeiten an einer Schweizer Hochschule bearbeitet werden, als Personendaten betrachtet, wenn sie in einem Repositorium (also ohne einen Identifikationsschlüssel) veröffentlicht werden? Wenn ja, was bedeutet dies rechtlich gesehen? Ist die Antwort dieselbe, wenn die Daten dem Humanforschungsgesetz unterliegen? ... 78

XI. Secret de fonction / Amtsgeheimnis ... 79

Question / Frage 72 ... 79

Est-ce que tous les cas où aucun secret spécifique n'est applicable sont « par défaut » couverts par le secret de fonction ? En d'autres termes, est-ce que les données de recherche comportant des données personnelles collectées par des chercheurs et chercheuses d'une haute école dans le cadre de leurs projets sont soumises au secret de fonction (ce qui aurait des conséquences importantes en matière de partage) ? Concernant la portée du secret de fonction, est-il possible d'appliquer une méthode autre qu'une appréciation qu'au cas par cas ? ... 79

Wenn keine spezifische Geheimhaltungspflicht zur Anwendung kommt, findet dann «standardmässig» das Amtsgeheimnis Anwendung? Mit anderen Worten: fallen Forschungsdaten mit Personendaten, die von Forschern einer Hochschule im Rahmen ihrer Projekte gesammelt werden, unter das Amtsgeheimnis (was erhebliche Konsequenzen für die Bekanntgabe hätte)? Ist es in Bezug auf den Umfang des Amtsgeheimnisses möglich, eine andere Methode als eine Einzelfallbeurteilung anzuwenden? ... 79

XII. Archives / Archivierung ... 80

Question / Frage 73 ... 80

Est-il possible d'archiver des données dans des dépôts de données (conformément à la Loi sur l'archivage) ? ... 80

Ist es möglich, Daten in Repositorien zu archivieren (gemäss dem Archivierungsgesetz)? ... 80

Question / Frage 74 ... 80

La responsabilité des données change-t-elle avec la remise du processus et des données aux archives de l'État ? ... 80

Ändert sich die Verantwortung für die Daten mit der Übergabe des Prozesses und der Daten an das Staatsarchiv? ... 80

Question / Frage 75 ... 81

Qu'entend-on par « archives » au sens juridique du terme ? Comment le terme est-il utilisé dans le domaine de la recherche, notamment dans le contexte des dépôts ? ... 81

Was versteht man unter "Archiven" im rechtlichen Sinne? Wie wird der Begriff in der Forschung verwendet, insbesondere im Zusammenhang mit Datenablagen? ... 81

Question / Frage 76 81

Dans quelle mesure les résultats de la recherche doivent-ils être confiés aux archives d'État ? 81

In welchem Umfang sollten die Forschungsergebnisse den Staatsarchiven angeboten werden? 81

XIII. Durée de conservation et destruction des données / Speicherdauer und Datenvernichtung.....82

Question / Frage 77 82

Combien de temps puis-je conserver des données personnelles ?..... 82

Wie lange dürfen Personendaten aufbewahrt werden? 82

Question / Frage 78 82

Dans quelles conditions un délai de rétention exprimé sans une fin déterminée (qui reviendrait à conserver les données personnelles « tant qu'elles représentent un intérêt pour la recherche scientifique ») est-il acceptable ? 82

Unter welchen Bedingungen ist eine Speicherfrist, die ohne ein bestimmtes Ende festgelegt wird (was darauf hinauslaufen würde, dass Personendaten so lange gespeichert werden, «wie sie für die wissenschaftliche Forschung von Interesse sind»), akzeptabel? 82

Question / Frage 79 83

Quelles sont les mesures techniques pour garantir la destruction des données ? 83

Welche technischen Massnahmen gibt es, um die Vernichtung von Daten zu gewährleisten?..... 83

Question / Frage 80 84

Qui devrait prendre la décision de détruire des données ou de lever un embargo ? Si, par exemple, des données ont été déposées sous embargo pour 20 ans et que les chercheurs et chercheuses en charge ne travaillent plus dans la haute école ou l'université, sont décédés ou retraités, qui doit prendre cette décision et en assumer la responsabilité ? 84

Wer muss die Entscheidung über die Vernichtung von Daten oder die Aufhebung eines Embargos treffen? Wenn beispielsweise Daten für 20 Jahre mit einem Embargo versehen wurden und die verantwortlichen Forschenden nicht mehr an der Hochschule oder Universität arbeiten, verstorben oder pensioniert sind, wer sollte diese Entscheidung treffen und die Verantwortung dafür übernehmen? 84

Question / Frage 81 85

Combien de temps les données de recherche confidentielles (par exemple, les données personnelles et leur cryptage ; les déclarations de consentement), qui sont encore disponibles dans une haute école ou une université en plus des données de recherche ouvertes, doivent-elles rester disponibles ?..... 85

Wie lange müssen vertrauliche Forschungsdaten (z. B. Personendaten und deren Verschlüsselung; Einwilligungserklärungen), die an einer Hochschule oder Universität zusätzlich zu den veröffentlichten Forschungsdaten noch verfügbar sind, verfügbar bleiben? 85

Question / Frage 82 85

Pour combien d'années devons-nous garantir qu'un fichier soit ouvrable et lisible ? Qui doit se charger de maintenir les fichiers accessibles (ouvrables et lisibles) ? Qu'en est-il des logiciels pour que ces fichiers soient ouvrables ?..... 85

Für wie viele Jahre muss garantiert sein, dass eine Datei geöffnet und lesbar ist? Wer muss sich darum kümmern, dass die Dateien zugänglich (zu öffnen und lesbar) bleiben? Was ist mit der Software, die notwendig ist, damit diese Dateien geöffnet werden können? ... 86

Question / Frage 83 ... 86

Est-ce que le devoir d'information pour chaque communication ne s'applique plus si l'on a un consentement pour le partage des données en ORD ? ... 86

Gilt die Pflicht zur Information für jede Bekanntgaben von Personendaten nicht mehr, wenn eine Einwilligung zur Weiterverwendung von Daten im Rahmen von ORD vorliegt? ... 86

XIV. Autres / Weitere ... 88

Question / Frage 84 ... 88

Dans le cadre d'un projet de recherche dans le domaine de la santé, nous souhaitons utiliser le numéro AVS comme donnée d'identification. Le numéro AVS fait-il l'objet de dispositions particulières en matière de protection des données ? Est-il une donnée sensible ? Comment traiter cette donnée ? ... 88

Im Rahmen eines Forschungsprojekts im Gesundheitsbereich sollen die AHV-Nummern als Identifikationsdaten verwendet werden. Unterliegt die AHV-Nummer besonderen Datenschutzbestimmungen? Handelt es sich um besonders schützenswerte Personendaten? Wie soll mit diesen Daten umgegangen werden? ... 88

Question / Frage 85 ... 88

Qui peut signer un NDA professionnel pour données de recherche, par exemple pour le mode *restricted* d'un dépôt de données ? ... 88

Wer kann ein berufsbezogenes NDA für Forschungsdaten unterzeichnen, z. B. für den *Restricted* Mode eines Repositoriums? ... 88

Question / Frage 86 ... 89

La maintenance des données doit-elle être réalisée régulièrement en vue de vérifier l'exactitude, l'exhaustivité, le respect des dispositions légales, la durée de conservation, etc. des données de recherche collectées ? Qui en a la responsabilité ? ... 89

Muss die Datenpflege regelmässig durchgeführt werden, um die Richtigkeit, Vollständigkeit, Einhaltung der gesetzlichen Bestimmungen, Aufbewahrungsdauer usw. der gesammelten Forschungsdaten zu überprüfen? Wer ist dafür verantwortlich? ... 89

Question / Frage 87 ... 89

Dans quelles situations la Loi relative à la recherche sur l'être humain (LRH) s'applique-t-elle ? ... 89

In welchen Situationen gilt das Humanforschungsgesetz (HFG)? ... 90

Question / Frage 88 ... 90

Les données vidéo, qui contiennent des données personnelles, peuvent-elles être utilisées pour la formation et la formation continue ? ... 90

Dürfen Videodaten, die Personendaten enthalten, für die Aus- und Weiterbildung verwendet werden? . 90

Question / Frage 89 ... 91

Si une haute école (Data Processor) héberge des données médicales de patient·e·s d'un prestataire de soins (Data Controller), peut-elle les réutiliser à des fins de recherche ? ... 91

Wenn eine Hochschule als Auftragsdatenbearbeiter medizinische Patientendaten eines Gesundheitsdienstleisters (Datencontroller) hostet, darf sie diese dann zu Forschungszwecken weiterverwenden? ... 91

Question / Frage 90 ... 91

Que faut-il entendre par un traitement ou une communication « à des fins de recherche » ? Comment traiter les différentes réglementations dans les lois cantonales sur la protection des données et dans la Loi fédérale sur la protection des données ? ... 91

Was ist unter einer Bearbeitung bzw. Bekanntgaben «zu Forschungszwecken» zu verstehen? Wie ist mit den unterschiedlichen Regelungen in den kantonalen Datenschutzgesetzen bzw. dem Bundesgesetz über den Datenschutz umzugehen? ... 91

Question / Frage 91 ... 92

Peut-on considérer que les hautes écoles sont toutes « soumises à la même loi » lorsqu'il s'agit de traiter des données de recherche sous le « privilège de la recherche » ? ... 92

Kann man davon ausgehen, dass die Hochschulen alle «demselben Gesetz unterworfen» sind, wenn es darum geht, Forschungsdaten unter dem sog. Forschungsprivileg zu bearbeiten? ... 92

Question / Frage 92 ... 92

Quelle est l'autorité cantonale de protection des données compétente lorsque plusieurs hautes écoles de différents cantons travaillent ensemble sur un projet de recherche ? ... 92

Welche Kantonale Datenschutzbehörde ist zuständig, wenn mehrere Hochschulen aus verschiedenen Kantonen gemeinsam an einem Forschungsprojekt arbeiten? ... 92

I. Données publiques / Öffentlich zugängliche Daten

Question / Frage 1

Puis-je librement collecter et traiter des données personnelles d'une personnalité publique telle qu'un·e politicien·ne ?

La Loi fédérale sur la protection des données (LPD), qui s'applique aux hautes écoles fédérales, prévoit des « allégements » lorsque la personne concernée a rendu les données personnelles accessibles à tout un chacun et ne s'est pas opposée expressément au traitement. En particulier, le traitement ne nécessite pas de base légale et un transfert à l'étranger peut être réalisé sans autre exigence. La portée de ces allégements est toutefois limitée : la personne doit avoir elle-même exposé publiquement des informations la concernant (dans le cas d'une personnalité publique, ce serait le cas si elle possède un site internet où elle se présente). Ces règles ne s'appliquent en revanche pas si les informations sont publiées par un tiers. En outre, les autres exigences de la protection des données s'appliquent au surplus. Il n'existe donc pas de « droit » à collecter et traiter sans condition les données personnelles d'une personnalité publique, mais uniquement des allégements concernant des exigences spécifiques.

Les lois cantonales sur la protection des données, applicables aux hautes écoles cantonales (universités, hautes écoles spécialisées et hautes écoles pédagogiques), prévoient parfois des règles similaires. Il convient toutefois de vérifier dans chaque cas d'espèce dans la loi cantonale applicable si une règle est prévue s'agissant des personnalités publiques ou des données rendues publiquement accessibles.

Dürfen Personendaten einer öffentlichen Person, wie z. B. eines Politikers, frei gesammelt und bearbeitet werden?

Das Bundesgesetz über den Datenschutz, das für die eidgenössischen Hochschulen gilt, sieht „Erleichterungen" vor, wenn die betroffene Person die Personendaten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat. Insbesondere bedarf die Bearbeitung keiner gesetzlichen Grundlage und eine Übermittlung ins Ausland kann ohne weitere Anforderungen erfolgen. Diese Erleichterungen sind jedoch begrenzt: Die betroffene Person muss die Informationen selbst über sich öffentlich zugänglich gemacht haben (im Fall einer öffentlichen Person wäre dies der Fall, wenn sie eine Website besitzt, auf der sie selbst sich darstellt). Diese Regeln gelten also nicht, wenn die Informationen von einem Dritten veröffentlicht werden. Darüber hinaus gelten die weiteren Anforderungen des Datenschutzes. Es gibt also kein „Recht", Personendaten einer öffentlichen Person bedingungslos zu sammeln und zu bearbeiten, sondern nur Erleichterungen in Bezug auf bestimmte Anforderungen.

Die kantonalen Datenschutzgesetze, die für die kantonalen Hochschulen (Universitäten, Fachhochschulen und Pädagogischen Hochschulen) gelten, sehen zum Teil ähnliche Regeln vor. Es muss jedoch in jedem Einzelfall das anwendbare kantonalen Gesetz geprüft werden, ob eine Regelung in Bezug auf Personen des öffentlichen Lebens oder öffentlich zugänglich gemachte Daten vorhanden ist.

Question / Frage 2

Utilisation des données personnelles archivées : est-ce que je peux utiliser des données personnelles issues d'archives publiques ?

L'archivage est une forme spécifique de traitement de données. Les données issues des archives sont réutilisables dans le respect des conditions fixées par les réglementations applicables non seulement en matière d'archivage et de protection des données mais également des règles sectorielles spécifiques réglant le domaine.

S'agissant plus particulièrement de la protection des données, les principes suivants doivent notamment être respectés :

- le traitement doit avoir lieu pour l'accomplissement d'une tâche légale (dans le cas d'une haute école, il s'agit en l'occurrence de l'enseignement et de la recherche) ;
- le but du traitement doit être déterminé ;
- le traitement doit être approprié et nécessaire à la réalisation du but (dans le cas présent, il ne doit être effectué qu'avec les données nécessaires et pendant la durée nécessaire) ;
- il n'y a pas de violation de la bonne foi par le traitement ;
- les prescriptions en matière de sécurité et de confidentialité sont respectées ;
- si un consentement est requis, il faut s'assurer qu'il existe effectivement.

Zur Verwendung von archivierten Personendaten: Können Personendaten aus öffentlichen Archiven verwendet werden?

Die Archivierung ist eine spezifische Form der Datenbearbeitung. Daten aus Archiven sind unter den Bedingungen wiederverwendbar, welche nach den Vorschriften zur Archivierung und zum Datenschutz, darüber hinaus aber auch nach allfälligen bereichsspezifischen Vorschriften, gelten.

Im Hinblick auf den Datenschutz müssen insbesondere die folgenden Grundsätze beachtet werden:

- die Bearbeitung muss zur Erfüllung einer gesetzlichen Aufgabe erfolgen (im Falle einer Hochschule sind dies Lehre und Forschung);
- der Zweck der Bearbeitung muss bestimmt sein;
- die Bearbeitung muss für die Erreichung des Zwecks geeignet und erforderlich sein (in diesem Fall nur mit den erforderlichen Daten und für die erforderliche Dauer);
- es liegt keine Verletzung des guten Glaubens durch die Bearbeitung vor
- die Sicherheits- und Vertraulichkeitsvorschriften werden eingehalten;
- falls eine Einwilligung erforderlich ist, muss sichergestellt werden, dass diese tatsächlich vorliegt.

Question / Frage 3

Est-ce que je peux, dans le cadre de mes recherches, utiliser puis publier/diffuser des données personnelles (personnes en vie) qui sont accessibles publiquement par exemple sur des sites internet, des bases de données accessibles en ligne ?

La Loi fédérale sur la protection des données (LPD), qui s'applique aux écoles polytechniques fédérales, prévoit des « allégements » lorsque la personne concernée a rendu les données personnelles accessibles à tout un chacun et ne s'est pas opposée expressément au traitement ou si les données personnelles proviennent d'un registre prévu par la loi et accessible au public. En particulier, dans ces deux cas, un transfert à l'étranger peut être réalisé sans autre exigence. La portée de ces allégements est toutefois limitée s'agissent des données personnelles rendues accessibles : la personne doit avoir elle-même exposé publiquement des informations la concernant (ce serait le cas si elle possède un site internet où elle se présente). Ces règles ne s'appliquent en revanche pas si les informations sont publiées par un tiers. En outre, les autres exigences de la protection des données s'appliquent au surplus. Il n'existe donc pas de « droit » à collecter et traiter sans condition des données personnelles accessibles publiquement, mais uniquement des allégements concernant des exigences spécifiques.

Les lois cantonales sur la protection des données, qui s'appliquent aux hautes écoles cantonales (universités, hautes écoles spécialisées et hautes écoles pédagogiques), prévoient parfois des règles similaires. Il convient toutefois de vérifier dans chaque cas d'espèce dans la loi cantonale applicable si une règle est prévue s'agissant des données personnelles publiquement accessibles.

Darf ich im Rahmen meiner Forschung Personendaten (von lebenden Personen), die öffentlich zugänglich sind, z. B. auf Websites, in online zugänglichen Datenbanken verwenden und dann veröffentlichen/verbreiten?

Das Bundesgesetz über den Datenschutz, das für die eidgenössischen Hochschulen gilt, sieht „Erleichterungen“ vor, wenn die betroffene Person die Personendaten allgemein zugänglich gemacht und eine Bearbeitung nicht

ausdrücklich untersagt hat oder wenn die Personendaten aus einem gesetzlich vorgesehenen und öffentlich zugänglichen Register stammen. In diesen beiden Fällen kann eine Übermittlung ins Ausland ohne weiteres erfolgen. Diese Erleichterung ist jedoch begrenzt, wenn es um zugänglich gemachte Personendaten geht: Die betroffene Person muss die Informationen selbst über sich öffentlich zugänglich gemacht haben (dies wäre der Fall, wenn die Person eine Website besitzt, auf der sie selbst sich darstellt). Diese Regeln gelten also nicht, wenn die Informationen von einem Dritten veröffentlicht werden. Darüber hinaus gelten die weiteren Anforderungen des Datenschutzes. Es gibt also kein „Recht", öffentlich zugängliche Personendaten bedingungslos zu sammeln und zu bearbeiten, sondern nur Erleichterungen in Bezug auf bestimmte Anforderungen.

Die kantonalen Datenschutzgesetze, die für die kantonalen Hochschulen (Universitäten, Fachhochschulen und Pädagogischen Hochschulen) gelten, sehen zum Teil ähnliche Regeln vor. Es muss jedoch in jedem Einzelfall das anwendbare kantonalen Gesetz geprüft werden, ob eine Regelung in Bezug auf öffentlich zugängliche Personendaten vorhanden ist.

II. Application du RGPD / Anwendbarkeit der DSGVO

Question / Frage 4

Si je mène depuis la Suisse (affiliation à une haute école suisse) des recherches sur des citoyen·ne·s européen·ne·s qui impliquent le traitement de leurs données personnelles, quelle loi sur la protection des données prévaut ? Est-ce que la situation est différente si je mène ces recherches depuis le territoire européen avec affiliation à une haute école suisse ?

Dans le premier cas (chercheur ou chercheuse en Suisse et institution en Suisse), la législation suisse en matière de protection des données s'applique (loi fédérale si l'institution est une haute école fédérale, loi cantonale si l'institution est une haute école cantonale (université, haute école spécialisée ou haute école pédagogique)). La législation européenne s'applique au surplus si la recherche implique un suivi (par exemple, suivi des habitudes) de personnes concernées qui se trouvent sur le territoire de l'UE (c'est donc le lieu où se trouve la personne, et non sa nationalité, qui est pertinent), ainsi que dans le cas où le traitement des données est lié à la fourniture d'un service qui vise des résident·e·s européen·ne·s. Dans ces deux cas, les législations suisse et européenne doivent être respectées.

Dans le deuxième cas (chercheur ou chercheuse dans un pays de l'UE, affiliation à une institution suisse), le RGPD s'applique en cas de suivi comme exposé ci-dessus, mais également dans les deux hypothèses suivantes: (i) si le chercheur ou la chercheuse travaille depuis un établissement stable dans l'UE (par exemple, un poste de travail mis à disposition par une université de l'UE avec une certaine régularité) ou (ii) si le chercheur ou la chercheuse est également rattachée à un établissement situé dans l'UE. L'affiliation à la haute école suisse impliquera également l'application du droit suisse.

À noter que, si la recherche s'inscrit dans une véritable collaboration avec une haute école ou une université située dans l'UE, la haute école ou l'université de l'UE sera soumise au RGPD et considérée comme responsable du traitement conjoint avec la haute école ou l'université suisse. Cela ne change rien aux conditions d'application du RGPD : il ne s'applique que dans les cas susmentionnés. Toutefois, les deux institutions peuvent décider qu'elles respecteront toutes deux la législation suisse et le RGPD.

Remarque : une extension du RGPD à l'espace EEE a été effectuée par décision du Comité mixte de l'EEE, de sorte que le RGPD est également directement applicable en Norvège, en Islande et dans la Principauté de Liechtenstein.

Wenn ich von der Schweiz aus (mit Zugehörigkeit zu einer Schweizer Hochschule) Forschung über EU-Bürger betreibe und dabei deren Personendaten bearbeite, welches Datenschutzgesetz gilt dann? Ist die Situation anders, wenn ich diese Forschung von europäischem Territorium aus betreibe und (trotzdem) einer Schweizer Hochschule angehöre?

Im ersten Fall (Forscher*in in der Schweiz und Institution in der Schweiz) gilt die schweizerische Datenschutzgesetzgebung (Bundesgesetz, wenn die Institution eine eidgenössische Hochschule ist, kantonales Gesetz, wenn die Institution eine kantonale Hochschule (Universität, Fachhochschule oder Pädagogische Hochschule) ist). Das EU-Recht gilt darüber hinaus, wenn die Forschung eine Überwachung (z. B. Überwachung der Gewohnheiten) von Personen beinhaltet, die sich im EU-Gebiet befinden (relevant ist also der Ort, an dem sich eine betroffene Person befindet, und nicht ihre Staatsangehörigkeit), sowie in Fällen, in denen die Datenbearbeitung mit der Erbringung einer Dienstleistung verbunden ist, die sich an in der EU ansässige Personen richtet. In diesen beiden Fällen müssen sowohl die schweizerische als auch die europäische Gesetzgebung eingehalten werden.

Im zweiten Fall (Forscher*in in einem EU-Land, Zugehörigkeit zu einer Schweizer Institution) gilt die DSGVO jedenfalls in den oben beschrieben Fällen, zudem in den beiden folgenden Konstellationen: (i) wenn der/die Forscher/in von einer festen Institution im EU-Raum aus arbeitet (z. B. ein Arbeitsplatz, der von einer Hochschule

in der EU mit einer gewissen Regelmässigkeit zur Verfügung gestellt wird) oder (ii) wenn der*die Forsche*/in auch einer Institution in der EU zugeordnet ist. Die Zugehörigkeit zu einer Schweizer Hochschule impliziert zudem die Anwendung des Schweizer Rechts.

Sofern die Forschung Teil einer echten Zusammenarbeit mit einer Hochschule oder Universität im EU-Raum ist, gilt zu beachten, dass die Hochschule oder Universität im EU-Raum der DSGVO unterliegt und beide Hochschulen als gemeinsame Verantwortliche gelten für die Datenbearbeitung. Dies ändert nichts an den Bedingungen für die Anwendung der DSGVO: Sie gilt nur in den oben genannten Fällen. Beide Institutionen können jedoch beschliessen, dass sie beide sowohl das Schweizer Recht als auch die DSGVO einhalten werden.

Anmerkung: Eine Ausdehnung der DSGVO auf den EWR-Raum ist durch Beschluss des Gemeinsamen EWR-Ausschusses erfolgt, so dass die DSGVO auch in Norwegen, Island und im Fürstentum Liechtenstein unmittelbare Anwendung findet.

Question / Frage 5

À quel moment le RGPD s'applique-t-il et avec quelles conséquences sur l'ORD :
(1) si les données de recherche traitées contiennent des données personnelles de citoyen·ne·s européen·ne·s ?
(2) si des données de recherche contenant des données personnelles sont stockées voire traitées dans un pays de l'UE ?

La nationalité de la personne concernée ne joue pas de rôle dans l'application du RGPD. C'est le lieu de résidence de la personne concernée qui est déterminant ou le lieu où les données sont traitées.

Dans le premier cas (données de recherche traitées contenant des données personnelles de citoyen·ne·s européen·ne·s), si le chercheur ou la chercheuse travaille depuis la Suisse, sans affiliation à une institution établie dans l'UE et sans stockage ou traitement de données personnelles dans l'UE, le RGPD s'applique uniquement si la recherche implique un suivi (par exemple, suivi des habitudes) de personnes qui se trouvent sur le territoire de l'UE. La citoyenneté n'est pas pertinente à cet égard, c'est le fait de se trouver sur le territoire de l'UE qui importe.

Dans le deuxième cas (données de recherche contenant des données personnelles stockées voire traitées dans un pays de l'UE), le RGPD s'applique en cas de suivi de personnes qui se trouvent sur le territoire de l'UE (situation ci-dessus), mais également dans les situations suivantes :

(i) si les données sont stockées ou traitées dans l'UE,
(ii) si le chercheur ou la chercheuse travaille depuis un « établissement stable » dans l'UE (par exemple, un poste de travail mis à disposition par une haute école de l'UE) ou
(iii) si le chercheur ou la chercheuse est également rattachée à un établissement situé dans l'UE.

Si l'hébergement est effectué par un sous-traitant dans le champ d'application territorial du RGPD, il sera soumis au RGPD (mais pas la haute école).

Le fait d'être soumis au RGPD n'implique a priori pas de restrictions particulières s'agissant de l'ORD ; les principes valables lorsque seule la législation suisse s'applique restent applicables.

Remarque : une extension du RGPD à l'espace EEE a été effectuée par décision du Comité mixte de l'EEE, de sorte que le RGPD est également directement applicable en Norvège, en Islande et dans la Principauté de Liechtenstein.

In welchen Fällen muss eine Hochschule die DSGVO anwenden und welche Einschränkungen bestehen ggf. bei der Veröffentlichung von Daten?
(1) wenn die bearbeiteten Forschungsdaten Personendaten von EU-Bürgern enthalten?
(2) wenn Forschungsdaten, die Personendaten enthalten, in einem EU-Land gespeichert oder bearbeitet werden?

Die Staatsangehörigkeit einer betroffenen Person spielt bei der Anwendung der DSGVO keine Rolle. Entscheidend für die Geltung der DSGVO ist der Aufenthaltsort der betroffenen Person bzw. der Ort, an dem die Daten bearbeitet werden.

Im ersten Fall (bearbeitete Forschungsdaten enthalten Personendaten von EU-Bürgern), d.h., wenn der Forscher*die Forscherin von der Schweiz aus tätig wird, keiner Institution mit Sitz in der EU angehört und keine Personendaten im EU-Raum speichert oder bearbeitet, findet die DSGVO nur Anwendung, wenn die Forschung eine Überwachung (z. B. Überwachung der Gewohnheiten) von Personen beinhaltet, die sich im Gebiet der EU befinden.

Die Staatsbürgerschaft ist in hierbei nicht relevant, sondern die Tatsache, dass man sich auf dem Gebiet der EU befindet.

Im zweiten Fall (Forschungsdaten enthalten Personendaten, die in einem EU-Land gespeichert oder bearbeitet werden) findet die DSGVO Anwendung, wenn eine Überwachung von in der EU sich befindlichen Personen stattfindet (siehe oben), zudem in den folgenden Situationen:

(i) wenn die Daten im EU-Raum gespeichert oder bearbeitet werden,
(ii) wenn der Forscher*die Forscherin von einer „festen Institution“ im EU-Raum aus arbeitet (z. B. von einem Arbeitsplatz, der von einer Hochschule im EU-Raum zur Verfügung gestellt wird) oder
(iii) wenn der Forscher*die Forscherin auch einer Institution im EU-Raum angegliedert ist.

Wenn ein Datenhosting von einem Subunternehmer im räumlichen Anwendungsbereich der DSGVO durchgeführt wird, unterliegt dieser Subunternehmer der DSGVO (aber nicht die Hochschule).

Sofern man der DSGVO unterliegt, zieht dies a priori keine besonderen Einschränkungen in Bezug auf ORD nach sich; die Grundsätze, die nach Schweizer Recht gelten sind, sind anwendbar.

Anmerkung: Eine Ausdehnung der DSGVO auf den EWR-Raum ist durch Beschluss des Gemeinsamen EWR-Ausschusses erfolgt, so dass die DSGVO auch in Norwegen, Island und im Fürstentum Liechtenstein unmittelbare Anwendung findet.

III. Responsabilité / Verantwortung

Question / Frage 6

Si l'anonymisation d'un jeu de données est incomplète, et que le jeu de données est mis à disposition publiquement, qui a la responsabilité finale ?

Du point de vue juridique, la haute école ou l'université est responsable du traitement des données personnelles et donc responsable de respecter les règles en matière de protection des données et de sécurité de l'information.

En pratique, l'institution doit veiller à ce que son personnel connaisse et applique les exigences légales dans ce domaine. Les chercheurs et chercheuses responsables d'un projet doivent s'assurer que leur recherche respecte la protection des données, en suivant notamment les éventuelles instructions ou lignes directrices de l'institution.

De plus, les collaborateurs et collaboratrices sont soumis au secret de fonction à titre individuel.

Si la responsabilité d'une institution est engagée, celle-ci peut toutefois, à certaines conditions, se retourner contre l'employé·e, notamment si ce dernier ou cette dernière a commis une négligence grave ou une faute intentionnelle.

Wenn die Anonymisierung des Datensatzes unvollständig ist und der Datensatz öffentlich zugänglich gemacht wird, wer trägt dann die endgültige Verantwortung?

Aus rechtlicher Sicht ist die Hochschule oder Universität für die Bearbeitung der Personendaten verantwortlich und damit auch für die Einhaltung der Vorschriften zum Datenschutz und zur Informationssicherheit.

In der Praxis muss die Institution dafür sorgen, dass ihre Mitarbeitenden die gesetzlichen Anforderungen in diesem Bereich kennen und anwenden. Die für ein Projekt verantwortlichen Forscher*innen müssen sicherstellen, dass bei ihrer Forschung der Datenschutz eingehalten wird, indem sie insbesondere etwaige Anweisungen oder Richtlinien der Institution befolgen.

Darüber hinaus unterliegen die Mitarbeitenden individuell dem Amtsgeheimnis.

Wenn eine Institution haftbar gemacht wird, kann sie unter bestimmten Bedingungen auf den*die verantwortliche*n Mitarbeiter*in Rückgriff nehmen, namentlich, wenn dieser*diese grobfahrlässig oder vorsätzlich gehandelt hat.

Question / Frage 7

Comment déterminer le ou la propriétaire des données ?

Il s'agit d'une question de responsabilité des données et non de propriété sur les données en tant que telle. La question doit être analysée sous l'angle de la notion de responsable de traitement (et éventuellement de responsabilité conjointe).

Du point de vue juridique, la haute école ou l'université est responsable du traitement des données personnelles et donc responsable de respecter les règles en matière de protection des données et de sécurité de l'information.

En pratique, l'institution doit veiller à ce que son personnel connaisse et applique les exigences légales dans ce domaine. Les chercheurs et chercheuses responsables d'un projet doivent s'assurer que leur recherche respecte la protection des données, en suivant notamment les éventuelles instructions ou lignes directrices de l'institution.

De plus, les collaborateurs et collaboratrices sont soumis au secret de fonction à titre individuel.

Wie bestimmt man den Dateneigentümer?

Im Zusammenhang mit dem Datenschutz geht es um die Frage nach der Verantwortlichkeit für eine Datenbearbeitung und nicht nach dem Eigentum an Daten. Die Frage muss insofern unter dem Gesichtspunkt des

für eine Bearbeitung Verantwortlichen (und möglicherweise einer gemeinsamen Verantwortlichkeit) beleuchtet werden.

Aus rechtlicher Sicht ist die Hochschule oder Universität für die Bearbeitung von Personendaten verantwortlich und damit auch für die Einhaltung der Vorschriften zum Datenschutz und zur Informationssicherheit.

In der Praxis muss die Institution dafür sorgen, dass ihre Mitarbeitenden die gesetzlichen Anforderungen in diesem Bereich kennen und anwenden. Die für ein Projekt verantwortlichen Forscher*innen müssen sicherstellen, dass bei ihrer Forschung der Datenschutz eingehalten wird, indem sie insbesondere etwaige Anweisungen oder Richtlinien der Institution befolgen.

Darüber hinaus unterliegen die Mitarbeitenden individuell dem Amtsgeheimnis.

Question / Frage 8

Qui est responsable de la sécurité de l'information et de la protection des données en clair (c'est-à-dire lisibles ou non chiffrées) ?

Du point de vue juridique, la haute école ou l'université est responsable du traitement des données personnelles et donc responsable de respecter les règles en matière de protection des données et de sécurité de l'information.

En pratique, l'institution doit veiller à ce que son personnel connaisse et applique les exigences légales dans ce domaine. Les chercheurs et chercheuses responsables d'un projet doivent s'assurer que leur recherche respecte la protection des données, en suivant notamment les éventuelles instructions ou lignes directrices de l'institution.

De plus, les collaborateurs et collaboratrices sont soumis au secret de fonction à titre individuel.

Wer ist verantwortlich für die Informationssicherheit und den Schutz von Daten im Klartext (d. h. lesbar oder unverschlüsselt)?

Aus rechtlicher Sicht ist die Hochschule oder Universität für die Bearbeitung von Personendaten verantwortlich und damit auch für die Einhaltung der Vorschriften zum Datenschutz und zur Informationssicherheit.

In der Praxis muss die Institution dafür sorgen, dass ihre Mitarbeitenden die gesetzlichen Anforderungen in diesem Bereich kennen und anwenden. Die für ein Projekt verantwortlichen Forscher*innen müssen sicherstellen, dass bei ihrer Forschung der Datenschutz eingehalten wird, indem sie insbesondere etwaige Anweisungen oder Richtlinien der Institution befolgen.

Darüber hinaus unterliegen die Mitarbeitenden individuell dem Amtsgeheimnis.

Question / Frage 9

Qui est le·la responsable de traitement pour les données ORD : la plateforme, le chercheur ou la chercheuse, la haute école ? Est-ce que cette responsabilité peut être transférée ?

Du point de vue juridique, la haute école ou l'université est responsable du traitement des données personnelles et donc responsable de respecter les règles en matière de protection des données et de sécurité de l'information.

En pratique, l'institution doit veiller à ce que son personnel connaisse et applique les exigences légales dans ce domaine. Les chercheurs et chercheuses responsables d'un projet doivent s'assurer que leur recherche respecte la protection des données, en suivant notamment les éventuelles instructions ou lignes directrices de l'institution.

De plus, les collaborateurs et collaboratrices sont soumis au secret de fonction à titre individuel.

Un transfert de responsabilité (par exemple sur une base contractuelle) est exclu ; en communiquant les données à un tiers pour que celui-ci puisse les traiter sous sa propre responsabilité (à ses propres fins), ce tiers assume la

responsabilité des données reprises ; pour les données restantes (même si elles sont désormais disponibles auprès de deux organisations), la responsabilité reste celle de l'organisation d'origine.

Wer ist der/die Verantwortliche für die Bearbeitung von ORD-Daten: die Plattform, der*die Forscher*in oder die Hochschule? Kann diese Verantwortung übertragen werden?

Aus rechtlicher Sicht ist die Hochschule oder Universität für die Bearbeitung von Personendaten verantwortlich und damit auch für die Einhaltung der Vorschriften zum Datenschutz und zur Informationssicherheit.

In der Praxis muss die Institution dafür sorgen, dass ihre Mitarbeitenden die gesetzlichen Anforderungen in diesem Bereich kennen und anwenden. Die für ein Projekt verantwortlichen Forscher*innen müssen sicherstellen, dass bei ihrer Forschung der Datenschutz eingehalten wird, indem sie insbesondere etwaige Anweisungen oder Richtlinien der Institution befolgen.

Darüber hinaus unterliegen die Mitarbeitenden individuell dem Amtsgeheimnis.

Eine Übertragung der Datenverantwortlichkeit (z. B. auf vertraglicher Grundlage) ist ausgeschlossen. Indem die Daten an einen Dritten zur Bearbeitung in eigener Verantwortlichkeit (zu eigenen Zwecken) bekanntgegeben werden, übernimmt dieser Dritte indes die Verantwortlichkeit für die übernommenen Daten. Für die verbleibenden Daten (auch wenn sie nun bei zwei Organisationen verfügbar sind) verbleibt die Verantwortlichkeit bei der ursprünglichen Organisation.

Question / Frage 10

Qui est responsable de la conformité et du caractère non frauduleux des données ? C'est en principe le ou la chercheuse qui dépose. Mais qu'en est-il quand le chercheur ou la chercheuse est accompagné par des data stewards et qu'une autre personne dépose effectivement ses données avec son accord ? Que se passe-t-il en cas de révocation du consentement ?

Du point de vue juridique, la haute école ou l'université est responsable du traitement des données personnelles et donc responsable de respecter les règles en matière de protection des données et de sécurité de l'information.

En pratique, l'institution doit veiller à ce que son personnel connaisse et applique les exigences légales dans ce domaine. Les chercheurs et chercheuses responsables d'un projet doivent s'assurer que leur recherche respecte la protection des données, en suivant notamment les éventuelles instructions ou lignes directrices de l'institution.

De plus, les collaborateurs et collaboratrices sont soumis au secret de fonction à titre individuel.

En cas d'intervention de data stewards ou de tiers, il convient de définir comment les responsabilités (internes) sont partagées.

En cas de révocation du consentement, il en va de même que pour la responsabilité : il faut clarifier, par le biais de réglementations internes des compétences, qui traite et met en œuvre la révocation ou ses conséquences (suppression des données personnelles).

Wer ist dafür verantwortlich, dass Daten korrekt und nicht manipuliert sind? Im Prinzip ist es der*die Forscher*in, welche*r die Daten ablegt. Aber was passiert, wenn der*die Forscher*in von Data Stewards unterstützt wird und eine andere Person die Daten im Auftrag des*der Forschers*in ablegt? Was passiert im Falle eines Widerrufs?

Aus rechtlicher Sicht ist die Hochschule oder Universität für die Bearbeitung von Personendaten verantwortlich und damit auch für die Einhaltung der Vorschriften zum Datenschutz und zur Informationssicherheit.

In der Praxis muss die Institution dafür sorgen, dass ihre Mitarbeitenden die gesetzlichen Anforderungen in diesem Bereich kennen und anwenden. Die für ein Projekt verantwortlichen Forscher*innen müssen sicherstellen, dass bei ihrer Forschung der Datenschutz eingehalten wird, indem sie insbesondere etwaige Anweisungen oder Richtlinien der Institution befolgen.

Darüber hinaus unterliegen die Mitarbeitenden individuell dem Amtsgeheimnis.

Im Falle Data Stewards oder Dritten eingesetzt werden, ist zu regeln, wie die (internen) Verantwortlichkeiten aufgeteilt werden.

Im Falle eines Widerrufs der Einwilligung gilt das Gleiche wie bei der Verantwortlichkeit: Es muss durch interne Kompetenzregelungen geklärt werden, wer den Widerruf oder dessen Folgen (Löschung der Personendaten) bearbeitet und umsetzt.

Question / Frage 11

Dans quelle mesure la responsabilité d'une université ou haute école peut-elle être engagée en cas de conflit vis-à-vis des données de recherche ? Notamment en ce qui concerne :
(1) La production de données frauduleuses ;
(2) La rétractation d'un article ;
(3) Un leak de données sensibles ;
(4) La publication de données personnelles, sensibles ou soumises au secret sans consentement effectif sur une plateforme de partage de données (par exemple, SwissUBase) (que l'erreur provienne soit du chercheur ou de la chercheuse, des data stewards, de la curation de la haute école, de la curation des partenaires)

Du point de vue juridique, la haute école ou l'université est responsable du traitement des données personnelles et responsable de respecter les règles en matière de protection des données et de sécurité de l'information.

Si la responsabilité d'une institution est engagée, celle-ci peut toutefois, à certaines conditions, se retourner contre l'employé·e qui aurait commis une faute.

Inwieweit kann eine Universität oder Hochschule im Falle eines Problems im Zusammenhang mit Forschungsdaten verantwortlich gemacht werden? Insbesondere im Hinblick auf:
(1) eine Fälschung von Daten?
(2) einen Rückzug eines Artikels?
(3) en Bekanntwerden von besonders schützenswerten Daten?
(4) eine Veröffentlichung von persönlichen, sensiblen oder geheimhaltungsbedürftigen Daten auf einer Datensharing-Plattform (z.B. SwissUBase) ohne wirksame Einwilligung (unabhängig davon, ob der Fehler von den Forschenden, den Data Stewards, einem Hochschul-Vertreter oder einem Partner erfolgte)

Aus rechtlicher Sicht ist die Hochschule oder Universität für die Bearbeitung von Personendaten verantwortlich und damit auch für die Einhaltung der Vorschriften zum Datenschutz und zur Informationssicherheit.

Wenn eine Institution zur Verantwortung gezogen wird, kann sie jedoch unter bestimmten Bedingungen auf den*die Arbeitnehmer*in Rückgriff nehmen, der*die den Fehler begangen hat.

Question / Frage 12

Si un chercheur ou une chercheuse quitte la haute école à laquelle il·elle est affilié·e (départ à la retraite, fin de contrat ou encore changement de poste au sein de l'institution), qui s'occupe des droits de la personne concernée si les données n'ont pas encore été rendues anonymes (ne peuvent pas être rendues anonymes) ?

Une personne concernée a des droits et il faut mettre en œuvre un processus qui permet de gérer ses éventuelles demandes même si la chercheuse ou le chercheur a quitté la haute école ou l'université. D'un point de vue juridique, la responsabilité de gérer ces demandes incombera à la haute école ou l'université. Pour chaque traitement, la question doit en principe être réglée avant même le début du traitement par le responsable du traitement (c'est-à-dire la haute école ou l'université) en vertu de son obligation d'assurer la protection des données dès la conception et par défaut, ou au plus tard durant le traitement (art. 7 Loi fédérale sur la protection des données).

Wenn ein*e Forscher*in die Hochschule, der er*sie angehört, verlässt (Pensionierung, Vertragsende oder Stellenwechsel innerhalb der Institution), wer kümmert sich dann um die Rechte der betroffenen Person, wenn die Daten noch nicht anonymisiert wurden (nicht anonymisiert werden können)?

Eine betroffene Person hat Rechte und es muss ein Prozess implementiert werden, der es ermöglicht, allfällige Anträge zu verwalten, auch wenn der*die Forscher*in die Hochschule oder Universität verlassen hat. Aus rechtlicher Sicht liegt die Verantwortung für die Verwaltung dieser Anfragen bei der Hochschule oder Universität. Bei jeder Datenbearbeitung muss die Frage grundsätzlich schon zu Beginn, spätestens aber während der Bearbeitung durch den für die Bearbeitung Verantwortlichen (d. h. die Hochschule oder Universität) geklärt sein, da ihn die Verpflichtung trifft, den Datenschutz von Anfang an und standardmässig zu gewährleisten (Art. 7 Bundesgesetz über den Datenschutz).

Question / Frage 13

Qui est responsable du partage des données personnelles collectées dans le cadre d'un projet de recherche d'une haute école ?

La haute école ou l'université est responsable du traitement des données personnelles, et donc également du partage de ces données.

En cas de partage de données personnelles avec une autre entité (p. ex. une autre institution), cette entité peut devenir responsable *conjoint* du traitement (p. ex. si un projet de recherche est géré en commun) ou responsable indépendant du traitement (p. ex. si elle réutilise des données pour un autre projet). Dans tous les cas, il est préférable de clarifier les droits et obligations par contrat ou convention.

Il est judicieux de faire examiner les décisions relatives à la transmission de données de recherche à l'interne de la haute école ou de l'université en suivant le processus mis en place (s'il en existe un).

Wer ist für die Bekanntgabe von Personendaten verantwortlich, die im Rahmen eines Forschungsprojekts an einer Hochschule gesammelt wurden?

Die Hochschule oder Universität ist für die Bearbeitung von Personendaten verantwortlich und damit auch für die Bekanntgabe dieser Daten.

Werden Personendaten mit einer anderen Stelle (z. B. einer anderen Institution) geteilt, kann diese Stelle gemeinsame Verantwortliche der Datenbearbeitung werden (z. B. wenn ein Forschungsprojekt gemeinsam durchgeführt wird) oder sie kann unabhängig von der teilenden Institution Verantwortliche für die Datenbearbeitung werden (z. B. wenn sie Daten für ein anderes Projekt weiterverwendet). In allen Fällen ist es am besten, die Rechte und Pflichten durch einen Vertrag oder eine Vereinbarung zu klären.

Es ist sinnvoll, Entscheidungen über die Bekanntgabe von Forschungsdaten innerhalb der Hochschule oder Universität anhand eines bestehenden Prozesses (falls vorhanden) überprüfen zu lassen.

Question / Frage 14

Quels sont les risques si les exigences de sécurité des répertoires ne sont pas suffisantes ?

L'institution est exposée à des risques juridiques (p. ex. une éventuelle indemnisation d'une personne lésée suite à la sécurité insuffisante) ainsi que réputationnels. Si la responsabilité d'une institution est engagée, celle-ci peut toutefois, à certaines conditions, se retourner contre le chercheur employé ou la chercheuse employée qui aurait commis une faute.

Le chercheur ou la chercheuse responsable risque (à titre personnel) principalement une sanction pénale (violation du secret de fonction) et disciplinaire, d'être tenu responsable en cas de dommage, ainsi que ne de plus pouvoir utiliser les données.

Was passiert, wenn Repositorien den Schutzanforderungen nicht genügen?

Die Institution ist sowohl rechtlichen Risiken (z. B. einer möglichen Forderung einer geschädigten Person aufgrund unzureichenden Schutzes) als auch Reputationsrisiken ausgesetzt. Wenn eine Institution haftbar gemacht wird, kann sie jedoch unter bestimmten Bedingungen bei dem*der angestellten Forscher*in, der*die einen Fehler begangen hat, Rückgriff nehmen.

Der*Die verantwortliche Forscher*in riskiert (als Einzelperson) vor allem eine strafrechtliche Massnahme (durch die Verletzung des Amtsgeheimnisses), eine disziplinarische Sanktion und eine Haftung im Schadensfall, muss sich allfällig aber auch darauf einstellen, die Daten nicht mehr verwenden zu können.

Question / Frage 15

Qui est responsable des données transmises aux archives de l'État ?

Voir à ce sujet la Question / Frage 74.

Wer ist verantwortlich für Daten, die an das Staatsarchiv übergeben werden?

Siehe hierzu Question / Frage 74.

IV. Transfert de données personnelles à l’étranger / Übermittlung von Personendaten ins Ausland

Question / Frage 16

Quelles conditions dois-je respecter pour transférer des données personnelles hors de la Suisse (par exemple sur la plateforme autrichienne Pangaea pour les géosciences), et surtout hors de l'UE ?

La Loi fédérale sur la protection des données (qui s'applique aux écoles fédérales) et les lois cantonales (qui s'appliquent aux hautes écoles cantonales (universités, hautes écoles spécialisées et hautes écoles pédagogiques)) contiennent des dispositions spécifiques pour la communication (ou transfert) de données à l’étranger.

En principe, il faudra s’assurer que le pays concerné dispose d'une législation assurant un niveau de protection adéquat. L’annexe 1 de l’Ordonnance sur la protection des données (OPDo) donne une liste des États adéquats au niveau fédéral. Les cantons y renvoient généralement. Dans le cas des États-Unis, le Conseil fédéral a décidé le 14.08.2024 d'ajouter les États-Unis à la liste à partir du 15.09.2024 avec la précision que les organisations doivent être certifiées ; le Conseil fédéral considère ainsi qu'en cas d'échange de données avec une entreprise américaine, un niveau de protection adéquat est assuré, pour autant que l'entreprise américaine soit certifiée selon le Swiss-U.S. Data Privacy Framework.

Si le pays de destination ne se trouve pas dans cette liste, un transfert à l'étranger est possible à d'autres conditions, notamment si des clauses contractuelles types sont mises en place avec le destinataire des données personnelles.

Par ailleurs, si les données personnelles dont le transfert est envisagé constituent du matériel biologique ou des données génétiques au sens de la Loi fédérale relative à la recherche sur l’être humain, le transfert à l'étranger nécessite le consentement éclairé de la personne concernée.

Enfin, précisons que le chercheur ou la chercheuse doit aussi vérifier s'il·elle a le droit de communiquer les données à un tiers (ou, si le·la destinataire intervient comme sous-traitant, il·elle doit s'assurer d'avoir un contrat de sous-traitance qui inclut également la protection du secret de fonction).

Le chercheur ou la chercheuse qui ne respecte pas ces règles risque (à titre personnel) principalement une sanction pénale (violation du secret de fonction) et disciplinaire, d'être tenu·e responsable en cas de dommage, ainsi que ne de plus pouvoir utiliser les données.

En outre, il faudra déterminer le rôle du destinataire (sous-traitant ou tiers) et les exigences qui en découlent, ainsi que respecter les règles en matière de communication (sur ces éléments, voir la Question / Frage 28).

Welche Bedingungen müssen erfüllt sein, um Personendaten ausserhalb der Schweiz (bspw. auf die österreichische Plattform Pangaea für Geowissenschaften) und vor allem ausserhalb der EU zu übermitteln?

Das Bundesgesetz über den Datenschutz (das für die Eidgenössischen Hochschulen gilt) und die kantonalen Gesetze (die für die kantonalen Hochschulen (Universitäten, Fachhochschulen und Pädagogischen Hochschulen) gelten) enthalten spezifische Bestimmungen für die Bekanntgabe (oder Übermittlung) von Daten ins Ausland.

Grundsätzlich muss sichergestellt werden, dass das betreffende Land über eine Gesetzgebung verfügt, die ein angemessenes Schutzniveau gewährleistet. Anhang 1 der Verordnung über den Datenschutz enthält auf Bundesebene eine Liste dieser Staaten. Die Kantone verweisen in der Regel darauf. Im Falle der USA hat der Bundesrat am 14.08.2024 beschlossen, die USA ab dem 15.09.2024 in die Liste aufzunehmen mit der einschränkenden Ergänzung, dass Organisationen zertifiziert sein müssen; der Bundesrat geht somit davon aus,

dass im Falle eines Datenaustauschs mit einem US-Unternehmen ein angemessenes Schutzniveau gewährleistet ist, sofern das US-Unternehmen nach dem Swiss-U.S. Data Privacy Framework zertifiziert ist.

Ist das Zielland nicht in dieser Liste enthalten, ist eine Übermittlung ins Ausland unter anderen Bedingungen möglich, insbesondere wenn mit dem Empfänger der Personendaten Standardvertragsklauseln vereinbart werden.

Wenn es sich bei den Personendaten, deren Übermittlung geplant ist, um biologisches Material oder genetische Daten im Sinne des Bundesgesetzes über die Forschung am Menschen handelt, ist für die Übermittlung ins Ausland ausserdem eine informierte Einwilligung der betroffenen Person erforderlich.

Abschliessend sei noch erwähnt, dass Forschende zudem prüfen müssen, ob die Daten an Dritte überhaupt bekanntgegeben werden dürfen (oder, falls der Empfänger als Subunternehmer auftritt, sicherstellen müssen, dass ein Subunternehmervertrag existiert, der auch den Schutz des Amtsgeheimnisses beinhaltet).

Ein*e Forscher*in, der*die sich nicht an diese Vorgaben hält, riskiert (als Einzelperson) vor allem eine strafrechtliche Massnahme (durch die Verletzung des Amtsgeheimnisses), eine disziplinarische Sanktion und eine Haftung im Schadensfall, muss sich allfällig aber auch darauf einstellen, die Daten nicht mehr verwenden zu können.

Darüber hinaus müssen die Rolle des Empfängers (Subunternehmer oder Dritte) und die sich daraus ergebenden Anforderungen bestimmt sowie die Regeln für die Bekanntgabe eingehalten werden (zu diesen Themenkreisen siehe Question / Frage 28).

Question / Frage 17

Quels sont les risques juridiques qu'encourt un chercheur ou une chercheuse s'il·elle dépose son jeu de données (avec restrictions d’accès), sur une plateforme (data repository) américaine ?

Voir à ce sujet la Question / Frage 16.

Welche rechtlichen Risiken bestehen für Forschende, wenn sie einen Datensatz (mit Zugangsbeschränkungen) auf einer amerikanischen Plattform (Datenrepositorium) ablegen?

Siehe hierzu Question / Frage 16.

Question / Frage 18

Les solutions américaines de stockage telles que OneDrive, Teams sont-elles fiables pour stocker les données personnelles collectées dans le cadre de mes recherches ?

Voir à ce sujet la Question / Frage 16.

Sind amerikanische Speicherlösungen wie OneDrive, MS Teams sicher, um Personendaten zu speichern, die im Rahmen einer Forschungsarbeit gesammelt werden?

Siehe hierzu Question / Frage 16.

Question / Frage 19

Peut-on conseiller le dépôt de données de recherche suisse dans des dépôts étrangers ?

Voir à ce sujet la Question / Frage 16.

Kann die Ablage von Schweizer Forschungsdaten in ausländischen Repositorien empfohlen werden?

Siehe hierzu Question / Frage 16.

Question / Frage 20

À quelles conditions et avec quelles mesures de protection les données ORD (en particulier contenant des données personnelles) peuvent-elles être stockées voire traitées par des sous-traitants domiciliés dans un État dont la législation ne garantit pas un niveau de protection adéquat des données ?

En cas de sous-traitance, il faut s'assurer d'avoir un contrat de sous-traitance sur la protection des données personnelles qui inclut également la protection du secret de fonction.

Si le pays de destination n'est pas adéquat, un transfert à l'étranger est possible à d'autres conditions, notamment si des clauses contractuelles types sont mises en place avec le destinataire des données personnelles. Il convient de vérifier ces conditions dans la loi applicable (la Loi fédérale sur la protection des données (LPD) s'applique aux écoles fédérales et les lois cantonales s'appliquent aux hautes écoles cantonales (universités, hautes écoles spécialisées et hautes écoles pédagogiques)).

Par ailleurs, si les données personnelles dont le transfert est envisagé constituent du matériel biologique ou des données génétiques au sens de la Loi fédérale relative à la recherche sur l'être humain (LRH), le transfert à l'étranger nécessite le consentement éclairé de la personne concernée.

Unter welchen Bedingungen und mit welchen Datenschutzmassnahmen können ORD-Daten (insbesondere Personendaten) von Subunternehmen mit Sitz in einem Staat, dessen Gesetze kein angemessenes Datenschutzniveau gewährleisten, gespeichert oder bearbeitet werden?

Bei der Vergabe von Unteraufträgen muss sichergestellt werden, dass ein Vertrag mit dem Unterauftragnehmer zum Schutz der Personendaten vorliegt, der auch den Schutz des Amtsgeheimnisses beinhaltet.

Wenn das Zielland kein angemessenes Datenschutzniveau bietet, ist eine Übermittlung ins Ausland unter anderen Bedingungen möglich, namentlich wenn Standardvertragsklauseln mit dem Empfänger der Personendaten vereinbart werden. Diese Bedingungen sollten im anwendbaren Recht überprüft werden (das Bundesgesetz über den Datenschutz gilt für die Eidgenössischen Hochschulen und die kantonalen Gesetze gelten für die kantonalen Hochschulen (Universitäten, Fachhochschulen und Pädagogischen Hochschulen)).

Wenn es sich bei den Personendaten, deren Übermittlung geplant ist, um biologisches Material oder genetische Daten im Sinne des Bundesgesetzes über die Forschung am Menschen handelt, ist für die Übermittlung ins Ausland ausserdem eine informierte Einwilligung der betroffenen Person erforderlich.

Question / Frage 21

Comment permettre et faciliter le partage voire l'ouverture de données personnelles dans des projets de recherche réunissant des hautes écoles soumises à différentes législations (cantonales, suisse, européenne) en matière de protection des données personnelles ? Quid si certains partenaires de recherche ne sont pas situés dans un État garantissant un niveau adéquat de protection des données personnelles ?

Il faut trouver le régime juridique le plus strict qui s'applique à l'opération de traitement spécifique.

Pour les partenaires de recherche établis dans des pays tiers ne bénéficiant pas d'un niveau de protection adéquat, des clauses contractuelles types (SCC) ou des dispositions contractuelles appropriées peuvent être utilisées. Il convient toutefois de prendre en compte les risques : ces mesures sont parfois insuffisantes pour garantir une protection des données personnelles adéquate.

L'implication d'acteurs étrangers situés dans un pays qui n'offre pas le même niveau de protection que la Suisse peut nécessiter une décision au cas par cas sur la base du profil de risque des ensembles de données (l'utilisation du SCC [seulement pour les contrats], etc. peut être limitée si certaines catégories de données sont traitées ou si des exigences réglementaires existent).

Wie können der Austausch und die Offenlegung von Personendaten in Forschungsprojekten ermöglicht und erleichtert werden, wenn die teilnehmenden Hochschulen unterschiedlichen Rechtsvorschriften (kantonal, schweizerisch, europäisch) betreffend den Schutz von Personendaten unterliegen? Was, wenn einige Forschungspartner nicht in einem Staat ansässig sind, der ein angemessenes Datenschutzniveau gewährleistet?

Es muss die strengste Rechtsvorschrift gefunden werden, die für den spezifischen Bearbeitungsvorgang gilt.

Bei Forschungspartnern, die in Drittländern ohne angemessenem Datenschutzniveau ansässig sind, können Standardvertragsklauseln (SCC) oder geeignete Vertragsbestimmungen angewendet werden. Dabei sollten jedoch die Risiken berücksichtigt werden: Diese Massnahmen reichen teilweise nicht aus, um einen angemessenen Schutz der Personendaten zu gewährleisten.

Die Einbeziehung ausländischer Akteure, die sich in einem Land befinden, das nicht das gleiche Datenschutzniveau wie die Schweiz bietet, kann eine Einzelfallentscheidung auf der Grundlage des Risikoprofils der Datensätze erfordern (die Verwendung von SCC [nur für Verträge] usw. kann eingeschränkt sein, wenn bestimmte (sensible) Datenkategorien bearbeitet werden oder wenn regulatorische Anforderungen bestehen).

V. Obligations légales / Gesetzliche Verpflichtungen

Question / Frage 22

Qui a l'obligation de tenir un registre des activités de traitement (données personnelles) ?

Si une recherche est réalisée dans une école fédérale, la Loi fédérale sur la protection des données (LPD) s'applique et l'école, en tant qu'organe fédéral, a l'obligation de tenir un registre (interne).

Si une recherche est réalisée dans une haute école cantonale (université, haute école spécialisée ou haute école pédagogique), la loi sur la protection des données du canton concerné s'applique. Il convient alors de vérifier dans cette loi s'il existe une disposition sur la tenue d'un registre. Généralement, les législations cantonales n'imposent pas aux responsables de traitement de tenir un registre des activités de traitement, mais elles doivent déclarer leurs traitements à l'autorité cantonale qui tient le registre.

La tenue d'un registre, respectivement la déclaration de fichiers à l'autorité est une activité qui est généralement centralisée dans l'institution. Il est donc conseillé de prendre contact avec le·la DPO de l'institution pour comprendre comment déclarer une activité de traitement.

Wer ist verpflichtet, ein Register der Bearbeitungstätigkeiten (zu Personendaten) zu führen?

Wird Forschung an einer Eidgenössischen Hochschule durchgeführt, gilt das Bundesgesetz über den Datenschutz und die Hochschule ist als Bundesorgan verpflichtet, ein (internes) Register zu führen.

Wird Forschung an einer kantonalen Hochschule (Universität, Fachhochschule oder Pädagogischen Hochschule) durchgeführt, gilt das Datenschutzgesetz des jeweiligen Kantons. Es muss dann geprüft werden, ob es in diesem Gesetz eine Bestimmung zur Führung eines Registers gibt. Im Allgemeinen schreiben die kantonalen Datenschutzgesetze den für die Bearbeitung Verantwortlichen nicht vor, ein Register der Bearbeitungstätigkeiten zu führen, stattdessen müssen sie ihre Bearbeitungen bei der kantonalen Behörde melden, die das Register führt.

Das Führen eines Registers bzw. die Anmeldung von Datensammlungen bei der zuständigen Behörde ist eine Tätigkeit, die in der Regel zentral seitens der Universität oder Hochschule erfolgt. Es ist daher ratsam, sich mit dem Data Protection Officer (DPO) der Universität oder Hochschule in Verbindung zu setzen, um zu erfahren, wie eine Bearbeitungstätigkeit angemeldet werden soll.

Question / Frage 23

Dans quel cas un chercheur ou une chercheuse doit-il·elle mener une analyse d'impact en matière de protection des données (AIPD) ?

Les conditions auxquelles une analyse d'impact est requise sont définies dans les lois (cantonales/fédérales) applicables aux hautes écoles et aux universités (cantonales/fédérales).

Le principe directeur (selon la Loi fédérale sur la protection des données (LPD) et souvent repris dans les lois cantonales) est le suivant : une AIPD doit être effectuée lorsqu'un traitement est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. S'agissant de savoir quand un risque élevé existe, voir Question / Frage 24.

In welchen Fällen müssen Forschende eine Datenschutz-Folgenabschätzung (Risikoanalyse) durchführen?

Die Bedingungen, unter denen eine Datenschutz-Folgenabschätzung (DSFA) erforderlich ist, sind in den Gesetzen (kantonal/eidgenössisch) festgelegt, die für die Hochschulen und Universitäten gelten.

Der wichtigste Grundsatz (nach dem Bundesgesetz über den Datenschutz und häufig in den kantonalen Gesetzen übernommen) lautet: Eine DSFA muss durchgeführt werden, wenn eine Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann. Zur Frage, wann ein hohes Risiko besteht, siehe Question / Frage 24).

Question / Frage 24

Quels critères permettent de déterminer s'il y a traitement de données personnelles à risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée dans le cadre de recherches académiques ? Des exemples concrets pourraient être utiles

L'existence d'un risque élevé lors d'un traitement de données personnelles entraîne en particulier l'obligation de procéder à une analyse d'impact selon la LPD et certaines lois cantonales. La Loi fédérale sur la protection des données (LPD) indique qu'un risque élevé existe notamment en cas (i) de traitement de données sensibles à grande échelle ou (ii) de surveillance systématique de grandes parties du domaine public.

Un risque élevé peut également résulter d'autres circonstances. Si deux des neuf critères suivants sont réunis, un risque élevé devra généralement être retenu :

- (1) lorsqu'une évaluation ou une appréciation est effectuée,
- (2) prise de décision automatisée avec effet juridique ou effet similaire significatif,
- (3) surveillance systématique,
- (4) données sensibles ou données à caractère hautement personnel,
- (5) données traitées à grande échelle,
- (6) croisement ou combinaison d'ensembles de données,
- (7) données concernant des personnes vulnérables,
- (8) utilisation innovante ou application de nouvelles solutions technologiques ou organisationnelles,
- (9) traitement qui empêche les personnes concernées d'exercer un droit ou de bénéficier d'un service ou d'un contrat.

Anhand welcher Kriterien lässt sich feststellen, ob bei Forschungsarbeiten die Bearbeitung von Personendaten ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann? Konkrete Beispiele könnten hilfreich sein

Das Vorliegen eines hohen Risikos bei der Bearbeitung von Personendaten führt zur Pflicht, eine Datenschutz-Folgenabschätzung gemäss Bundesgesetz über den Datenschutz bzw. allfällig gemäss kantonalen Gesetzen durchzuführen. Das Bundesgesetz über den Datenschutz besagt, dass ein hohes Risiko insbesondere dann besteht, wenn (i) besonders schützenswerte Personendaten in grossem Umfang bearbeitet werden oder (ii) systematisch umfangreiche öffentliche Bereiche überwacht werden.

Ein hohes Risiko kann sich auch aus anderen Umständen ergeben. Wenn zwei der folgenden neun Kriterien zutreffen, sollte generell von einem hohen Risiko ausgegangen werden:

- (1) wenn eine Beurteilung oder Bewertung erfolgt,
- (2) bei einer automatisierten Entscheidungsfindung mit rechtlicher Wirkung oder erheblicher ähnlicher Wirkung,
- (3) bei einer systematischen Überwachung,
- (4) wenn besonders schützenswerte Personendaten oder höchstpersönliche Personendaten bearbeitet werden,
- (5) wenn in grossem Umfang Personendaten bearbeitet werden,
- (6) bei der Verknüpfung oder Kombination von Datensätzen,
- (7) wenn Personendaten zu schutzbedürftigen Personen bearbeitet werden,

- (8) bei Verwendung neuer Technologien oder Anwendung neuer technologischer oder organisatorischer Lösungen
- (9) wenn eine Bearbeitung vorliegt, welche die betroffenen Personen daran hindert, ein Recht auszuüben oder eine Dienstleistung oder einen Vertrag in Anspruch zu nehmen.

Question / Frage 25

Quelles sont les obligations concrètes des hautes écoles en matière de sécurité des données ? Quels sont les moyens à mettre en œuvre ? Quels sont les résultats/objectifs à atteindre ?

Les hautes écoles et universités suisses sont soumises à une obligation de prendre des mesures de sécurité pour protéger les données personnelles en vertu de la loi. L'art. 3 de l'Ordonnance sur la protection des données (OPDo) et l'art. 5 de l'Ordonnance relative à la recherche sur l'être humain (ORH) indiquent les types de mesures à prendre. La législation n'impose toutefois aucune mesure concrète.

Pour des exemples pratiques, il est possible de se référer au « Guide relatif aux mesures techniques et organisationnelles de la protection des données (TOM) » élaboré par le Préposé fédéral à la protection des données et à la transparence (PFPDT) (disponible sur https://www.edoeb.admin.ch/dam/edoeb/fr/Dokumente/datenschutz/leitfaden_tom.pdf.download.pdf/TOM_FR.pdf).

Welche konkreten Pflichten haben Hochschulen im Hinblick auf den Datenschutz? Welche Mittel sind einzusetzen? Welche Ergebnisse/Ziele sind zu erreichen?

Die Schweizer Hochschulen und Universitäten sind gesetzlich verpflichtet, Sicherheitsmassnahmen zum Schutz von Personendaten zu ergreifen. Art. 3 Datenschutzverordnung und Art. 5 Humanforschungsverordnung geben an, welche Arten von Massnahmen zu ergreifen sind. Das Gesetz schreibt jedoch keine konkreten Handlungen vor.

Für praktische Beispiele kann der vom Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten erstellte «Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes (TOM)» herangezogen werden (abrufbar unter https://www.edoeb.admin.ch/dam/edoeb/fr/Dokumente/datenschutz/leitfaden_tom.pdf.download.pdf/TOM_FR.pdf).

Question / Frage 26

Une université ou haute école peut-elle et doit-elle imposer ses standards à ses partenaires recevant des données de sa part ? Si oui, quels sont les critères concrets permettant d'évaluer la capacité des infrastructures partenaires à respecter ces standards ?

Pour répondre à cette question, deux aspects doivent être pris en compte :

- la qualification du partenaire concerné :
    - si celui-ci est un sous-traitant (ce qui est le cas, par exemple, si le partenaire fait uniquement du stockage de données), l'institution doit s'assurer, par le biais d'un contrat, que le sous-traitant respecte ses standards, notamment des mesures techniques et organisationnelles de sécurité minimales. Les standards peuvent aussi faire partie des instructions à destination du sous-traitant.
    - Si le partenaire est un tiers (par exemple une autre université ou haute école qui fait une utilisation propre des données personnelles), l'université n'est pas responsable des standards appliqués par ce tiers. Elle doit évidemment mettre des conditions pour la protection des données personnelles avant de communiquer des données.

    - Finalement si c'est un traitement conjoint, les standards peuvent faire partie de l'accord de traitement conjoint.
- le lieu où se situe le partenaire : si le partenaire (qu'il soit un sous-traitant ou un tiers) se situe dans un pays qui n'est pas considéré comme adéquat du point de vue de la protection des données (cf. liste figurant dans l'annexe 1 de l'Ordonnance sur la protection des données (OPDo)), des clauses contractuelles types doivent en principe être signées. Celles-ci contiennent des articles relatifs à la sécurité.

Kann und soll eine Universität oder Hochschule ihren Partnern, die Daten von ihr erhalten, ihre Standards vorschreiben? Wenn ja, anhand welcher konkreten Kriterien lässt sich beurteilen, ob die Partnerinfrastrukturen in der Lage sind, diese Standards einzuhalten?

Um diese Frage zu beantworten, müssen zwei Aspekte berücksichtigt werden:

- Die Einordnung des jeweiligen Partners:
    - Wenn es sich um einen Auftragsdatenbearbeiter (Auftragnehmer) handelt (was z. B. der Fall ist, wenn der Partner nur die Datenspeicherung vornimmt), muss die Hochschule durch einen Vertrag sicherstellen, dass der Auftragsdatenbearbeiter dieselben Standards wie die Hochschule, insbesondere technische und organisatorische Mindestsicherheitsmassnahmen, einhält. Diese Standards können auch Teil von konkreten Anweisungen an den Auftragsdatenbearbeiter sein.
    - Wenn der Partner ein Dritter ist (z. B. eine andere Universität oder Hochschule, welche die Personendaten eigenverantwortlich nutzt), ist die Hochschule nicht für die von diesem Dritten angewandten Standards verantwortlich. Sie muss aber natürlich Bedingungen zum weiteren Schutz der Personendaten stellen, bevor sie Daten bekanntgibt.
    - Wenn es sich um eine gemeinsame Bearbeitung handelt, können die Standards Teil der Vereinbarung über die gemeinsame Bearbeitung sein.
- Den Standort des Partners: Wenn der Partner (sei es ein Auftragsdatenbearbeiter oder ein Dritter) in einem Land ansässig ist, das aus Sicht des Datenschutzes nicht als angemessen gilt (siehe Liste in Anhang 1 der Datenschutzverordnung), müssen in der Regel Standardvertragsklauseln abgeschlossen werden. Diese enthalten sicherheitsrelevante Regelungen.

VI. Open research data (ORD) et dépôt / Open Research Data (ORD) und Repositorien

Question / Frage 27

Peut-on déposer sur une plateforme des données personnelles en ORD pour leur réutilisation ?

Il convient d'abord de déterminer si les données peuvent être déposées sur une plateforme en ORD sous forme anonymisée. Si c'est envisageable, cette solution doit être préférée. Si une anonymisation n'est pas envisageable (par exemple en présence de données qualitatives ou d'interviews d'expert·e·s, pour lesquelles les personnes concernées sont importantes), il faut vérifier si le droit applicable permet la communication de données. Si oui, un dépôt est généralement possible aux conditions suivantes :

- Il doit y avoir le consentement du participant ou de la participante. Cela nécessite des informations complètes sur le traitement des données et la liberté pour le·la participant·e d'accepter ou non le dépôt.
- La publication doit déjà être planifiée et communiquée au moment où le consentement est demandé.
- L'infrastructure de publication (référentiel) doit être équipée de manière à pouvoir gérer un retrait de consentement.

Si les conditions ci-dessus ne peuvent être remplies, le dépôt dans un référentiel entraînera toujours un dépôt dans une archive à accès fermé (avec restrictions d'accès), à condition que le référentiel soit approuvé (en ce qui concerne la sécurité des données). Dans les cas les où la protection doit être plus stricte, seules les métadonnées peuvent être publiées.

À noter qu'il existe un risque de révocation du consentement, auquel les personnes concernées ont droit. Dans le cas de données déjà publiées, il n'est toutefois pas possible de garantir, en cas de révocation, que les données ne sont pas déjà utilisées et traitées par des tiers ; en outre, une révocation peut avoir pour conséquence que les dépenses engagées dans le cadre de la publication ont été vaines ; à cet égard, il convient de prévoir d'éventuelles demandes de dommages et intérêts dès l'information relative à l'obtention du consentement.

Si le partage implique un transfert à l'étranger de données personnelles (par exemple si le fournisseur du dépôt se trouve à l'étranger, si les données sont physiquement stockées à l'étranger ou si un téléchargement depuis l'étranger est possible), les règles sur le transfert à l'étranger doivent être respectées (sur cette problématique, voir Question / Frage 16).

En outre, si un dépôt sur une plateforme en ORD de données personnelles (donc non anonymisées) sensibles est prévu, une analyse d'impact est recommandée.

Enfin, pour ce qui est de la réutilisation de matériel biologique, de données génétiques ou de données liées à la santé, voir Question / Frage 29 et Question / Frage 58.

Kann man in einem Repositorium Personendaten als ORD zur Weiternutzung ablegen?

Zunächst muss geprüft werden, ob die Daten in anonymisierter Form auf einer ORD-Plattform abgelegt werden können. Wenn dies denkbar ist, sollte diese Lösung bevorzugt werden.

Wenn eine Anonymisierung nicht in Frage kommt (z. B. bei qualitativen Daten oder Experteninterviews, bei denen die betroffenen Personen relevant sind), muss geprüft werden, ob das anzuwendende Recht eine Ablage mit Klardaten erlaubt. Wenn dies grundsätzlich möglich ist, kann eine Ablage in der Regel unter folgenden Bedingungen erfolgen:

- Es muss eine Einwilligung der betroffenen Person vorliegen. Diese erfordert, dass umfassend über die Datenbearbeitung informiert wurde und die betroffene Person frei war, der Datenablage zuzustimmen oder sie abzulehnen.
- Die Veröffentlichung der Daten muss zu dem Zeitpunkt, zu dem die Einwilligung eingeholt wird, bereits geplant und der betroffenen Person mitgeteilt worden sein.

- Die Infrastruktur für die Veröffentlichung (Repository) muss so ausgestattet sein, dass sie mit einem Widerruf der Einwilligung umgehen kann.

Wenn die oben genannten Bedingungen nicht erfüllt werden können, muss die Ablage in einem Repositorium einen geschlossenen Zugang (mit Zugangsbeschränkungen) nach sich ziehen – vorausgesetzt, das Repositorium bietet auch sonst einen angemessenen Schutz (im Hinblick auf die Datensicherheit). In Fällen, in denen der Schutzbedarf der abzulegenden Daten höher als derjenige ist, der im Repositorium angeboten ist, können nur Metadaten veröffentlicht werden.

Zu beachten gilt, dass bei einer Ablage von Personendaten in einem Repositorium das Risiko besteht, dass die Einwilligung widerrufen wird, wozu die betroffenen Personen berechtigt sind. Bei bereits veröffentlichten Daten kann im Falle eines Widerrufs indes nicht sichergestellt werden, dass diese Daten nicht bereits von Dritten verwendet und bearbeitet werden. Darüber hinaus kann ein Widerruf dazu führen, dass die im Rahmen der Veröffentlichung getätigten Aufwendungen vergeblich waren; in diesem Zusammenhang bietet es sich an, mögliche Schadensersatzansprüche bereits bei Einholung der Einwilligung im Rahmen der Information vorzusehen.

Wenn die Datenfreigabe eine Übertragung von Personendaten ins Ausland impliziert (z. B. wenn sich der Anbieter der Datenablage im Ausland befindet, oder wenn die Daten physisch im Ausland gespeichert werden oder wenn ein Download aus dem Ausland möglich ist), müssen die Regeln für die Datenübertragung ins Ausland beachtet werden (zu dieser Problematik siehe Question / Frage 16).

Wenn eine Datenablage von besonders schützenswerten Personendaten (die also nicht anonymisiert sind) auf einer ORD-Plattform geplant ist, wird darüber hinaus eine Datenschutzfolgenabschätzung empfohlen.

Was schliesslich die Weiterverwendung von biologischem Material, genetischen Daten oder Gesundheitsdaten betrifft, siehe Question / Frage 29 und Question / Frage 58.

Question / Frage 28

Quelles sont les conditions à remplir pour que des données personnelles ou confidentielles puissent être partagées dans des dépôts ?

La réponse à cette question dépend des circonstances et il n'y a pas de règles absolues à appliquer. Les éléments ci-dessous sont donc des recommandations générales.

- Le rôle du dépôt doit être déterminé. Il peut s'agir d'un dépôt interne ou d'un dépôt fourni par un sous-traitant (auquel cas un contrat doit être conclu, incluant des clauses sur le secret de fonction) ou par un tiers (auquel cas le consentement des personnes concernées est nécessaire). Dans tous les cas, dans la mesure où le partage de données va impliquer une communication à des tiers, les règles relatives à la communication de données contenues dans les lois applicables (la Loi fédérale sur la protection des données (LPD) pour les écoles fédérales et les lois cantonales pour les hautes écoles cantonales (universités, hautes écoles spécialisées et hautes écoles pédagogiques)) doivent être respectées.
- Il convient de déterminer si les données peuvent être déposées sous forme anonymisée. Si c'est envisageable, cette solution doit être préférée (sur cette problématique, voir Question / Frage 63). Si une anonymisation des données n'est pas possible (par exemple en présence de données qualitatives ou d'interviews d'expert·e·s, pour lesquelles les personnes concernées sont importantes), le dépôt n'est admissible qu'avec le consentement des personnes concernées. Dans ce cas, il existe un risque de révocation du consentement, auquel les personnes concernées ont droit. Dans le cas de données déjà publiées, il n'est toutefois pas possible de garantir, en cas de révocation, que les données ne sont pas déjà utilisées et traitées par des tiers ; en outre, une révocation peut avoir pour conséquence que les dépenses engagées dans le cadre de la publication ont été vaines ; à cet égard, il convient de prévoir d'éventuelles demandes de dommages et intérêts dès l'information relative à l'obtention du consentement. Des solutions pour publier des données personnelles de manière non publique dans les dépôts sont parfois disponibles. Dans ce cas, les métadonnées ne contiennent que des indications sur la

présence de ces données. Sur demande et après vérification (de la légalité), les données personnelles peuvent être rendues accessibles. Les conditions préalables devraient être les suivantes : légitimité d'une consultation (par exemple à des fins de recherche), accord de confidentialité, utilisation ultérieure uniquement après autorisation préalable et accord sur le but et l'étendue de l'utilisation.

- Si le dépôt de données personnelles (donc non anonymisées) sensibles est prévu, une analyse d'impact est recommandée.

- Pour ce qui est de la réutilisation de matériel biologique, de données génétiques ou de données liées à la santé, voir Question / Frage 29 et Question / Frage 58.

- Si le partage implique un transfert à l'étranger de données personnelles (par exemple si le fournisseur du dépôt se trouve à l'étranger, si les données sont physiquement stockées à l'étranger ou si un téléchargement depuis l'étranger est possible), les règles sur le transfert à l'étranger doivent être respectées (sur cette problématique, voir Question / Frage 16).

- Le dépôt doit remplir des exigences de qualité fondamentales (p. ex. selon re3data.org) et respecter les mesures techniques et organisationnelles nécessaires pour déposer les données de manière sûre en fonction des besoins de protection. Il convient notamment de veiller aux possibilités de paramétrer les éléments suivants :

    - Différenciation en fonction du degré de confidentialité des données, avec des conséquences différentes en termes d'accessibilité ;

    - Droits et restrictions d'accès ;

    - Stockage de métadonnées accessibles au public pour les données de recherche confidentielles (notamment les données sensibles) ; l'accès aux données elles-mêmes ne devrait être autorisé qu'aux conditions suivantes : légitimité d'une consultation (par exemple à des fins de recherche), accord de confidentialité, utilisation ultérieure uniquement après autorisation préalable et accord sur le but et l'étendue de l'utilisation.

  Des contrats/réglementations appropriés doivent être mis en place concernant le dépôt de données lui-même et pour la réutilisation, si possible avec des approches « sur mesure ». En outre, les accès aux données doivent être traçables.

Welche Voraussetzungen müssen eingehalten werden, damit Personendaten oder vertrauliche Daten mittels Repositorien geteilt werden können?

- Die Funktion des Repositoriums muss bestimmt werden. Es kann sich bei diesem um eine internen Datenablage handeln oder aber um eine Datenablage, die von einem Auftragsdatenbearbeiter bereitgestellt wird (in diesem Fall muss ein Vertrag geschlossen werden, der unter anderem Klauseln zur Einhaltung des Amtsgeheimnisses enthält); oder es handelt sich um eine Datenablage, die von einem Dritten unterhalten wird (in diesem Fall ist die Einwilligung der betroffenen Personen erforderlich). In jedem Fall müssen die in den anwendbaren Gesetzen (das Bundesgesetz über den Datenschutz für die Eidgenössischen Hochschulen und die kantonalen Gesetze für die kantonalen Hochschulen (Universitäten, Fachhochschulen und Pädagogischen Hochschulen)) enthaltenen Regeln über die Bekanntgabe von Daten eingehalten werden, sofern die gemeinsame Nutzung von Daten eine Bekanntgabe an Dritte mit sich bringt.

- Es ist zu prüfen, ob die Daten in anonymisierter Form abgelegt werden können. Wenn dies möglich ist, sollte dieser Lösung der Vorzug gegeben werden (zu dieser Problematik siehe Question / Frage 63). Wenn eine Anonymisierung der Personendaten nicht in Frage kommt (z. B. bei qualitativen Daten oder Experteninterviews, bei denen die betroffenen Personen relevant sind), ist eine Ablage nur mit der Einwilligung der betroffenen Personen zulässig. In diesem Fall besteht das Risiko eines Widerrufs der Einwilligung, wozu die betroffenen Personen berechtigt. Bei bereits veröffentlichten Daten kann im Falle eines Widerrufs indes nicht sichergestellt werden, dass die Daten nicht bereits von Dritten verwendet

und bearbeitet werden; darüber hinaus kann ein Widerruf dazu führen, dass die im Rahmen der Veröffentlichung getätigten Aufwendungen vergeblich waren; in diesem Zusammenhang bietet es sich an, mögliche Schadensersatzansprüche bereits bei Einholung der Einwilligung im Rahmen der Information vorzusehen. Manchmal gibt es Lösungen, um Personendaten nicht-öffentlich in Repositorien abzulegen. In diesem Fall enthalten die Metadaten nur Hinweise auf das Vorhandensein dieser Daten. Auf Antrag und nach (Rechtmässigkeits-)Prüfung können diese Personendaten dann zugänglich gemacht werden. Voraussetzungen dafür sollten sein: Legitimation einer Abfrage (z. B. zu Forschungszwecken), Vertraulichkeitsvereinbarung, Absprache zur weiteren Nutzung nur nach vorheriger Genehmigung und Einigung über Zweck und Umfang der Nutzung.

- Wenn eine Datenablage von besonders schützenswerten Personendaten (also von nicht anonymisierten Daten) auf einer ORD-Plattform geplant ist, wird darüber hinaus eine Datenschutzfolgenabschätzung empfohlen.

- Zur Weiterverwendung von biologischem Material, genetischen Daten oder Gesundheitsdaten siehe Question / Frage 29 und Question / Frage 58.

- Wenn die Datenfreigabe eine Übertragung von Personendaten ins Ausland impliziert (z. B. wenn sich der Anbieter der Datenablage im Ausland befindet, oder wenn die Daten physisch im Ausland gespeichert werden oder wenn ein Download aus dem Ausland möglich ist), müssen die Vorschriften für die Datenübertragung ins Ausland beachtet werden (zu dieser Problematik siehe Question / Frage 16).

- Die Ablage muss grundlegende Qualitätsanforderungen (z. B. nach re3data.org) erfüllen und die technischen und organisatorischen Massnahmen anwenden, die notwendig sind, um die Daten entsprechend ihren Schutzbedürfnissen sicher abzulegen. Dabei ist insbesondere auf folgende Einstellungsmöglichkeiten zu achten:

    - Differenzierung nach dem Grad der Vertraulichkeit der Daten, mit unterschiedlichen Konsequenzen für die Zugänglichkeit;

    - Zugriffsrechte und -beschränkungen;

    - Öffentlich zugängliche Speicherung von Metadaten für vertrauliche Forschungsdaten (insbesondere besonders schützenswerte Personendaten); der Zugang zu den Daten selbst sollte nur unter folgenden Bedingungen gestattet werden: Legitimation einer Abfrage (z. B. zu Forschungszwecken), Vertraulichkeitsvereinbarung, Absprache zur weiteren Nutzung nur nach vorheriger Genehmigung und Einigung über Zweck und Umfang der Nutzung.

  Es müssen geeignete Verträge/Regelungen bezüglich der Datenablage selbst und für die Weiterverwendung geschaffen werden, möglichst mit „massgeschneiderten“ Ansätzen. Darüber hinaus muss der Zugriff auf die Daten rückverfolgbar sein.

Question / Frage 29

Dans le cadre de recherches académiques, peut-on réutiliser des données personnelles de santé sans le consentement des personnes concernées ?

En vertu du privilège de la recherche, les hautes écoles et universités suisses peuvent traiter des données personnelles à des fins de recherche à des conditions plus souples. Dans ce contexte, le consentement n'est généralement pas nécessaire pour réutiliser les données personnelles, même si elles sont sensibles (ce qui est le cas des données personnelles de santé). Il convient de noter que le privilège de la recherche n'est pas conçu de la même manière dans toutes les lois sur la protection des données ; il faut tenir compte des particularités.

Si la recherche est soumise à la Loi fédérale relative à la recherche sur l’être humain (LRH) (ce qui est le cas lorsqu’elle porte sur les maladies humaines ou sur la structure et le fonctionnement du corps humain, et qu’elle est pratiquée sur des personnes, des personnes décédées, des embryons et des fœtus, du matériel biologique ou

des données personnelles liées à la santé), les art. 32 et suivants déterminent les conditions auxquelles des données de santé peuvent être réutilisées. Ils prévoient des règles qui permettent, à certaines conditions, de réutiliser des données personnelles de santé collectées dans un autre contexte que celui de la recherche envisagée (p. ex. des données collectées dans un hôpital ou dans le cadre d'une autre recherche). Ces règles priment les règles des lois de protection des données prévoyant des privilèges de recherche.

En principe, si les données personnelles de santé ne sont pas codées, un consentement éclairé est nécessaire pour la réutilisation (art. 32 et 33 LRH). La réutilisation est exceptionnellement possible sans consentement si les conditions suivantes sont remplies de manière cumulative (art. 34 et 45 al. 1 let. b LRH) :

1) l'obtention du consentement ou l'information sur le droit d'opposition est impossible ou pose des difficultés disproportionnées, ou on ne peut raisonnablement l'exiger de la personne concernée ;
2) aucun document n'atteste un refus de la personne concernée ;
3) l'intérêt de la science prime celui de la personne concernée à décider de la réutilisation de son matériel biologique ou de ses données ;
4) la commission d'éthique compétente a donné son autorisation.

Können im Rahmen der Forschung erhobene Gesundheitsdaten ohne die Einwilligung der betroffenen Personen weiterverwendet werden?

Aufgrund des Forschungsprivilegs können Schweizer Hochschulen und Universitäten Personendaten zu Forschungszwecken unter erleichterten Bedingungen bearbeiten. In diesem Zusammenhang ist daher in der Regel keine Einwilligung erforderlich, um Personendaten weiterzuverwenden, selbst wenn es sich um besonders schützenswerte Personendaten handelt (was bei personenbezogenen Gesundheitsdaten der Fall ist). Es ist zu beachten, dass das Forschungsprivileg nicht in allen Datenschutzgesetzen gleich ausgestaltet ist; die Besonderheiten müssen berücksichtigt werden.

Wenn die Forschung dem Humanforschungsgesetzes (HFG) unterliegt (was der Fall ist, wenn sie menschliche Krankheiten oder den Aufbau und die Funktionsweise des menschlichen Körpers zum Gegenstand hat und mit Personen, verstorbenen Personen, Embryonen und Föten, biologischem Material oder gesundheitsbezogenen Personendaten durchgeführt wird), legen Art. 32 ff. fest, unter welchen Bedingungen Gesundheitsdaten weiterverwendet werden dürfen. Die Artikel enthalten zudem Regelungen, die unter bestimmten Voraussetzungen die Weiterverwendung von Gesundheitsdaten erlauben, die in einem anderen Kontext als dem der geplanten Forschung erhoben wurden (z.B. Daten, die in einem Spital oder im Rahmen einer anderen Forschung erhoben wurden). Diese Regeln haben Vorrang vor den Regeln der Datenschutzgesetze, die Forschungsprivilegien vorsehen.

Grundsätzlich gilt: Wenn die Gesundheitsdaten nicht verschlüsselt sind, ist für die Weiterverwendung eine Einwilligung nach Aufklärung erforderlich (Art. 32 und 33 HFG). Die Weiterverwendung ist ausnahmsweise ohne Einwilligung möglich, wenn die folgenden Bedingungen kumulativ erfüllt sind (Art. 34 und 45 Abs. 1 Bst. b HFG):

1) Die Einholung der Einwilligung oder die Information über das Widerspruchsrecht ist unmöglich oder mit unverhältnismässigen Schwierigkeiten verbunden oder kann von der betroffenen Person vernünftigerweise nicht erfragt werden;
2) es gibt keine Unterlagen, die eine Ablehnung der betroffenen Person belegen;
3) das Interesse der Forschung überwieg gegenüber dem Interesse der betroffenen Person, über die Weiterverwendung ihres biologischen Materials oder ihrer Daten zu bestimmen;
4) die zuständige Ethikkommission hat ihre Zustimmung erteilt.

Question / Frage 30

Puis-je partager mes données dans n'importe quel dépôt ?

Voir à ce sujet la Question / Frage 27.

Kann ich meine Daten in jedem Repositorium zugänglich machen?

Siehe hierzu Question / Frage 27.

Question / Frage 31

Comment préparer les données (en particulier leur désignation) pour les partager dans un dépôt en étant conforme aux exigences légales ?

L'EPFL a publié un guide sur la gestion des données de recherche, qui donne (notamment) des indications sur la manière de préparer les données en vue de les conserver dans un dépôt (https://zenodo.org/records/3327830#.Y9eLyy9XaZB) et qui expose quelques principes juridiques à respecter.

Wie bereitet man Daten (insbesondere ihre Bezeichnung) für die Freigabe in einem Repositorium auf und erfüllt dabei die rechtlichen Anforderungen?

Die EPFL hat einen Leitfaden zur Verwaltung von Forschungsdaten veröffentlicht, der (unter anderem) Hinweise zur Aufbereitung von Daten für die Aufbewahrung in einem Repositorium gibt und einige rechtliche Grundsätze erläutert, die es zu beachten gilt, siehe https://zenodo.org/records/3327830#.Y9eLyy9XaZB.

Question / Frage 32

Existe-t-il des règles ou des recommandations sur le moment où les données doivent être déposées (par exemple par rapport au déroulement d'un projet ou d'une thèse) ?

Il n'existe pas de dispositions légales relatives à l'obligation de dépôt ou à la date de ce dépôt. Dans le cadre d'une stratégie de science ouverte, le dépôt doit être effectué lorsque les données sont importantes pour la traçabilité/vérification des résultats de la recherche. En règle générale, cela doit être fait dès que les données ont été utilisées pour une publication ou à la fin d'un projet.

Gibt es Regeln oder Empfehlungen, wann Daten (in einem Repositorium) abgelegt werden sollten (z. B. in Bezug auf den Verlauf eines Projekts oder einer Dissertation)?

Es gibt keine gesetzlichen Bestimmungen dazu, ob oder wann eine Ablage erfolgen muss. Im Rahmen einer Open-Science-Strategie sollte die Ablage erfolgen, wenn die Daten für die Nachvollziehbarkeit/Überprüfung der Forschungsergebnisse gebraucht werden. Dies ist in der Regel der Fall, sobald die Daten im Rahmen einer Veröffentlichung verwendet wurden oder am Ende eines Projekts.

Question / Frage 33

À quoi les chercheurs et chercheuses doivent-ils faire attention lors du choix des dépôts, en particulier s'ils veulent déposer des données personnelles (sensibles) ?

Voir à ce sujet la Question / Frage 27 et la Question / Frage 28.

Worauf sollten Forschende bei der Wahl von Repositorien achten, insbesondere, wenn sie (besonders schützenswerte) Personendaten ablegen wollen?

Siehe hierzu Question / Frage 27 und Question / Frage 28.

Question / Frage 34

À quoi peut ressembler une grille d'évaluation pour déterminer si une mise à disposition du public est appropriée ?

Il s'agit ici de mettre à disposition un outil permettant aux chercheurs/chercheuses d'évaluer si leurs jeux de données se prêtent à l'ORD dans des conditions définies.

Une grille d'évaluation permettant de déterminer si les données sont appropriées pour être mises à la disposition du public devrait tenir compte des aspects suivants :

- Aspects juridiques : Protection des données et droits de la personnalité, consentement à la publication, anonymisation ou pseudonymisation, droits d'auteur et de propriété, ainsi que restrictions contractuelles éventuelles.
- Aspects scientifiques : Reproductibilité et réutilisation des données, prise en compte des principes FAIR (Findable, Accessible, Interoperable, Reusable), et qualité et cohérence des données.
- Aspects techniques : Utilisation de formats de données ouverts et courants, de normes de métadonnées pour garantir la facilité de recherche et de compréhension, ainsi que de lieux de stockage et d'infrastructures appropriés pour l'archivage à long terme.
- Aspects financiers et de ressources : Préservation à long terme des données, mise à disposition des ressources et du financement nécessaires pour la curation et l'accès.

Wie kann ein Beurteilungsraster aussehen, zur Feststellung der Eignung für eine öffentlichen Zugänglichmachung?

Es geht hier um die Zurverfügungstellung eines Werkzeugs, anhand dessen Forscher beurteilen können, ob ihre Datensätze unter definierten Bedingungen für ORD geeignet sind.

Ein Bewertungsschema zur Feststellung, ob Daten geeignet sind, der Öffentlichkeit zugänglich gemacht zu werden, sollte die folgenden Aspekte berücksichtigen:

- Rechtliche Aspekte: Datenschutz und Persönlichkeitsrechte, Einwilligung zur Veröffentlichung, Anonymisierung oder Pseudonymisierung, Urheber- und Eigentumsrechte sowie mögliche vertragliche Einschränkungen.
- Wissenschaftliche Aspekte: Reproduzierbarkeit und Wiederverwendung von Daten, Berücksichtigung der FAIR-Prinzipien (Findable, Accessible, Interoperable, Reusable) sowie Qualität und Kohärenz der Daten.
- Technische Aspekte: Verwendung von offenen und gängigen Datenformaten, Metadatenstandards zur Gewährleistung der leichten Auffindbarkeit und Verständlichkeit sowie geeignete Speicherorte und Infrastrukturen für die Langzeitarchivierung.
- Finanzielle und ressourcenbezogene Aspekte: Langfristige Erhaltung der Daten, Bereitstellung der notwendigen Ressourcen und Finanzierung für Pflege und Zugang.

Question / Frage 35

Comment s'assurer que les jeux de données prévus pour l'ORD soient préparés de manière à être facilement réutilisables ? Ce faisant, ils ne devraient pas être modifiés par des exigences légales de manière à réduire ou à fausser leur contenu informatif.

La réutilisabilité des jeux de données prévus pour l'ORD peut être assurée par :

- Le suivi des normes et les guides éprouvés (par exemple le guide ORD de la bibliothèque universitaire de l'EPFL, https://zenodo.org/records/3327830#.Y9eLyy9XaZB).
- L'utilisation de listes de contrôle et des grilles d'évaluation (voir Question / Frage 34) pour garantir que les données sont bien documentées, disponibles dans des formats appropriés et préparées selon les principes FAIR (Findable, Accessible, Interoperable, Reusable).

- L'utilisation d'un plan de gestion des données (DMP) : un DMP est obligatoire pour les projets, notamment ceux du FNS, et aide à prendre en compte les exigences de réutilisabilité tout au long du processus de recherche.
- La mise à disposition de personnel qualifié et des ressources suffisantes pour répondre aux exigences spécifiques de la discipline et de la méthodologie concernées.

Wie kann man sicherstellen, dass für ORD vorgesehene Datensätze so aufbereitet werden, dass sie leicht wiederverwendbar sind? Dabei sollten sie nicht durch rechtliche Vorgaben so verändert werden, dass ihr Informationsgehalt reduziert oder verfälscht wird.

Die Wiederverwendbarkeit der für ORD vorgesehenen Datensätze kann sichergestellt werden durch:

- Die Einhaltung von Standards und bewährten Leitfäden (z.B. durch den ORD-Leitfaden der Universitätsbibliothek der EPFL, https://zenodo.org/records/3327830#.Y9eLyy9XaZB.
- Die Verwendung von Checklisten und Bewertungsrastern (siehe Question / Frage 34), um sicherzustellen, dass die Daten gut dokumentiert, in geeigneten Formaten verfügbar und nach den FAIR-Prinzipien (Findable, Accessible, Interoperable, Reusable) aufbereitet sind.
- Die Verwendung eines Datenmanagementplans (DMP): Ein DMP ist für Projekte, insbesondere für SNF-Projekte, obligatorisch und hilft, die Anforderungen an die Wiederverwendbarkeit während des gesamten Forschungsprozesses zu berücksichtigen.
- Die Bereitstellung von qualifiziertem Personal und ausreichenden Ressourcen, um die spezifischen Anforderungen des jeweiligen Fachgebiets und der jeweiligen Methodik zu erfüllen.

Question / Frage 36

À quelles données précises se réfère l'expression « données de recherche ouvertes » ? En d'autres termes, quelles données de recherche doivent être rendues publiques ?

Le terme « données de recherche ouvertes » se réfère à toutes les données rendues publiquement accessibles et qui sont à la base d'une publication, d'une recherche, ou qui sont nécessaires à la compréhension et à la traçabilité des résultats d'un projet.

Il ne s'agit généralement pas d'une obligation légale mais d'un principe devant favoriser la recherche scientifique. Il est en revanche souvent imposé contractuellement par les bailleurs de fonds. Cela comprend notamment les données issues de la recherche financée par des fonds publics, qui sont nécessaires à la reproduction et à la réutilisation des résultats de la recherche, ainsi que les données d'intérêt général. Si des restrictions juridiques (p. ex. protection des données, droits d'auteur) rendent impossible la publication des données de recherche, les métadonnées doivent au moins être rendues accessibles afin de garantir la possibilité de trouver et de suivre la recherche. Le principe « aussi ouvert que possible, aussi protégé que nécessaire » s'applique ici. Les différences disciplinaires doivent être prises en compte, en particulier dans les domaines où la définition de « données » est interprétée différemment.

Welche Daten sind vom Verständnis «offene Forschungsdaten» umfasst? Mit anderen Worten: Welche Forschungsdaten sollen offengelegt werden?

Der Begriff «offene Forschungsdaten» bezieht sich auf alle Daten, die öffentlich zugänglich gemacht werden; sie bilden die Grundlage einer Veröffentlichung oder einer Forschungsarbeit oder sind für das Verständnis und die Nachvollziehbarkeit von Projektergebnissen erforderlich.

Bei der Offenlegung handelt es sich in der Regel nicht um eine gesetzliche Verpflichtung, sondern um einen Grundsatz, der die wissenschaftliche Forschung fördern soll. Gleichzeitig wird eine Offenlegung häufig von den Geldgebern vertraglich vorgeschrieben. Dazu gehören insbesondere Daten aus öffentlich finanzierter Forschung, die für die Reproduktion und Weiterverwendung von Forschungsergebnissen erforderlich sind, sowie Daten von allgemeinem Interesse. Wenn rechtliche Einschränkungen (z. B. Datenschutz, Urheberrecht) die Veröffentlichung

von Forschungsdaten unmöglich machen, müssen zumindest die Metadaten zugänglich gemacht werden, um die Auffindbarkeit und Nachvollziehbarkeit der Forschung zu gewährleisten. Hier gilt der Grundsatz „so offen wie möglich, so geschützt wie nötig“. Unterschiede in den verschiedenen Forschungsgebieten müssen berücksichtigt werden, insbesondere in Bereichen, in denen sich die Definition von «Daten» unterscheidet.

Question / Frage 37

Comment les données personnelles doivent-elles être traitées dans le cadre de l'ORD si ces données personnelles ne peuvent pas être anonymisées, par exemple parce qu'il s'agit d'une interview d'expert·e ?

Il est tout à fait possible de rendre publiques des données personnelles en ORD si les conditions légales applicables à la communication de données personnelles sont respectées et si les exigences suivantes sont remplies :

- Il doit y avoir le consentement valable du participant ou de la participante. Cela nécessite des informations complètes sur le traitement des données prévu et la liberté pour le·la participant·e d'accepter ou non le dépôt ainsi qu'une référence au droit de rétractation de retirer son consentement.
- En particulier, la publication doit déjà être planifiée et communiquée au moment où le consentement est demandé.
- L'infrastructure de publication (référentiel) doit être équipée de manière à pouvoir gérer un retrait de consentement et permettre d'effectuer des contrôles d'accès.

Si les conditions ci-dessus ne peuvent être remplies, le dépôt dans un référentiel entraînera toujours un dépôt dans une archive à accès fermé (avec restrictions d'accès). Dans les cas où la protection doit être plus stricte, seules les métadonnées peuvent être publiées.

En cas de consentement, il existe un risque de révocation du consentement. Dans le cas de données déjà publiées, il n'est généralement pas possible de garantir qu'en cas de révocation, les données n'ont pas déjà été utilisées et traitées ultérieurement par des tiers ; ce risque doit également être signalé lors du consentement. En fin de compte, toute dépense déjà engagée pour la publication sera vaine après une révocation. Dans ce contexte, il convient d’envisager d’inclure d’éventuelles demandes de dommages-intérêts dans les informations relatives à l’obtention du consentement.

Wie wird mit Personendaten im Zusammenhang mit ORD umgegangen, wenn diese Personendaten nicht anonymisiert werden können, bspw. weil es sich um ein Experteninterview handelt?

Es ist durchaus möglich, Personendaten als ORD zu veröffentlichen, wenn die rechtlichen Bedingungen für die Bekanntgabe von Personendaten eingehalten werden und die folgenden Anforderungen erfüllt sind:

- Es muss eine wirksame Einwilligung der betroffenen Person vorliegen. Dies erfordert eine umfassende Information über die geplante Datenbearbeitung und die Freiwilligkeit der betroffenen Person hinsichtlich der Zustimmung oder Ablehnung dieser Veröffentlichung als ORD; zudem ist Hinweis auf das Recht, die Einwilligung zu widerrufen, notwendig.
- Die Veröffentlichung muss bereits zu dem Zeitpunkt geplant und mitgeteilt werden, zu dem die Einwilligung eingeholt wird.
- Die Infrastruktur für die Veröffentlichung (das Repositorium) muss so ausgestaltet sein, dass sie einen Widerruf der Einwilligung umsetzen kann und Zugriffskontrollen ermöglicht.

Wenn die oben genannten Bedingungen nicht erfüllt werden können, folgt daraus, dass eine Ablage in einem Repositorium nur mit geschlossenem Zugang (mit Zugangsbeschränkungen) erfolgen kann. In Fällen, in denen der Schutzbedarf höher ist, dürfen nur Metadaten veröffentlicht werden.

Im Falle einer Einwilligung besteht das Risiko, dass diese Einwilligung widerrufen wird. Bei bereits veröffentlichten Daten kann im Falle eines Widerrufs indes nicht sichergestellt werden, dass die Daten nicht bereits von Dritten verwendet und bearbeitet werden; auf dieses Risiko muss auch bei der Einwilligung hingewiesen werden. Letztendlich sind im Falle eines Widerrufs alle für die Veröffentlichung getätigten Aufwendungen vergeblich. In diesem Zusammenhang sollte erwogen werden, mögliche Schadensersatzansprüche bereits bei Einholung der Einwilligung im Rahmen der Information vorzusehen.

Question / Frage 38

Qui est responsable, au sens d'une loi sur la protection des données, de la fourniture de données (en particulier de données claires) dans le contexte ORD, si plusieurs chercheurs et chercheuses les utilisent ? S'agit-il d'un chercheur ou d'une chercheuse en personne (c'est lui·elle qui les a recueillies dans un but précis) ou est-ce les universités qui les emploient ? Comment peut-on le régler ?

Du point de vue juridique, la haute école ou l'université est responsable du traitement des données personnelles et donc responsable de respecter les règles en matière de protection des données et de la sécurité de l'information.

En pratique, l'institution doit veiller à ce que son personnel connaisse et applique les exigences légales dans ce domaine. Les chercheurs et chercheuses responsables d'un projet doivent s'assurer que leur recherche respecte la protection des données, en suivant notamment les éventuelles instructions ou lignes directrices de l'institution. De plus, les collaborateurs et collaboratrices sont soumis au secret de fonction à titre individuel.

En cas de partage de données personnelles avec une autre entité (p. ex. une autre institution), cette entité peut devenir responsable *conjoint* du traitement (p. ex. si un projet de recherche est géré en commun) ou responsable indépendant du traitement (p. ex. si elle réutilise des données pour un autre projet). L'institution qui communique les données reste néanmoins responsable des données qu'elle conserve. Dans tous les cas, il est préférable de clarifier les droits et obligations par contrat ou convention.

Wer ist im Sinne eines Datenschutzgesetzes verantwortlich bei Datenbereitstellung (insbesondere von Klardaten) im Kontext mit ORD, wenn diverse Forscher diese Daten nutzen? Ist es der*die Forscher*in persönlich (nachdem er*sie die Daten zu einem definierten Zweck erhoben hat) oder sind es die Hochschulen, bei denen der*die Forscher*in angestellt ist? Wie kann man dies regeln?

Aus rechtlicher Sicht ist die Hochschule oder Universität für die Bearbeitung von Personendaten verantwortlich und damit auch für die Einhaltung der Vorschriften zum Datenschutz und zur Informationssicherheit.

In der Praxis muss die Institution dafür sorgen, dass ihre Mitarbeitenden die gesetzlichen Anforderungen in diesem Bereich kennen und anwenden. Die für ein Projekt verantwortlichen Forscher*innen müssen sicherstellen, dass bei ihrer Forschung der Datenschutz eingehalten wird, indem sie insbesondere etwaige Anweisungen oder Richtlinien der Institution befolgen. Darüber hinaus unterliegen die Mitarbeitenden individuell dem Amtsgeheimnis.

Werden Personendaten mit einer anderen Stelle (z. B. einer anderen Institution) geteilt, kann diese Stelle zur gemeinsamen Verantwortlichen für die Datenbearbeitung werden (z. B. wenn ein Forschungsprojekt gemeinsam geleitet wird) oder die andere Stelle kann unabhängig zur Datenverantwortlichen für die Datenbearbeitung werden (z. B. wenn sie Daten für ein anderes Projekt weiterverwendet). Die Institution, welche die Daten bekanntgibt, bleibt jedoch für die von ihr bearbeiteten Daten verantwortlich.

In jedem Fall ist es sinnvoll, die Rechte und Pflichten durch einen Vertrag oder eine Vereinbarung klarzustellen.

Question / Frage 39

Sur la base de quels critères l'accès aux données doit-il être accordé à des tiers ? Peut-on déterminer/imposer ce que les utilisateurs et les utilisatrices ultérieurs sont autorisés à faire ? Et si oui, comment ?

S'agissant de la notion de données ouvertes, voir la réponse donnée à la Question / Frage 36.

Les règles relatives à la communication de données contenues dans les lois applicables (la Loi fédérale sur la protection des données (LPD) pour les écoles fédérales et les lois cantonales pour les hautes écoles cantonales (universités, hautes écoles spécialisées et hautes écoles pédagogiques)) doivent être respectées dans un tel cas. En vertu du privilège de la recherche – en principe prévu par les lois applicables – le principe de finalité ne trouve généralement pas application et les données peuvent être partagées avec des tiers même si cela ne correspond pas à la finalité du traitement initial. Il convient de noter que le privilège de la recherche n'est pas conçu de la même manière dans toutes les lois sur la protection des données ; il faut tenir compte des particularités. Voir à ce sujet Question / Frage 90.

Toutefois, si un accès à des données sensibles est accordé, la loi fédérale sur la protection des données ainsi que certaines lois cantonales sur la protection des données prévoient de manière restrictive que ces données sensibles ne peuvent en principe être communiquées à des personnes privées que sous une forme ne permettant pas d'identifier la personne concernée.

Un accord contractuel peut imposer des obligations à la personne qui a accès à un ensemble de données, telles que la confidentialité, des restrictions d'utilisation et de publication ou la citation de la source.

Nach welchen Kriterien ist der Zugang zu Forschungsdaten zu gewähren? Kann bestimmt / vorgeschrieben werden, was spätere Nutzer machen dürfen? Und wenn ja: wie?

Zum Begriff der offenen Forschungsdaten siehe die Antwort auf Question / Frage 36.

Die in den anwendbaren Gesetzen (das Bundesgesetz über den Datenschutz für die Eidgenössischen Hochschulen und die kantonalen Gesetze für die kantonalen Hochschulen (Universitäten, Fachhochschulen und Pädagogischen Hochschulen)) enthaltenen Regeln über die Datenbekanntgabe müssen in einem solchen Fall beachtet werden. Aufgrund des Forschungsprivilegs – das grundsätzlich in den Datenschutzgesetzen vorgesehen ist – findet der Grundsatz der Zweckbindung in der Regel keine Anwendung, und die Daten können mit Dritten geteilt werden, auch wenn dies nicht dem Zweck der ursprünglichen Datenbearbeitung entspricht. Zu beachten gilt hierbei, dass das sog. Forschungsprivileg nicht in allen Datenschutzgesetzen gleich ausgestaltet ist; Besonderheiten gilt es zu beachten. Zu dieser Thematik siehe Question / Frage 90.

Wenn Zugang zu besonders schützenswerten Personendaten gewährt wird, schreiben das Bundesgesetz über den Datenschutz sowie manche kantonalen Datenschutzgesetze einschränkend vor, dass besonders schützenswerte Personendaten gegenüber privaten Personen nur in einer Form bekannt gemacht werden dürfen, die keine Identifizierung der betroffenen Person ermöglicht.

Eine vertragliche Vereinbarung kann der Person, der Zugang zu einem Datensatz gewährt wird, Verpflichtungen auferlegen, wie z. B. Vertraulichkeit, Nutzungs- und Veröffentlichungsbeschränkungen oder die Angabe der Quelle.

Question / Frage 40

Les accords d'utilisation d'ORD peuvent-ils être conclus pour une durée limitée ? À quoi ressemblent-ils ? Les données peuvent-elles être supprimées à la fin de la période d'utilisation ?

En principe, un accord peut être conclu sur l'utilisation de l'ORD ou l'utilisation de l'ORD peut être soumise à certaines conditions. Ceci entre en considération si la confidentialité des données l'exige, par exemple s'il existe une déclaration de consentement limitée. Un tel accord ou de telles conditions peuvent également inclure la suppression des données sur les structures de stockage (internes). Étant donné que les données doivent être anonymisées avant leur publication, un accord visant à supprimer certaines données (données personnelles) après un certain temps semble également compréhensible.

Chez SwissUbase, si l'ensemble de données contient des données personnelles, il existe une limite de temps d'utilisation liée au projet (finalité) pour lequel les données ont été téléchargées. Un rappel apparaîtra indiquant que les données doivent être supprimées.

En revanche, il peut y avoir une obligation de publier les données de la recherche, par exemple si le projet est financé par des fonds publics. Il faudra alors concilier les intérêts contradictoires (période de publication limitée et publication permanente).

Können Nutzungsvereinbarungen für ORD für einen begrenzten Zeitraum getroffen werden? Wie sehen diese aus? Kann am Ende der Nutzungslaufzeit eine Datenlöschung vereinbart werden?

Grundsätzlich kann eine Vereinbarung über die Verwendung von ORD getroffen werden, bzw. die Verwendung von ORD kann an bestimmte Bedingungen geknüpft werden. Dies kommt in Betracht, wenn die Vertraulichkeit der Daten dies erfordert, z. B. wenn eine einschränkende Einwilligungserklärung vorliegt. Eine solche Vereinbarung oder solche Bedingungen kann/können auch die Löschung von Daten auf (internen) Speicherstrukturen umfassen. Da Personendaten vor ihrer Veröffentlichung sowieso anonymisiert werden müssen, erscheint eine Vereinbarung zur Löschung bestimmter Daten (Personendaten) nach einer bestimmten Zeit nachvollziehbar.

Bei SwissUbase gibt es für den Fall, dass ein Datensatz Personendaten enthält, eine zeitliche Begrenzung der Nutzung, die an das Projekt (und dessen Zweck) gekoppelt ist, für welche die Daten hochgeladen wurden. Es erscheint dann eine Erinnerung, die darauf hinweist, dass die Daten gelöscht werden müssen.

Es kann auf der anderen Seite auch eine Verpflichtung zur Veröffentlichung von Forschungsdaten innerhalb eines Projekts vorliegen, z. B. wenn das Projekt mit öffentlichen Mitteln finanziert ist. Dann müssen allfällige widerstreitende Interessen (begrenzter Veröffentlichungszeitraum und dauerhafte Veröffentlichung) in Einklang gebracht werden.

Question / Frage 41

Dans quelle mesure est-ce que les chercheurs et chercheuses doivent ouvrir leurs données soit sous la pression du FNS, soit sous la pression des éditeurs ?

Il n'y a pas d'obligation absolue / légale de publier les données de recherche, mais l'ORD est un principe important du paysage de la recherche suisse.

Les chercheurs et chercheuses devraient en premier lieu publier leurs données conformément aux directives des bailleurs de fonds de la recherche publique, en particulier lorsque ces directives sont en accord avec les politiques nationales et internationales en matière de science ouverte. Il faut toujours veiller à ce que les dispositions légales en vigueur, telles que les lois sur la protection des données, les droits d'auteur et les droits des brevets, soient respectées.

La pression des éditeurs ne doit pas être la seule raison de la publication et il faut toujours s'assurer qu'il n'y a pas de violation des droits de tiers. Dans les cas où il n'y a pas d'obligation (contractuelle) de publication, la manière et l'étendue de la divulgation des données relèvent avant tout d'une décision éthique en matière de recherche.

Les chercheurs et chercheuses ont également la liberté d'opter pour les options qui correspondent à leurs principes de protection des données et de science ouverte lorsqu'ils sollicitent des fonds tiers et choisissent des lieux de publication. Le respect des principes éthiques et des dispositions légales reste la priorité absolue.

Lorsqu'il s'agit de l'accès à des données de recherche confidentielles, les éditeurs ou les bailleurs de fonds sont soumis aux mêmes conditions que les autres personnes qui demandent l'accès. L'accès ne doit donc être accordé que s'il peut se faire légalement (par exemple parce que les données doivent être utilisées à des fins statistiques) et si des mécanismes de sécurité suffisants, notamment un accord de confidentialité, sont garantis.

Inwieweit sollten Forschende ihre Daten veröffentlichen, sei es auf Druck des SNF oder auf Druck eines Verlags?

Es gibt keine absolute / gesetzliche Verpflichtung zur Veröffentlichung von Forschungsdaten, aber ORD ist ein wichtiger Grundsatz innerhalb der Schweizer Forschungslandschaft.

In erster Linie sollten Forscher deshalb ihre Daten gemäss den Richtlinien der öffentlichen Forschungsförderer veröffentlichen, insbesondere wenn diese Richtlinien mit der nationalen und internationalen Open Science Politik übereinstimmen. Es sollte hierbei stets darauf geachtet werden, dass die geltenden gesetzlichen Bestimmungen, wie Datenschutzgesetze, Urheber- und Patentrechte, eingehalten werden.

Der Druck eines Verlags darf nicht der einzige Grund für eine Veröffentlichung sein und es muss immer sichergestellt werden, dass keine Rechte Dritter verletzt werden. In Fällen, in denen keine (vertragliche) Veröffentlichungspflicht besteht, ist es in erster Linie eine forschungsethische Entscheidung, wie und in welchem Umfang Forschungsdaten offengelegt werden.

Auch bei der Beantragung von Drittmitteln und der Wahl der Veröffentlichungsorte haben die Forscher die Möglichkeit, sich für eine Optionen zu entscheiden, die den Grundsätzen des Datenschutzes und der Open Science Politik entsprechen. Die Einhaltung ethischer Grundsätze und gesetzlicher Bestimmungen hat weiterhin oberste Priorität.

Wenn es um den Zugang zu vertraulichen Forschungsdaten geht, gelten für Verleger oder Geldgeber die gleichen Bedingungen wie für andere Personen, die Zugang beantragen. Der Zugang darf nur gewährt werden, wenn er rechtlich zulässig ist (z. B. weil die Daten für statistische Zwecke verwendet werden sollen) und wenn ausreichende Sicherheitsmechanismen, einschliesslich einer Geheimhaltungsvereinbarung, gewährleistet sind.

Question / Frage 42

Un bailleur de fonds exige la conservation à long terme des données de recherche sur un dépôt de données « FAIR ». Quelles données devraient être conservées tout en respectant le cadre légal et éthique ?

Pour déterminer quelles données conserver dans un projet ORD, il est crucial de trouver un équilibre entre la valeur des données et le risque de réidentification.

Voici quelques étapes et critères à considérer :

1. **Objectifs du projet** : Définissez clairement les objectifs de votre projet et identifiez les données essentielles pour atteindre ces objectifs. Conservez uniquement les données qui sont directement pertinentes.
2. **Valeur scientifique et/ou historique** : Évaluez la valeur scientifique et/ou historique des données. Les données qui apportent une contribution significative à la recherche ou qui peuvent être réutilisées par d'autres chercheurs/chercheuses devraient être prioritaires.

3. **Obligations légales et éthiques** : Assurez-vous de respecter les obligations légales et éthiques en matière de conservation des données. Certaines données peuvent devoir être conservées pour des raisons de conformité réglementaire ou de transparence scientifique.
4. **Anonymisation et pseudonymisation** : Appliquez des techniques d'anonymisation ou de pseudonymisation pour réduire le risque de réidentification. Conservez les données pseudonymisées séparément des clés de pseudonymisation.
5. **Critères techniques** : Prenez en compte les aspects techniques tels que le format des données, leur volume, et les coûts de stockage. Les données doivent être stockées dans des formats durables et accessibles.
6. **Durée de conservation** : Déterminez la durée pendant laquelle les données doivent être conservées. Certaines données peuvent ou doivent être archivées à long terme, tandis que d'autres peuvent ou doivent être supprimées après une période définie.

En suivant ces étapes, vous pouvez minimiser les risques tout en maximisant la valeur des données conservées.

Ein Geldgeber verlangt die langfristige Aufbewahrung von Forschungsdaten in einem „FAIR"-Datendepot. Welche Daten sollten unter Einhaltung der rechtlichen und ethischen Rahmenbedingungen aufbewahrt werden?

Bei der Entscheidung, welche Daten in einem ORD-Projekt aufbewahrt werden sollen, ist es massgeblich, ein Gleichgewicht zwischen dem Nutzen der Daten und dem Risiko einer Re-Identifizierung von Personen zu finden.

Hier sind Schritte und Kriterien, die berücksichtigt werden sollten:

1. **Projektziele:** Legen Sie die Ziele Ihres Projekts klar fest und bestimmen Sie die Daten, die für die Erreichung dieser Ziele wesentlich sind. Bewahren Sie nur die Daten auf, die direkt relevant sind.
2. **Wissenschaftlicher und/oder historischer Wert:** Bewerten Sie den wissenschaftlichen und/oder historischen Wert der Daten. Daten, die einen bedeutenden Beitrag zur Forschung leisten oder die von anderen Forscherenden wiederverwendet werden können, sollten Vorrang haben.
3. **Rechtliche und ethische Verpflichtungen:** Stellen Sie sicher, dass Sie die rechtlichen und ethischen Verpflichtungen zur Datenaufbewahrung einhalten. Einige Daten müssen möglicherweise aus Gründen der Einhaltung gesetzlicher Vorschriften oder der wissenschaftlichen Transparenz aufbewahrt werden.
4. **Anonymisierung und Pseudonymisierung:** Wenden Sie Anonymisierungs- oder Pseudonymisierungstechniken an, um das Risiko einer Identifizierung zu verringern. Bewahren Sie pseudonymisierte Daten getrennt von Pseudonymisierungsschlüsseln auf.
5. **Technische Kriterien:** Berücksichtigen Sie technische Aspekte wie das Datenformat, die Datenmenge und die Speicherkosten. Die Daten sollten in langlebigen und zugänglichen Formaten gespeichert werden.
6. **Aufbewahrungsdauer:** Bestimmen Sie, wie lange die Daten aufbewahrt werden müssen. Einige Daten können oder müssen langfristig aufbewahrt werden, während andere nach einer bestimmten Zeit gelöscht werden können oder müssen.

Wenn diese Schritte befolgt werden, können die Risiken minimiert und gleichzeitig der Nutzen der abgelegten Daten maximiert werden.

Question / Frage 43

Dans quelles circonstances les chercheurs et chercheuses peuvent-ils·elles déposer des données génomiques (données personnelles sensibles qui requièrent une protection particulière) dans un repository / dans une archive ?

- S'agissant des éléments à considérer lors du choix d'un dépôt, voir Question / Frage 27.
- S'agissant de la différence entre la mise à disposition de données personnelles dans un dépôt et l'archivage, voir Question / Frage 73.

Unter welchen Umständen dürfen Forschende genomische Daten (besonders schützenswerte Personendaten, die einen besonderen Schutz erfordern) in einem Repositorium / in einem Archiv abgelegt werden?

- Zu den Aspekten, die bei der Auswahl eines Repositoriums zu berücksichtigen sind, siehe Question / Frage 27.
- Zum Unterschied zwischen der Bereitstellung von Personendaten in einem Repositorium und der Archivierung siehe Question / Frage 73.

Question / Frage 44

Des outils appropriés seront-ils mis à disposition ou devront-ils être développés pour une préparation uniforme des données de recherche selon FAIR, si nécessaire ?

Actuellement, il n'existe pas d'outils universellement utilisables pour le traitement uniforme des données de recherche selon les principes FAIR. En lieu et place, il existe des listes de contrôle et des lignes directrices générales, comme par exemple celles de fairdata.fi, qui aident les chercheurs et chercheuses lors de la préparation. Lors du développement de tels outils, il faut tenir compte des différentes exigences juridiques et de la diversité des disciplines. La disponibilité des outils correspondants dépend souvent de l'institution et il existe un besoin de personnel formé dans ce domaine. L'uniformisation reste un défi en raison de la diversité des exigences et des types de données.

Werden für eine ggf. erforderliche einheitliche Aufbereitung von Forschungsdaten nach FAIR entsprechende Werkzeuge zur Verfügung stehen bzw. sollen diese entwickelt werden?

Derzeit gibt es keine universell einsetzbaren Werkzeuge für die einheitliche Aufbereitung von Forschungsdaten nach den FAIR-Prinzipien. Stattdessen gibt es Checklisten und allgemeine Richtlinien, wie z. B. die von fairdata.fi, die Forschenden bei der Aufbereitung helfen. Bei der Entwicklung solcher Tools müssen die unterschiedlichen rechtlichen Anforderungen und die vielfältigen Forschungsgebiete berücksichtigt werden. Die Verfügbarkeit der entsprechenden Tools hängt oft von der jeweiligen Institution ab, und es besteht ein Bedarf an geschultem Personal in diesem Bereich. Die Vereinheitlichung bleibt aufgrund der unterschiedlichen Anforderungen und Datentypen eine Herausforderung.

Question / Frage 45

Comment stocker / conserver les données vidéo à long terme en conformité avec la protection des données et l'ORD ?

Les principes généraux exposés à la Question / Frage 27 s’appliquent également pour les vidéos contenant des données personnelles. Pour ce qui est de l’anonymisation des vidéos, on pourra se référer à la Question / Frage 46.

Wie sollen Videodaten in Übereinstimmung mit dem Datenschutz und der DSGVO langfristig gespeichert/aufbewahrt werden?

Die allgemeinen Grundsätze, die in Question / Frage 27 dargelegt sind, gelten auch für Videos, die Personendaten enthalten. Bezüglich der Anonymisierung von Videos wird auf Question / Frage 46 verwiesen.

Question / Frage 46

Comment préparer des enregistrements sonores ou vidéo en vue d'une réutilisation ultérieure qui respecte la protection des données et les principes de l'ORD ?

Il convient d'abord de déterminer si les données peuvent être déposées sur une plateforme en ORD sous forme anonymisée. Pour des enregistrements audio ou vidéo, des mesures techniques telles que la coupure de certains passages, le floutage, la pixellisation, l'ajout de bruit ou la modification des voix peuvent être mises en œuvre. Il peut toutefois être difficile de réussir à anonymiser des enregistrements, même avec ces techniques.

Si une anonymisation n'est pas envisageable (par exemple en présence de données qualitatives ou d'interviews d'expert.es, pour lesquelles les personnes concernées sont importantes), il faut vérifier si le droit applicable permet la communication de données. Si oui, un dépôt est généralement possible aux conditions suivantes :

- Il doit y avoir le consentement du participant ou de la participante. Cela nécessite des informations complètes sur le traitement des données et la liberté pour le·la participant·e d'accepter ou non le dépôt.
- La publication doit déjà être planifiée et communiquée au moment où le consentement est demandé.
- L'infrastructure de publication (référentiel) doit être équipée de manière à pouvoir gérer un retrait de consentement.

Si les conditions ci-dessus ne peuvent être remplies, le dépôt dans un référentiel entraînera toujours un dépôt dans une archive à accès fermé (avec restrictions d'accès), à condition que le référentiel soit approuvé (en ce qui concerne la sécurité des données). Dans les cas où la protection doit être plus stricte, seules les métadonnées peuvent être publiées.

En outre, si un dépôt sur une plateforme en ORD de données personnelles (donc non anonymisées) sensibles est prévu, une analyse d'impact est recommandée.

Wie bereitet man Ton- oder Videoaufnahmen für eine spätere Weiterverwendung auf, die dem Datenschutz und den Grundsätzen der DSGVO entspricht?

Zunächst ist zu prüfen, ob die Daten in anonymisierter Form auf einer ORD-Plattform abgelegt werden können. Bei Audio- oder Videoaufnahmen können technische Massnahmen wie das Herausschneiden bestimmter Passagen, Weichzeichnen, Verpixeln, Hinzufügen von Geräuschen oder Verändern der Stimmen eingesetzt werden. Es kann sich jedoch als schwierig erweisen, Aufnahmen auch mit diesen Techniken erfolgreich zu anonymisieren.

Wenn eine Anonymisierung nicht möglich ist (z. B. bei qualitativen Daten oder Experteninterviews, bei denen die betroffenen Personen wichtig sind), muss geprüft werden, ob das anwendbare Recht eine Offenlegung der Daten erlaubt. Ist dies der Fall, ist eine Ablage in der Regel unter folgenden Bedingungen möglich:

- Es muss eine Einwilligung der betroffenen Person vorliegen. Dies erfordert eine vollständige Information über die Datenbearbeitung und die Freiwilligkeit der betroffenen Person, der Ablage zuzustimmen oder sie abzulehnen.
- Die Veröffentlichung muss bereits geplant und kommuniziert sein, wenn die Einwilligung eingeholt wird.
- Die Infrastruktur für die Veröffentlichung (Repositorium) muss so ausgestattet sein, dass ein Widerruf der Einwilligung bearbeitet werden kann.

Wenn die oben genannten Bedingungen nicht erfüllt werden können, zieht die Ablage in einem Repositorium immer eine Ablage mit geschlossenem Zugang (mit Zugangsbeschränkungen) nach sich, vorausgesetzt, das Repositorium ist (im Hinblick auf die Datensicherheit) ausreichend. In Fällen, in denen ein höherer Schutz erforderlich ist, können nur die Metadaten veröffentlicht werden.

Darüber hinaus wird empfohlen, eine Datenschutzfolgenabschätzung durchzuführen, wenn die Ablage besonders schützenswerter (d. h. nicht anonymisierter) Personendaten auf einer ORD-Plattform geplant ist.

Question / Frage 47

Comment traiter les données qualitatives (par exemple, les entretiens personnels non structurés) ? A quoi faut-il faire attention ?

Voir à ce sujet la Question / Frage 46, Question / Frage 27 et Question / Frage 28.

Les données personnelles ne peuvent être publiées qu'avec le consentement des personnes concernées (sauf s'il s'agit de personnes de l'histoire contemporaine). La divulgation d'une personne est pertinente lors de la collecte de données qualitatives ou d'une interview d'expert·e, où la personne concrète est essentielle.

Dans ce cas, il existe en particulier le risque d'une révocation du consentement, avec pour conséquence que les données personnelles doivent être effacées - selon l'ampleur de la révocation - dans leur intégralité ou en relation avec la publication. Dans le cas de données déjà publiées, il n'est toutefois pas possible de garantir, en cas de révocation, que les données ne sont pas déjà utilisées et traitées par des tiers ; en outre, une révocation peut avoir pour conséquence que les dépenses engagées en relation avec la publication sont vaines. Ces circonstances devraient déjà être signalées dans le cadre de l'information sur la demande de consentement et une éventuelle demande de dommages et intérêts devrait être prévue.

Wie ist mit qualitativen Datensätzen (bspw. unstrukturierte persönliche Interviews) umzugehen? Was gilt es zu beachten?

Siehe hierzu Question / Frage 46, Question / Frage 27 et Question / Frage 28.

Personendaten können nur mit Einwilligung der betroffenen Personen veröffentlicht werden (es sei denn es handelt sich um Personen der Zeitgeschichte). Die Offenlegung einer Person bietet sich bei einer qualitativen Datenerhebungen bzw. einem Experteninterview an, bei dem es auf die konkrete Person ankommt.

Hier besteht insbesondere das Risiko eines Widerrufs der Einwilligung mit der Folge, dass Personendaten - ja nach Umfang des Widerrufs - gänzlich oder im Zusammenhang mit der Veröffentlichung zu löschen sind. Bei bereits veröffentlichten Daten kann bei einem Widerruf allerdings nicht sichergestellt werden, dass die Daten nicht bereits durch Dritte genutzt und bearbeitet werden; weiter kann ein Widerruf dazu führen, dass im Zusammenhang mit der Veröffentlichung erfolgte Aufwendungen vergebens waren. Auf diese Umstände sollten bereits im Zusammenhang mit der Information zur Einholung der Einwilligung hingewiesen werden und eine allfällige Schadensersatzforderungen vorgesehen werden.

Question / Frage 48

Est-il possible d'informer de manière générale les participant·e·s à une recherche que leurs données personnelles seront communiquées pour des « projets de recherche nationaux et internationaux, dans les secteurs public et privé » (à l'instar de ce qui se fait pour le consentement général selon la LRH) ?

Le devoir d'information de l'art. 19 de la Loi fédérale sur la protection des données (LPD) prévoit que « les destinataires ou les catégories de destinataires auxquels des données personnelles sont transmises » doivent être communiqués à la personne concernée. Il est donc possible de mentionner uniquement des catégories de destinataires (p. ex. « les données personnelles peuvent être transmises à d'autres institutions ou à des entreprises privées pour des projets de recherche nationaux et internationaux »).

Le consentement doit porter sur le libre accès aux données et leur réutilisation - c'est-à-dire que la personne doit accepter que ses données personnelles soient rendues librement accessibles et puissent être utilisées par des tiers.

Lorsque la Loi fédérale relative à la recherche sur l'être humain (LRH) s'applique, il convient de vérifier si les exigences de cette loi sont également remplies en cas de réutilisation des données.

Ist es möglich, Teilnehmende eines Forschungsprojekts allgemein darüber zu informieren, dass ihre Personendaten für «nationale und internationale Forschungsprojekte im öffentlichen und privaten Sektor» bekanntgegeben werden (nach dem Vorbild der allgemeinen Einwilligung nach HFG)?

Die Informationspflicht nach Art. 19 Bundesgesetz über den Datenschutz sieht vor, dass «die Empfänger oder Kategorien von Empfängern, an die Personendaten bekannt gegeben werden», der betroffenen Person mitgeteilt werden müssen. Es ist also möglich, nur Kategorien von Empfängern zu nennen (z.B. «Personendaten können für nationale und internationale Forschungsprojekte an andere Institutionen oder an private Unternehmen bekannt gegeben werden»).

Die Einwilligung muss sich auf den freien Zugang zu den Daten und deren Weiterverwendung beziehen, d.h. die Person muss zustimmen, dass ihre Personendaten frei zugänglich sind und von Dritten verwendet werden dürfen.

Findet das HFG Anwendung, ist zu prüfen, ob die Anforderungen dieses Gesetzes auch bei der Weiterverwendung der Daten erfüllt sind.

VII. Partage et réutilisation de données / Teilen und Weiterverwendung von Daten

Question / Frage 49

Quel est le statut des données pour le chercheur ou la chercheuse qui réutilise des données de tiers? Dans quel cas faut-il prévoir un contrat pour cette réutilisation ?

En cas de réutilisation de données, du point de vue juridique, la haute école ou l'université qui les réutilise est responsable du traitement et donc responsable de respecter les règles en matière de protection des données et de sécurité de l'information.

En pratique, l'institution doit veiller à ce que son personnel connaisse et applique les exigences légales dans ce domaine. Les chercheurs et chercheuses responsables d'un projet doivent s'assurer que leur recherche respecte la protection des données, en suivant notamment les éventuelles instructions ou lignes directrices de l'institution. De plus, les collaborateurs et collaboratrices sont soumis au secret de fonction à titre individuel.

En cas de réutilisation, il est effectivement recommandé de prévoir un contrat ; en règle générale, un tel contrat est dans l'intérêt du tiers qui met à disposition les données car il porte la responsabilité de la communication des données.

Wie sind Daten rechtlich einzuordnen, wenn Forschende diese von Dritten weiterverwenden? In welchem Fall ist ein Vertrag für die Weiterverwendung erforderlich?

Bei der Weiterverwendung von Daten ist aus rechtlicher Sicht die Hochschule oder Universität, die die Daten nutzt, für die Bearbeitung und damit auch für die Einhaltung der Datenschutz- und Informationssicherheitsbestimmungen verantwortlich.

In der Praxis muss die nutzende Institution sicherstellen, dass ihre Mitarbeitenden die rechtlichen Anforderungen in diesem Bereich kennen und anwenden. Die für ein Projekt verantwortlichen Forschenden müssen sicherstellen, dass bei ihrer Forschung der Datenschutz eingehalten wird, indem sie insbesondere etwaige Anweisungen oder Richtlinien der Institution befolgen.

Darüber hinaus unterliegen die Mitarbeitenden individuell dem Amtsgeheimnis.

Im Falle einer Bekanntgabe von Daten empfiehlt sich der Abschluss eines Vertrages; in der Regel liegt ein solcher Vertrag im Interesse des Dritten, der die Daten zur Verfügung stellt, da er die Verantwortung für die Bekanntgabe der Daten trägt.

Question / Frage 50

Que faut-il prendre en compte lors du partage de données de recherche entre institutions en ce qui concerne les données personnelles ?

Lors du partage de données de recherche entre institutions, en particulier lorsqu'il s'agit de données à caractère personnel, les aspects suivants doivent être pris en compte :

- Législation sur la protection des données : Les lois en vigueur sur la protection des données doivent être respectées, tant au niveau national qu'international.
- Consentement : Si les données de recherche contiennent des informations à caractère personnel, il est important de s'assurer que les personnes concernées ont consenti au transfert de données ou qu'il existe une base juridique pour le traitement de ces données. Un consentement valable doit être transparent, informé et volontaire.
- Sécurité des données : des mesures de sécurité appropriées doivent être prises pour garantir la confidentialité, l'intégrité et la disponibilité des données transmises. Cela peut inclure le cryptage des données, les contrôles d'accès et d'autres mesures techniques.

Accords et contrats : Il est conseillé de conclure des accords et des contrats clairs entre les institutions participantes, qui régissent les conditions d'échange et d'utilisation des données de recherche. Ces accords devraient couvrir des aspects tels que la protection des données, la confidentialité, les droits de propriété et la responsabilité.

Was muss beim Austausch von Forschungsdaten zwischen Institutionen in Bezug auf Personendaten beachtet werden?

Beim Austausch von Forschungsdaten zwischen Institutionen, insbesondere wenn es sich um Personendaten handelt, sind folgende Aspekte zu berücksichtigen:

- Datenschutzgesetze: Die geltenden Datenschutzgesetze auf nationaler und internationaler Ebene müssen eingehalten werden.
- Einwilligung: Wenn die Forschungsdaten Informationen zu Personen enthalten, ist es wichtig sicherzustellen, dass die betroffenen Personen der Bekanntgabe der Daten zugestimmt haben oder dass es eine gesetzliche Grundlage für die Bearbeitung dieser Daten gibt. Eine rechtsgültige Einwilligung muss transparent, informiert und freiwillig sein.
- Datensicherheit: Es müssen geeignete Sicherheitsmassnahmen getroffen sein, um die Vertraulichkeit, Integrität und Verfügbarkeit der übermittelten Daten zu gewährleisten. Dies kann die Verschlüsselung von Daten, Zugangskontrollen und andere technische Massnahmen umfassen.

Vereinbarungen und Verträge: Es wird empfohlen, klare Vereinbarungen und Verträge zwischen den betreffenden Institutionen abzuschliessen, welche die Bedingungen für den Austausch und die Nutzung von Forschungsdaten regeln. Diese Vereinbarungen sollten Aspekte wie Datenschutz, Vertraulichkeit, Eigentumsrechte und Haftung abdecken.

VIII. Consentement / Einwilligung

Question / Frage 51

D'un point de vue juridique et pratique, que signifie pour une recherche le retrait du consentement pour l'utilisation et pour le partage des données personnelles ? Quelle est la situation si les données personnelles ont déjà été publiées ?

La personne concernée peut révoquer à tout moment son consentement pour le traitement ou la poursuite du traitement de ses données. Elle doit être informée explicitement de ce droit.

Avec la révocation du consentement, la haute école, l'université ou le partenaire de recherche n'est plus autorisé à poursuivre le traitement des données personnelles. Celles-ci doivent être supprimées. Toutefois, la révocation ne concerne que les données personnelles. Dans cette mesure, les autres données (p. ex. statistiques ou résultats ne comprenant plus de données personnelles) peuvent continuer à être utilisées (au final, une anonymisation complète des données est nécessaire).

En ce qui concerne les données déjà publiées, il n'est pas possible de garantir, en cas de révocation, que les données ne sont pas déjà utilisées et traitées par des tiers ; en outre, une révocation peut avoir pour conséquence que les dépenses engagées dans le cadre de la publication ont été vaines ; dans ce cas, d'éventuelles demandes de dommages et intérêts devraient déjà être prévues dans le cadre de l'information sur la demande de consentement. Il convient d'informer de ces circonstances dès l'obtention du consentement.

Was bedeutet es aus rechtlicher und praktischer Sicht für ein Forschungsprojekt, wenn die Einwilligung zur Verwendung und Bekanntgabe von Personendaten widerrufen wird? Wie sieht die Situation aus, wenn die Personendaten bereits veröffentlicht sind?

Die betroffene Person kann ihre Einwilligung in die Bearbeitung oder Bekanntgabe ihrer Personendaten jederzeit widerrufen. Auf dieses Recht muss ausdrücklich hingewiesen werden.

Nach einem Widerruf der Einwilligung dürfen die Hochschule oder Universität sowie Forschungspartner die Personendaten nicht mehr verwenden. Diese sind zu löschen. Der Widerruf bezieht sich allerdings nur auf die Personendaten. Andere Daten (z.B. Statistiken oder Ergebnisse, die keine Personendaten enthalten), dürfen insofern weiterverwendet werden (es ist also eine vollständige Anonymisierung der Daten erforderlich).

Bei bereits veröffentlichten Daten kann im Falle eines Widerrufs nicht sichergestellt werden, dass diese Daten nicht bereits von Dritten verwendet und bearbeitet werden. Darüber hinaus kann ein Widerruf dazu führen, dass die im Rahmen der Veröffentlichung getätigten Aufwendungen vergeblich waren; in diesem Zusammenhang bietet es sich an, mögliche Schadensersatzansprüche bereits bei Einholung der Einwilligung im Rahmen der Information vorzusehen.

Question / Frage 52

Quelles sont les bonnes pratiques pour stocker et conserver des consentements pendant et après le projet ? Comment gérer pratiquement les consentements lors du dépôt et du partage de données ? Sur quel support la conservation est-elle préconisée et peut-on passer d'un format papier à un format numérique ? Qu'en est-il du cycle de vie de ce consentement ?

Il n'existe pas de règles légales s'agissant du stockage des consentements. Ils devraient être conservés dans un emplacement sûr et accessible en cas de besoin (p. ex. pour vérifier un consentement ou prendre acte de sa révocation). Si la haute école ou l'université dispose d'une gestion centrale des contrats, les consentements peuvent être classés sous le contrat de projet correspondant.

Le consentement doit également porter sur le dépôt ou le partage de résultats de recherche, si ces résultats contiennent des données personnelles pour lesquelles un consentement avait été donné.

Certaines lois exigent que le consentement soit donné par écrit (c'est-à-dire avec signature à la main ou signature électronique qualifiée), par exemple l'art. 16 de la Loi fédérale relative à la recherche sur l'être humain (LRH). Dans ce cas, les originaux doivent impérativement être conservés. Il est bien sûr possible d'avoir un scan en plus du document original si cela est utile. Si aucune condition n'est posée, les consentements peuvent être donnés électroniquement.

S'agissant du cycle de vie du consentement, les déclarations de consentement peuvent en principe être détruites lorsque les données personnelles sont effacées (par exemple lors de l'anonymisation définitive). Il faut toutefois réserver d'éventuels motifs, pratiques ou légaux, imposant la conservation des consentements même après la suppression des données personnelles.

Welche bewährten Verfahren gibt es für die Speicherung und Aufbewahrung von Einwilligungserklärungen während und nach dem Projekt? Wie können Einwilligungen im Rahmen der Ablage und Bekanntgabe von Daten verwaltet werden? Auf welchem Medium wird die Aufbewahrung empfohlen und kann von Papier auf digitale Formate umgestellt werden? Wie sieht es mit dem Lebenszyklus der Einwilligung aus?

Es gibt keine gesetzlichen Vorschriften für die Aufbewahrung von Einwilligungserklärungen. Sie sollten an einem sicheren Ort aufbewahrt werden, auf den bei Bedarf zugegriffen werden kann (um z.B. eine Einwilligung zu überprüfen oder einen Widerruf aufzunehmen). Wenn die Hochschule über ein zentrales Vertragsmanagement verfügt, können die Einwilligungen unter dem entsprechenden Projektvertrag abgelegt werden.

Die Einwilligung muss sich auch auf die Ablage und/oder Bekanntgabe von Forschungsergebnissen beziehen, wenn diese Personendaten enthalten.

Einige Gesetze verlangen, dass die Einwilligung schriftlich (d.h. mit eigenhändiger Unterschrift oder qualifizierter elektronischer Unterschrift) erteilt wird, z.B. Art. 16 HFG. In diesem Fall müssen die Originale aufbewahrt werden. Selbstverständlich ist es möglich, zusätzlich zum Originaldokument einen Scan zu haben, wenn dies sinnvoll erscheint. Wenn keine Vorschriften vorliegen, kann die Einwilligung auch elektronisch erteilt werden.

Was den Lebenszyklus der Einwilligung betrifft, so können die Einwilligungserklärungen grundsätzlich vernichtet werden, wenn die Personendaten gelöscht werden (z. B. bei der endgültigen Anonymisierung). Vorbehalten bleiben mögliche praktische oder rechtliche Gründe, die eine Aufbewahrung von Einwilligungserklärungen auch nach Löschung der Personendaten erforderlich machen.

Question / Frage 53

Quel devrait être le contenu d'une déclaration de consentement pour le dépôt de données en ORD et leur réutilisation ? Cette déclaration est-elle différente si les données sont personnelles, sensibles, soumises à la LRH ou pseudonymisées ? Si oui, comment ? Est-il possible de construire un consentement général comme il est proposé dans la LRH ?

Le consentement (en vue d'une utilisation des données personnelles comme ORD) doit porter sur le libre accès aux données et leur réutilisation - c'est-à-dire que la personne doit accepter que ses données personnelles soient rendues librement accessibles et puissent être utilisées par des tiers. Il est recommandé d'obtenir un consentement exprès (et pas seulement implicite) dans tous les cas, même si la législation ne l'impose pas toujours, en particulier pour des questions de preuve.

Le contenu de la déclaration de consentement sera la même que les données personnelles soient sensibles ou non (à une différence près : le consentement doit être explicite pour le traitement de données personnelles sensibles). Si elles sont également soumises à la Loi fédérale relative à la recherche sur l'être humain (LRH), il

faudra s'assurer que la déclaration de consentement correspond aux exigences de cette loi. Enfin, si les données sont pseudonymisées (et donc en principe anonymes pour les personnes qui ne possèdent pas la table de référence ; cf. Question / Frage 67 et Question / Frage 68), un consentement n'est en principe nécessaire que dans les cas prévus par la LRH ou s'il y a un risque que les données puissent être réidentifiées par un autre moyen raisonnable.

Selon une partie de la doctrine*, un consentement dit « général » (c'est-à-dire autorisant la réutilisation des données pour tout projet actuel ou futur) est autorisé, sauf disposition légale contraire (notamment l'art. 32 al. 1 LRH, qui n'autorise pas le consentement général pour la réutilisation de matériel biologique et de données génétiques sous forme non codée).

* selon Conrad Valentin/Germond Tania, La protection des données personnelles et la valorisation des données de recherche, in: Métille Sylvain (édit.), Protection des données personnelles et recherche, Berne 2024, p. 192 s.

Welchen Inhalt sollte eine Einwilligungserklärung mit Blick auf die Ablage und die Weiterverwendung von Personendaten als ORD haben? Ist diese Erklärung anders, wenn die Daten personenbezogen, besonders schützenswert, dem Humanforschungsgesetz unterliegend oder pseudonymisiert sind? Wenn ja, wie? Ist es möglich, eine generelle Einwilligung zu formulieren, wie sie im HFG vorgesehen ist?

Die Einwilligung muss sich (mit Blick auf eine Nutzung der Personendaten als ORD) auf den freien Zugang zu den Daten und deren Weiterverwendung beziehen, d. h. die Person muss zustimmen, dass ihre Personendaten frei zugänglich sind und von Dritten verwendet werden dürfen. Es wird empfohlen, in jedem Fall eine ausdrückliche (und nicht nur konkludente) Einwilligung einzuholen, auch wenn dies nicht immer gesetzlich vorgeschrieben ist, insbesondere aus Nachweisgründen.

Der Inhalt der Einwilligungserklärung ist derselbe, unabhängig davon, ob die Personendaten besonders schützenswert sind oder nicht (mit dem Unterschied, dass die Einwilligung für die Bearbeitung von besonders schützenswerten Personendaten ausdrücklich erfolgen muss). Wenn die Daten auch dem Humanforschungsgesetz unterliegen, muss sichergestellt werden, dass die Einwilligungserklärung den Anforderungen dieses Gesetzes entspricht. Sind die Daten schliesslich pseudonymisiert (und damit im Prinzip anonym für Personen, die nicht im Besitz der Referenztabelle sind; vgl. Question / Frage 67 und Question / Frage 68), ist eine Einwilligung grundsätzlich nur in den Fällen erforderlich, die im Humanforschungsgesetz vorgesehen sind, oder wenn das Risiko besteht, dass die Personen identifiziert werden können.

Einem Teil der juristischen Lehre zufolge* ist eine «generelle» Einwilligung (d.h. eine Einwilligung, die die Weiterverwendung der Personendaten für jedes gegenwärtige oder zukünftige Projekt erlaubt) zulässig, sofern keine anderslautenden gesetzlichen Bestimmungen bestehen (insbesondere Art. 32 Abs. 1 HFG, der eine generelle Einwilligung für die Weiterverwendung von biologischem Material und genetischen Daten in unverschlüsselter Form nicht zulässt).

* nach Conrad Valentin/Germond Tania, La protection des données personnelles et la valorisation des données de recherche, in: Métille Sylvain (édit.), Protection des données personnelles et recherche, Berne 2024, S. 192 f.

Question / Frage 54

Dans le cadre de recherches académiques, peut-on réutiliser des données personnelles de santé sans le consentement des personnes concernées ?

En vertu du privilège de la recherche, les hautes écoles et universités suisses peuvent traiter des données personnelles à des fins de recherche à des conditions plus souples. Dans ce contexte, le consentement n'est donc généralement pas nécessaire pour réutiliser les données personnelles, même si elles sont sensibles (ce qui est le cas des données personnelles de santé). Il convient de noter que le privilège de la recherche n'est pas conçu de la même manière dans toutes les lois sur la protection des données ; il faut tenir compte des particularités.

Si la recherche est soumise à la Loi fédérale relative à la recherche sur l'être humain (LRH) (ce qui est le cas lorsqu'elle porte sur les maladies humaines ou sur la structure et le fonctionnement du corps humain, et qu'elle est pratiquée sur des personnes, des personnes décédées, des embryons et des fœtus, du matériel biologique ou des données personnelles liées à la santé), les art. 32 et suivants de la LRH déterminent les conditions auxquelles des données de santé peuvent être réutilisées. Ils prévoient des règles qui permettent, à certaines conditions, de réutiliser des données personnelles de santé collectées dans un autre contexte que celui de la recherche envisagée (p. ex. des données collectées dans un hôpital ou dans le cadre d'une autre recherche). Ces règles priment les règles des lois de protection des données prévoyant des privilèges de recherche dans ce contexte.

En principe, si les données personnelles de santé ne sont pas codées, un consentement éclairé est nécessaire pour la réutilisation (art. 32 et 33 LRH). La réutilisation est exceptionnellement possible sans consentement si les conditions suivantes sont remplies (art. 34 et 45 al. 1 let. b LRH) de manière cumulative :

1) l'obtention du consentement ou l'information sur le droit d'opposition est impossible ou pose des difficultés disproportionnées, ou on ne peut raisonnablement l'exiger de la personne concernée ;
2) aucun document n'atteste un refus de la personne concernée ;
3) l'intérêt de la science prime celui de la personne concernée à décider de la réutilisation de son matériel biologique ou de ses données,
4) la commission d'éthique compétente a donné son autorisation.

Dürfen im Rahmen der akademischen Forschung Gesundheitsdaten ohne die Einwilligung der betroffenen Personen weiterverwendet werden?

Aufgrund des Forschungsprivilegs können Schweizer Hochschulen und Universitäten Personendaten zu Forschungszwecken unter erleichterten Bedingungen bearbeiten. In diesem Zusammenhang ist daher in der Regel keine Einwilligung erforderlich, um Personendaten weiterzuverwenden, selbst wenn es sich um besonders schützenswerte Personendaten handelt (was bei personenbezogenen Gesundheitsdaten der Fall ist). Es ist zu beachten, dass das Forschungsprivileg nicht in allen Datenschutzgesetzen gleich ausgestaltet ist; die Besonderheiten müssen berücksichtigt werden.

Wenn die Forschung dem Humanforschungsgesetz (HFG) untersteht (was der Fall ist, wenn sie menschliche Krankheiten oder den Aufbau und die Funktionsweise des menschlichen Körpers zum Gegenstand hat und mit Personen, verstorbenen Personen, Embryonen und Föten, biologischem Material oder gesundheitsbezogenen Personendaten durchgeführt wird), legen die Art. 32 ff. HFG die Bedingungen fest, unter denen Gesundheitsdaten weiterverwendet werden dürfen. Die Art. 32 ff. Humanforschungsgesetz (HFG) regeln die Voraussetzungen für die Weiterverwendung von Gesundheitsdaten. Sie enthalten Regelungen, die unter bestimmten Voraussetzungen die Weiterverwendung von Gesundheitsdaten erlauben, welche in einem anderen Kontext als dem der geplanten Forschung erhoben wurden (z.B. Daten, die in einem Spital oder im Rahmen eines anderen Forschungsprojekts erhoben wurden). Diese Regelungen haben Vorrang vor den Regelungen der Datenschutzgesetze (die in diesem Zusammenhang Forschungsprivilegien vorsehen).

Grundsätzlich gilt: Wenn die Gesundheitsdaten nicht verschlüsselt sind, ist für die Weiterverwendung eine Einwilligung nach Aufklärung erforderlich (Art. 32 und 33 HFG). Die Weiterverwendung ist ausnahmsweise ohne Einwilligung möglich, wenn die folgenden Voraussetzungen kumulativ erfüllt sind (Art. 34 und 45 Abs. 1 lit. b HFG):

1) die Einholung der Einwilligung oder die Information über das Widerspruchsrecht ist unmöglich oder mit unverhältnismässigen Schwierigkeiten verbunden kann von der betroffenen Person vernünftigerweise nicht erfragt werden;
2) es gibt keine Unterlagen, die eine Ablehnung der betroffenen Person belegen;
3) das Interesse der Forschung überwieg gegenüber dem Interesse der betroffenen Person, über die Weiterverwendung ihres biologischen Materials oder ihrer Daten zu bestimmen;
4) die zuständige Ethikkommission hat ihre Zustimmung erteilt.

Question / Frage 55

Le consentement est-il le seul motif permettant d'ouvrir les données lorsque celle-ci sont encore personnelles ?

Voir la réponse donnée à la Question / Frage 27 et Question / Frage 28.

Bietet die Einwilligung die einzige Grundlage, um Personendaten mittels Repositorien zu teilen?

Siehe hierzu die Antwort auf Question / Frage 27 und Question / Frage 28.

Question / Frage 56

Sur la base du « privilège de la recherche », l'obtention d'un consentement pour l'utilisation des données personnelles peut-elle être considérée comme un motif suffisant ?

Le privilège de la recherche et le consentement sont deux problématiques différentes. Le privilège de la recherche permet aux hautes écoles et universités suisses de traiter des données personnelles à des fins de recherche à des conditions plus souples. Dans ce contexte, le consentement n'est donc généralement pas nécessaire pour traiter les données personnelles.

En revanche, même si le privilège de la recherche s'applique, le consentement peut être nécessaire pour une autre raison, par exemple si la recherche est soumise à la Loi fédérale relative à la recherche sur l'être humain (LRH).

Kann auf der Grundlage des «Forschungsprivilegs» die Einholung einer Einwilligung zur Verwendung von Personendaten als ausreichende Grundlage angesehen werden?

Das Forschungsprivileg und die Einwilligung sind zwei unterschiedliche Thematiken. Das Forschungsprivileg erlaubt den Schweizer Hochschulen und Universitäten, Personendaten zu Forschungszwecken unter erleichterten Bedingungen zu bearbeiten. In diesem Zusammenhang ist in der Regel keine Einwilligung für die Bearbeitung von Personendaten erforderlich.

Selbst wenn das Forschungsprivileg zur Anwendung kommt, kann eine Einwilligung aus einem anderen Grund erforderlich sein, z.B. wenn die Forschung dem Humanforschungsgesetz untersteht.

Question / Frage 57

Le consentement pour l'ouverture des données en ORD doit-il être obtenu séparément du consentement pour mener la recherche ?

Le consentement (non pas en tant que base juridique, mais qui serait nécessaire pour des raisons d'éthique de la recherche [cf. code d'intégrité scientifique] ou pour le traitement de données personnelles sensibles) ne peut se rapporter qu'à une seule opération de traitement ou à un seul ensemble d'opérations de traitement. S'il existe deux opérations distinctes qui peuvent être traitées séparément, un consentement est nécessaire pour chacune d'entre elles. Dans le cas présent, il s'agit de deux opérations de traitement : traitement pour la réalisation de travaux de recherche (dans le cadre d'un projet) et divulgation.

Il peut en aller autrement selon la Loi fédérale relative à la recherche sur l'être humain (LRH), où un consentement général (pour la recherche dans plusieurs projets) est possible.

Muss die Einwilligung zur Veröffentlichung von Personendaten als ORD getrennt von der Einwilligung zur Durchführung der Forschung eingeholt werden?

Eine Einwilligung (dient nicht als Rechtsgrundlage, die aber aus forschungsethischen Gründen [vgl. Kodex für wissenschaftliche Integrität] oder bei der Bearbeitung besonders schützenswerter Personendaten erforderlich ist) kann sich nur auf einen einzigen Bearbeitungsvorgang oder eine Reihe von Bearbeitungsvorgängen beziehen. Handelt es sich um zwei verschiedene Vorgänge, die getrennt bearbeitet werden können, ist die Einwilligung für jeden dieser Vorgänge erforderlich. Im vorliegenden Fall handelt es sich um zwei Bearbeitungsvorgänge: die Bearbeitung der Personendaten zu Forschungszwecken (im Rahmen eines Projekts) und die Veröffentlichung.

Nach dem Humanforschungsgesetz kann dies anders zu beurteilen sein, da hier eine generelle Einwilligung (für die Forschung in mehreren Projekten) möglich ist.

IX. Personnes ayant accès aux données / Personen mit Zugang zu Daten

Question / Frage 58

Qui peut être le porteur de code/clef après la fin d'un projet ?

Pour la clé des données personnelles, le principe de proportionnalité – qui implique que le traitement de données personnelles doit se limiter à ce qui est nécessaire – s'applique : seules les personnes qui doivent connaître la clé, c'est-à-dire celles pour lesquelles elle est nécessaire à la réalisation du projet, doivent la connaître.

Une règle spéciale s'applique en cas d'une réutilisation sous forme codée de matériel biologique, de données génétiques ou de données personnelles liées à la santé : il est stipulé à l'art. 26 al. 2 de l'Ordonnance relative à la recherche sur l'être humain (ORH) que « Le code doit être conservé par une personne qui est désignée dans la demande et n'est pas impliquée dans le projet de recherche, séparément du matériel biologique ou des données personnelles et conformément aux principes visés à l'art. 5, al. 1 ». La Commission cantonale vaudoise d'éthique de la recherche sur l'être humain (CER-VD) a confirmé que l'administrateur d'une plateforme comme REDCap peut être considéré comme « une personne extérieure au projet », même si l'administrateur de ce service appartient à la même institution que l'investigateur principal de la recherche concernée.

Wer kann nach Abschluss eines Projekts Inhaber des Pseudonymisierungsschlüssels sein?

Für den Schlüssel zu den Personendaten gilt das Verhältnismässigkeitsprinzip im Sinne der Erforderlichkeit: Nur Personen, die den Schlüssel kennen müssen, d.h. die ihn für die Durchführung des Projekts benötigen, dürfen ihn kennen.

Für die Weiterverwendung von biologischem Material, genetischen Daten oder Gesundheitsdaten in verschlüsselter Form enthält die Humanforschungsverordnung in Art. 26 Abs. 2 eine Sonderregelung: «Der Schlüssel muss von einer im Gesuch zu bezeichnenden Person oder Organisationseinheit, die nicht am Forschungsprojekt beteiligt ist, getrennt vom biologischen Material und den Personendaten sowie nach den Grundsätzen nach Artikel 5 Absatz 1 aufbewahrt werden.» Die Kantonale Ethikkommission Waadt hat bestätigt, dass der Administrator einer Plattform wie REDCap als «nicht am Projekt beteiligte Person» betrachtet werden kann, auch wenn der Administrator derselben Institution angehört wie der Projektleiter.

Question / Frage 59

Si un chercheur ou une chercheuse quitte la haute école à laquelle il·elle est affilié·e (départ à la retraite, fin de contrat ou encore changement de poste au sein de l'institution), qui a accès aux consentements éclairés relatifs au traitement de données personnelles que ce chercheur ou cette chercheuse a obtenus dans le cadre de ses recherches ?

Si un consentement est demandé, la personne concernée devra également pouvoir le retirer. Il faudra mettre en œuvre un processus qui permet de gérer cette demande même si le chercheur ou la chercheuse a quitté la haute école ou l'université. D'un point de vue juridique, la responsabilité de gérer ce consentement incombera à la haute école ou l'université.

Pour chaque traitement, la question doit en principe être réglée avant même le début du traitement par le responsable du traitement (c'est-à-dire la haute école ou l'université) en vertu de son obligation d'assurer la protection des données dès la conception et par défaut (art. 7 de la Loi fédérale sur la protection des données - LPD).

Wenn ein Forscher die Hochschule, der er angehört, verlässt (Pensionierung, Vertragsende oder auch Wechsel der Position innerhalb der Institution), wer hat dann Zugang zu den Einwilligungserklärungen, die dieser Forscher im Rahmen seiner Forschung betreffend die Bearbeitung von Personendaten eingeholt hat?

Wenn eine Einwilligung eingeholt wird, muss die betroffene Person diese auch widerrufen können. Es muss deshalb ein Prozess implementiert werden, der es ermöglicht, diese Anfrage auch dann noch zu adressieren, wenn der*die Forscher*in die Hochschule oder Universität verlassen hat. Aus rechtlicher Sicht liegt die Verantwortung für die Verwaltung dieser Einwilligungserklärungen bei der Hochschule oder Universität.

Bei jeder Bearbeitung von Personendaten muss diese Frage grundsätzlich vor Beginn der Bearbeitung durch den Verantwortlichen (d.h. die Hochschule oder Universität) aufgrund der Verpflichtung, den Datenschutz von Anfang an und standardmässig zu gewährleisten (Art. 7 Bundesgesetz über den Datenschutz), geklärt werden.

Question / Frage 60

Si un chercheur ou une chercheuse quitte l'institution mais est encore dans un projet FNS, est-ce qu'il·elle a le droit de partir sans autre avec les données acquises dans le cadre du FNS ? Si les données ne sont pas anonymisées ou suffisamment codées, est-ce que l'institution a le droit de les laisser partir comme ça hors de son périmètre ? Qu'en est-il de la responsabilité du chercheur ou de la chercheuse ? Un chercheur ou une chercheuse est-il·elle propriétaire des données collectées ?

Les données « appartiennent » à la haute école ou l'université, car elles ont été collectées dans le cadre de la relation de travail. La haute école ou l'université est donc responsable du traitement au sens de la protection des données. En outre, tous les résultats de la relation de travail appartiennent à l'institution en sa qualité d'employeur.

Dans la pratique, la haute école ou l'université et le chercheur ou la chercheuse ont tous deux intérêt à ce qu'un projet soit terminé et les données soient « données avec ». Dans ce cas, il est conseillé de conclure un accord avec le chercheur ou la chercheuse qui quitte l'institution pour l'utilisation ultérieure des données, y compris les droits de publication.

Lors de la réutilisation de données personnelles collectées par un chercheur ou une chercheuse quittant la haute école ou l'université, il y a par ailleurs transmission de données à une autre institution. Il faut donc déterminer si les conditions de la communication et du traitement des données personnelles par la nouvelle institution sont réunies (base légale et/ou privilège de la recherche).

En emportant les données, la nouvelle institution devient également responsable du traitement, même si elle ne dispose pas d'un droit d'utilisation illimité. Pour définir le droit d'utilisation, il convient de conclure un accord avec l'institution également.

Wenn ein Forscher eine Institution verlässt, aber noch in einem SNF-Projekt beteiligt ist, hat er dann das Recht, die im Rahmen des SNF-Projekts erworbenen Daten mitzunehmen? Wenn die Daten nicht anonymisiert oder ausreichend verschlüsselt sind, hat die Institution das Recht, sie aus ihrem Verantwortungsbereich entfernen zu lassen? Wie steht es mit der Verantwortung des Forschers? Ist ein Forscher Eigentümer der gesammelten Daten?

Die Daten «gehören» der Hochschule, da sie im Rahmen des Beschäftigungsverhältnisses erhoben wurden. Die Hochschule oder Universität ist daher datenschutzrechtlich für die Bearbeitung verantwortlich. Darüber hinaus gehören alle Ergebnisse aus dem Arbeitsverhältnis der Institution in ihrer Eigenschaft als Arbeitgeber.

In der Praxis haben sowohl die Hochschule als auch der*die Forscher*in ein Interesse daran, dass ein Projekt abgeschlossen wird und die Daten «mitgenommen werden». Es ist deshalb ratsam, mit einem*einer ausscheidenden Forscher*in eine Vereinbarung über die Weiterverwendung der Daten einschliesslich der Veröffentlichungsrechte zu treffen.

Die Weiterverwendung von Personendaten, die von einem*einer Forscher*in erhoben wurden, der die Hochschule oder Universität verlässt, bedeutet auch eine Bekanntgabe dieser Daten an eine andere Institution. Es ist daher zu klären, ob die Voraussetzungen für die Bekanntgabe und Bearbeitung der Personendaten durch die neue Institution gegeben sind (gesetzliche Grundlage und/oder Forschungsprivileg).

Mit der Übernahme der Daten wird die neue Institution auch für die Datenbearbeitung verantwortlich, selbst wenn sie kein uneingeschränktes Nutzungsrecht haben sollte. Um das Nutzungsrecht festzulegen, sollte mit der Institution eine weitere Vereinbarung getroffen werden.

Question / Frage 61

Qui doit avoir accès aux données codées collectées dans le cadre du projet FNS ? Qui doit avoir accès aux données anonymes collectées dans le cadre du projet ? Qui doit avoir accès à la clé des données d'identification personnelle ?

Le principe de proportionnalité – qui implique que le traitement de données personnelles doit se limiter à ce qui est nécessaire – s'applique. Il signifie que seules les personnes qui ont besoin des données personnelles dans le cadre de la réalisation du projet doivent avoir accès à ces données.

Dès que les données sont anonymisées, il n'y a plus de données personnelles. C'est pourquoi le critère est ici le besoin de protection des données/informations.

Pour la clé des données personnelles, le principe de proportionnalité s'applique également comme pour les données personnelles elles-mêmes : seules les personnes qui doivent connaître la clé, c'est-à-dire celles pour lesquelles elle est nécessaire à la réalisation du projet, doivent également la connaître.

Une règle spéciale s'applique en cas d'une réutilisation sous forme codée de matériel biologique, de données génétiques ou de données personnelles liées à la santé : il est stipulé à l'art. 26 al. 2 de l'Ordonnance relative à la recherche sur l'être humain (ORH) que « Le code doit être conservé par une personne qui est désignée dans la demande et n'est pas impliquée dans le projet de recherche, séparément du matériel biologique ou des données personnelles et conformément aux principes visés à l'art. 5, al. 1 ». La Commission cantonale vaudoise d'éthique de la recherche sur l'être humain (CER-VD) a confirmé que l'administrateur d'une plateforme comme REDCap peut être considéré comme « une personne extérieure au projet », même si l'administrateur de ce service appartient à la même institution que l'investigateur principal de la recherche concernée.

À noter encore que l'utilisation sans droit du numéro AVS fait l'objet de sanctions pénales (art. 153 i LAVS).

Wer soll Zugang zu den im Rahmen eines SNF-Projekts erhobenen verschlüsselten Daten haben? Wer soll Zugang zu den im Rahmen des Projekts erhobenen anonymen Daten haben? Wer soll Zugang zum Schlüssel für die Identifikation haben?

Es gilt der Grundsatz der Verhältnismässigkeit im Sinne der Erforderlichkeit. Dies bedeutet, dass nur diejenigen Personen Zugang zu den Personendaten haben sollen, die diese Daten im Rahmen der Durchführung des Projekts benötigen.

Sobald die Daten anonymisiert werden, liegen keine Personendaten mehr vor. Deshalb gilt dann als Kriterium die Frage nach der Notwendigkeit des Schutzes der Daten/Informationen.

Für den Schlüssel zu den Personendaten gilt – wie für die Personendaten selbst – ebenfalls das Verhältnismässigkeitsprinzip im Sinne der Erforderlichkeit: Nur Personen, die den Schlüssel kennen müssen, d.h. die ihn für die Durchführung des Projekts benötigen, dürfen ihn kennen.

Für die Weiterverwendung von biologischem Material, genetischen Daten oder Gesundheitsdaten in verschlüsselter Form enthält die Humanforschungsverordnung in Art. 26 Abs. 2 eine Sonderregelung: «Der Schlüssel muss von einer im Gesuch zu bezeichnenden Person oder Organisationseinheit, die nicht am Forschungsprojekt beteiligt ist, getrennt vom biologischen Material und den Personendaten sowie nach den Grundsätzen nach Artikel 5 Absatz 1 aufbewahrt werden.» Die Kantonale Ethikkommission Waadt hat bestätigt, dass der Administrator einer Plattform wie REDCap als «nicht am Projekt beteiligte Person» betrachtet werden kann, auch wenn der Administrator derselben Institution angehört wie der Projektleiter.

Ergänzend sei darauf hingewiesen, dass eine unberechtigte Verwendung der AHV-Nummer strafrechtlich verfolgt wird (Art. 153i AHVG).

X. Anonymisation et pseudonymisation / Anonymisierung und Pseudonymisierung

Question / Frage 62

Afin de garantir une publication complète des données collectées, il est important de s'assurer, dès la collecte des données, qu'aucune donnée personnelle n'est disponible. Quelles conditions doivent être remplies pour garantir une collecte anonyme ?

Des données sont considérées comme anonymes lorsqu'elles ne permettent pas d'identifier la personne concernée ou uniquement en déployant des efforts disproportionnés. Pour déterminer si des données sont bien anonymes, l'ensemble des circonstances doivent être prises en compte. Même si une seule donnée ne permet pas d'identifier une personne, la combinaison de différentes données collectées peut permettre de l'identifier. Il est particulièrement important de vérifier si la combinaison de données peut conduire à l'identification de personnes lorsque des recherches très précises sont effectuées (qui mentionnent, par exemple, l'âge ou l'année de naissance au lieu d'utiliser une fourchette d'âge) et lorsqu'une collecte de données est effectuée auprès d'un cercle fermé de personnes (par exemple, les collaborateurs et collaboratrices d'une certaine entreprise, les habitant·e·s d'une certaine commune, etc.). Dans ce cas, les cas isolés méritent une attention particulière (personnes particulièrement jeunes ou âgées, nationalités rarement rencontrées dans le pays où se déroule la recherche, etc.). Un risque important de réidentification existe également lorsque des données personnelles publiquement accessibles concernent les mêmes personnes.

Pour collecter des données de manière anonyme, il est nécessaire de vérifier, avant de récolter des informations, que celles-ci permettront d'atteindre le but de la recherche sans permettre l'identification des personnes. Dans le cadre d'un sondage, il faudra par exemple se demander, suivant le groupe cible, s'il est possible de demander l'âge des personnes ou uniquement une tranche d'âge (20-29 ans), le lieu de domicile ou uniquement le canton de domicile, etc.

Plusieurs méthodes existent pour assurer l'anonymisation des données ; les chercheurs et chercheuses pourront notamment se référer à la page « Anonymisation des données » proposée par l'EPFL : https://www.epfl.ch/campus/services/data-protection/fr/en-pratique/le-respect-de-la-vie-privee-dans-la-recherche/anonymisation-des-donnees/ .

Um eine vollständige Veröffentlichung der gesammelten Daten zu gewährleisten, kann es wichtig sein, bereits bei der Datenerhebung sicherzustellen, dass keine Personendaten vorhanden sind. Welche Bedingungen müssen erfüllt sein, um eine anonyme Sammlung von Daten zu gewährleisten?

Daten gelten als anonym, wenn eine betroffene Person nicht oder nur mit unverhältnismässigem Aufwand identifiziert werden kann. Um festzustellen, ob Daten tatsächlich anonym sind, müssen alle Umstände berücksichtigt werden. Selbst wenn ein einzelner Datensatz keine Identifizierung einer Person ermöglicht, kann die Kombination verschiedener, gesammelter Daten eine Identifizierung ermöglichen. Es ist deshalb besonders wichtig zu prüfen, ob die Kombination von Daten zur Identifizierung von Personen führen kann. Dies kann insbesondere der Fall sein, wenn sehr genaue Abfragen durchgeführt werden (z. B. Angabe des Alters oder des Geburtsjahrgangs anstelle einer Altersspanne) und wenn Daten von einer geschlossenen Gruppe von Personen erhoben werden (z. B. Mitarbeitende eines bestimmten Unternehmens, Einwohner einer bestimmten Gemeinde usw.). In diesem Fall verdienen Einzelfälle besondere Aufmerksamkeit (besonders junge oder alte Personen, Nationalitäten, die in dem Land, in dem die Forschung durchgeführt wird, selten sind usw.). Ein erhebliches Risiko der Re-Identifizierung besteht auch, wenn öffentlich zugängliche Personendaten dieselben Personen betreffen.

Um Daten anonym zu erheben, muss vor der Datenerhebung geprüft werden, ob die Informationen das Forschungsziel erreichen können, ohne die Identifizierung von Personen zu ermöglichen. So muss z.B. bei einer Umfrage je nach Zielgruppe überlegt werden, ob nach dem Alter der Personen oder nur nach einer bestimmten Altersgruppe (20-29 Jahre), nach dem Wohnort oder nur nach dem Wohnkanton usw. gefragt wird / werden kann.

Es gibt verschiedene Methoden, um die Anonymisierung der Daten zu gewährleisten; Forschende finden hierzu auf der Seite «Anonymisation des données» der EPFL weitere Informationen: https://www.epfl.ch/campus/services/data-protection/fr/en-pratique/le-respect-de-la-vie-privee-dans-la-recherche/anonymisation-des-donnees/.

Question / Frage 63

Pour préparer les données en vue d'une publication, les données personnelles éventuellement disponibles doivent être rendues anonymes. Quand des données personnelles sont-elles considérées comme pseudonymisées ? Quand sont-elles considérées comme anonymisées ? La réponse est-elle identique si les données sont soumises à la LRH ?

Des données sont considérées comme anonymes lorsqu'elles ne permettent pas d'identifier la personne concernée ou uniquement en déployant des efforts disproportionnés. Les données pseudonymisées - c'est-à-dire dont les informations identifiantes ont été remplacées par un pseudonyme (par exemple, remplacement du nom et prénom par un chiffre) - sont considérées juridiquement comme anonymes pour la personne qui les reçoit et qui ne dispose pas de la clé ou la table de correspondance, ni d'autres possibilités de les réidentifier (sous réserve des indications au paragraphe suivant). La pseudonymisation est réversible, tandis que l'anonymisation ne l'est pas.

Pour déterminer si des données sont bien anonymes, l'ensemble des circonstances doivent être prises en compte. Même si une seule donnée ne permet pas d'identifier une personne, la combinaison de différentes données collectées peut permettre de l'identifier : par exemple, dans la liste des patient·e·s d'un hôpital, [ID 8128136, Femme, 42 ans, habite (petit village), traitée pour le SIDA, date d'opération 12.07.2021] ne remplit pas les conditions d'anonymité, car cette personne pourrait être identifiée sans efforts disproportionnés. Il est particulièrement important de vérifier si la combinaison de données peut conduire à l'identification de personnes lorsque des recherches très précises sont effectuées (qui mentionne, par exemple, l'âge ou l'année de naissance au lieu d'utiliser une fourchette d'âge) et lorsqu'une collecte de données est effectuée auprès d'un cercle fermé de personnes (par exemple les collaborateurs et collaboratrices d'une certaine entreprise, les habitant·e·s d'une certaine commune, etc.). Dans ce cas, les cas isolés méritent une attention particulière (personnes particulièrement jeunes ou âgées, nationalités rarement rencontrées dans le pays où se déroule la recherche, etc.). Un risque important de réidentification existe également lorsque des données personnelles publiquement accessibles concernent les mêmes personnes.

Plusieurs méthodes existent pour anonymiser des données ; les chercheurs et chercheuses pourront notamment se référer à la page « Anonymisation des données » proposée par l'EPFL : https://www.epfl.ch/campus/services/data-protection/fr/en-pratique/le-respect-de-la-vie-privee-dans-la-recherche/anonymisation-des-donnees/.

Précisons que la LRH ne s'applique pas à la recherche sur du matériel biologique anonymisé ou sur des données liées à la santé qui ont été collectées anonymement ou anonymisées (cf. art. 2 al. 2 let. b et c LRH). Si les données peuvent être considérées comme anonymes, la LRH n'est donc plus pertinente.

Voir aussi la réponse donnée à la Question / Frage 70.

Um die Daten für eine Veröffentlichung vorzubereiten, müssen eventuell vorhandene Personendaten anonymisiert werden. Wann gelten Personendaten als pseudonymisiert? Wann gelten sie als anonymisiert? Ist die Antwort dieselbe, wenn die Daten dem Humanforschungsgesetz unterliegen?

Daten sind anonym, wenn sie nicht oder nur mit unverhältnismässigem Aufwand die Identifizierung einer betroffenen Person ermöglichen. Pseudonymisierte Daten - d. h. Daten, bei denen die identifizierenden Informationen durch ein Pseudonym ersetzt wurden (z. B. Ersetzen des Vor- und Nachnamens durch eine

Nummer) – gelten rechtlich als anonym für eine Person, die sie erhält und die weder über den Schlüssel oder die Zuordnungstabelle noch über andere Möglichkeiten zur Re-Identifizierung verfügt (vorbehaltlich der Ausführungen im nächsten Absatz). Die Pseudonymisierung ist reversibel, die Anonymisierung nicht.

Um festzustellen, ob Daten tatsächlich anonym sind, müssen alle Umstände berücksichtigt werden. Selbst wenn ein einzelner Datensatz nicht zur Identifizierung einer Person führt, kann die Kombination verschiedener gesammelter Daten eine Identifizierung ermöglichen: Beispielsweise erfüllen die folgenden Daten in der Patientenliste eines Krankenhauses [ID 8128136, weiblich, 42 Jahre, wohnhaft (kleines Dorf), wird wegen AIDS behandelt, Operationsdatum 12.07.2021] nicht die Anforderungen der Anonymität, da diese Person ohne unverhältnismässigen Aufwand identifiziert werden kann. Es ist deshalb besonders wichtig zu prüfen, ob die Kombination von Daten zur Identifizierung von Personen führen kann. Dies kann insbesondere der Fall sein, wenn sehr genaue Abfragen durchgeführt werden (z. B. Angabe des Alters oder des Geburtsjahrgangs anstelle einer Altersspanne) und wenn Daten von einer geschlossenen Gruppe von Personen erhoben werden (z. B. Mitarbeitende eines bestimmten Unternehmens, Einwohner einer bestimmten Gemeinde usw.). In diesem Fall verdienen Einzelfälle besondere Aufmerksamkeit (besonders junge oder alte Personen, Nationalitäten, die in dem Land, in dem die Forschung durchgeführt wird, selten sind usw.). Ein erhebliches Risiko der Re-Identifizierung besteht auch, wenn öffentlich zugängliche Personendaten dieselben Personen betreffen.

Es gibt verschiedene Methoden, um die Anonymisierung der Daten zu gewährleisten; Forschende finden hierzu auf der Seite «Anonymisation des données» der EPFL weitere Informationen: https://www.epfl.ch/campus/services/data-protection/fr/en-pratique/le-respect-de-la-vie-privee-dans-la-recherche/anonymisation-des-donnees/.

Das Humanforschungsgesetz (HFG) findet keine Anwendung bei einer Forschung mit anonymisiertem biologischem Material oder mit anonym erhobenen oder anonymisierten Gesundheitsdaten (vgl. Art. 2 Abs. 2 Bst. b und c HFG). Können die Daten als anonymisiert betrachtet werden, ist das HFG somit nicht mehr massgeblich.

Siehe hierzu auch die Antwort auf Question / Frage 70.

Question / Frage 64

Lors de la publication de données de recherche, il faut s'assurer qu'elles sont anonymisées. Différentes catégories de données collectées peuvent permettre - sans que les catégories de données individuelles rendent une personne identifiable - une fois réunies, une identification. La question se pose de savoir quand la combinaison de données collectées permet d'identifier une personne ?

Des données sont considérées comme anonymes lorsqu'elles ne permettent pas d'identifier la personne concernée ou uniquement en déployant des efforts disproportionnés.

Pour déterminer si des données sont bien anonymes, l'ensemble des circonstances doivent être prises en compte. Même si une seule donnée ne permet pas d'identifier une personne, la combinaison de différentes données collectées peut permettre de l'identifier : par exemple, dans la liste des patient·e·s d'un hôpital, [ID 8128136, Femme, 42 ans, habite (petit village), traitée pour le SIDA, date d'opération 12.07.2021] ne remplit pas les conditions d'anonymité, car cette personne pourrait être identifiée sans efforts disproportionnés. Il est particulièrement important de vérifier si la combinaison de données peut conduire à l'identification de personnes lorsque des recherches très précises sont effectuées (qui mentionne, par exemple, l'âge ou l'année de naissance au lieu d'utiliser une fourchette d'âge) et lorsqu'une collecte de données est effectuée auprès d'un cercle fermé de personnes (par exemple les collaborateurs et collaboratrices d'une certaine entreprise, les habitant·e·s d'une certaine commune, etc.). Dans ce cas, les cas isolés méritent une attention particulière (personnes particulièrement jeunes ou âgées, nationalités rarement rencontrées dans le pays où se déroule la recherche, etc.). Un risque important de réidentification existe également lorsque des données personnelles publiquement accessibles concernent les mêmes personnes.

Plusieurs méthodes existent pour anonymiser des données ; les chercheurs et chercheuses pourront notamment se référer à la page « Anonymisation des données » proposée par l'EPFL : https://www.epfl.ch/campus/services/data-protection/fr/en-pratique/le-respect-de-la-vie-privee-dans-la-recherche/anonymisation-des-donnees/ .

Bei der Veröffentlichung von Forschungsdaten muss sichergestellt werden, dass diese anonymisiert sind. Verschiedene Kategorien von gesammelten Daten können – ohne dass die einzelnen Datenkategorien eine Person identifizierbar machen - in ihrer Kombination eine Identifizierung ermöglichen. Es stellt sich die Frage, wann die Kombination an gesammelten Daten die Identifizierung einer Person ermöglicht?

Daten gelten als anonym, wenn eine betroffene Person nicht oder nur mit unverhältnismässigem Aufwand identifiziert werden kann.

Um festzustellen, ob Daten tatsächlich anonym sind, müssen alle Umstände berücksichtigt werden. Selbst wenn ein einzelner Datensatz nicht zur Identifizierung einer Person führt, kann die Kombination verschiedener gesammelter Daten eine Identifizierung ermöglichen: Beispielsweise erfüllen die folgenden Daten in der Patientenliste eines Krankenhauses [ID 8128136, weiblich, 42 Jahre, wohnhaft (kleines Dorf), wird wegen AIDS behandelt, Operationsdatum 12.07.2021] nicht die Anforderungen der Anonymität, da diese Person ohne unverhältnismässigen Aufwand identifiziert werden kann. Es ist deshalb besonders wichtig zu prüfen, ob die Kombination von Daten zur Identifizierung von Personen führen kann. Dies kann insbesondere der Fall sein, wenn sehr genaue Abfragen durchgeführt werden (z. B. Angabe des Alters oder des Geburtsjahrgangs anstelle einer Altersspanne) und wenn Daten von einer geschlossenen Gruppe von Personen erhoben werden (z. B. Mitarbeitende eines bestimmten Unternehmens, Einwohner einer bestimmten Gemeinde usw.). In diesem Fall verdienen Einzelfälle besondere Aufmerksamkeit (besonders junge oder alte Personen, Nationalitäten, die in dem Land, in dem die Forschung durchgeführt wird, selten sind usw.). Ein erhebliches Risiko der Re-Identifizierung besteht auch, wenn öffentlich zugängliche Personendaten dieselben Personen betreffen.

Es gibt verschiedene Methoden, um die Anonymisierung der Daten zu gewährleisten; Forschende finden hierzu auf der Seite «Anonymisation des données» der EPFL weitere Informationen: https://www.epfl.ch/campus/services/data-protection/fr/en-pratique/le-respect-de-la-vie-privee-dans-la-recherche/anonymisation-des-donnees/.

Question / Frage 65

Pour les données agrégées, l'exigence est qu'il ne soit pas possible de remonter aux données originales. Comment cela est-il garanti (par défaut) ? Est-ce que chaque chercheur ou chercheuse le fait à sa guise ?

On entend par « agrégation » le fait de réunir des identifiants et des attributs cibles en moyennes et totaux.

Pour garantir que les données originales ne puissent pas être déduites des données agrégées, plusieurs techniques et bonnes pratiques peuvent être mises en place en parallèle :

1. **Anonymisation** : Les données personnelles identifiables sont supprimées ou modifiées de manière à ce qu'elles ne puissent pas être reliées à une personne spécifique.
2. **Agrégation par niveaux** : Les données sont regroupées à un niveau de granularité suffisamment élevé pour empêcher la réidentification. Par exemple, au lieu de publier des données individuelles, on publie des moyennes ou des totaux par groupe (par exemple, par région ou par tranche d'âge).
3. **Suppression des identifiants uniques** : Les identifiants uniques ou les informations directement identifiables sont supprimés avant l'agrégation. Cela inclut les noms, adresses, numéros de téléphone, etc.
4. **Randomisation** : Cette technique consiste à ajouter du bruit statistique aux données avant l'agrégation. Cela rend plus difficile la réidentification des individus à partir des données agrégées.

5. **Généralisation** : Les données sont généralisées pour réduire leur spécificité. Par exemple, les âges peuvent être regroupés en tranches d'âge (20-30 ans, 30-40 ans, etc.) au lieu d'être rapportés individuellement.

Ces techniques s'accompagnent généralement de contrôles d'accès stricts : Seuls les chercheurs et chercheuses autorisés peuvent accéder aux données originales. Les données agrégées sont publiées de manière à minimiser les risques de réidentification.

En général, ces techniques sont appliquées de manière standardisée et suivent des protocoles établis pour garantir la confidentialité des données. Les chercheurs et chercheuses doivent se conformer à ces protocoles et aux réglementations en vigueur pour assurer la protection des données. Veuillez contacter votre Data Manager/Data Steward, DPO ou responsable informatique pour connaitre les bonnes pratiques en vigueur dans votre institution.

Bei zusammengefassten Daten besteht die Anforderung darin, dass diese nicht auf die Originaldaten zurückgeführt werden können dürfen. Wie wird dies (standardmässig) gewährleistet? Tut dies jeder Forscher nach eigenem Ermessen?

Unter einer Zusammenfassung (Aggregierung) von Daten ist die Zusammenführung von Zielkennungen und -attributen zu Mittelwerten und Summen zu verstehen.

Um sicherzustellen, dass von den zusammengefassten (aggregierten) Daten nicht auf die Originaldaten geschlossen werden kann, können mehrere Techniken und Verfahren parallel eingesetzt werden:

1. **Anonymisierung**: Identifizierbare Personendaten werden gelöscht oder so verändert, dass sie nicht mehr mit einer bestimmten Person in Verbindung gebracht werden können.
2. **Aggregation nach Ebenen**: Daten werden auf einer Granularitätsebene zusammengefasst, die hoch genug ist, um eine Re-Identifizierung zu verhindern. Beispielsweise werden anstelle von Einzeldaten Durchschnittswerte oder Gesamtwerte nach Gruppen (z. B. nach Region oder Altersgruppe) gebildet.
3. **Entfernung von eindeutigen Identifikatoren**: Eindeutige Identifikatoren oder direkt identifizierbare Informationen werden vor der Aggregation entfernt. Dazu gehören Namen, Adressen, Telefonnummern usw.
4. **Randomisierung**: Bei dieser Technik wird den Daten vor der Aggregation ein statistisches Rauschen hinzugefügt. Dadurch wird es schwieriger, Einzelpersonen aus den aggregierten Daten zu identifizieren.
5. **Verallgemeinerung**: Daten werden verallgemeinert, um Spezifika zu verringern. Beispielsweise können Altersangaben zu Altersgruppen zusammengefasst werden (20-30 Jahre, 30-40 Jahre usw.), anstatt sie einzeln zu nennen.

Diese Techniken gehen in der Regel mit strengen Zugangskontrollen einher: nur befugte Forscher haben Zugang zu den Originaldaten. Aggregierte Daten werden veröffentlicht, um das Risiko einer Re-Identifizierung zu minimieren.

Diese Techniken werden in der Regel standardisiert eingesetzt und folgen festgelegten Protokollen, um die Vertraulichkeit der Daten zu gewährleisten. Forscher müssen sich an diese Protokolle und die geltenden Datenschutzbestimmungen halten. Data Manager/Data Stewards, DSB und/oder IT-Beauftragte können in der Regel über die institutsspezifischen Verfahren informieren.

Question / Frage 66

Quelles sont les techniques d'anonymisation ? Peut-on mettre en place une démarche qui garantit que les données sont anonymes ? En particulier dans un contexte médical, quels sont les critères à vérifier / les mesures à prendre pour que des données personnelles soient réellement anonymisées, c'est-à-dire ne permettent pas de réidentifier des personnes concernées ? Comment garantir que les données (médicales et générales) restent anonymes dans le temps ? Qui a la responsabilité d'assurer cette garantie ?

- Pour l'anonymisation, voir Question / Frage 63 et Question / Frage 65.
- Pour la responsabilité, voir Question / Frage 6, Question / Frage 8 et Question / Frage 9.

Welche Anonymisierungstechniken gibt es? Kann ein Verfahren eingeführt werden, das garantiert, dass die Daten anonym sind? Welche Kriterien müssen insbesondere in einem medizinischen Kontext überprüft / welche Massnahmen ergriffen werden, damit Personendaten tatsächlich anonymisiert werden, d. h. keine Re-Identifizierung von betroffenen Personen möglich ist? Wie kann sichergestellt werden, dass (medizinische und allgemeine) Daten im Laufe der Zeit anonym bleiben? Wer ist dafür verantwortlich, die Anonymität zu gewährleisten?

- Zur Anonymisierung siehe Question / Frage 63 und Question / Frage 65.
- Zur Haftung siehe Question / Frage 6, Question / Frage 8 und Question / Frage 9.

Question / Frage 67

Des données pseudonymisées peuvent-elles être partagées si la clé de chiffrement est conservée dans l'université ou la haute école ayant mené la recherche initiale ?

Des données sont considérées comme anonymes lorsqu'elles ne permettent pas d'identifier la personne concernée ou uniquement en déployant des efforts disproportionnés. Les données pseudonymisées - c'est-à-dire dont les informations identifiantes ont été remplacées par un pseudonyme (par exemple, remplacement du nom et prénom par un chiffre) - sont considérées comme juridiquement anonymes pour la personne qui les reçoit et qui ne dispose pas de la clé ou la table de correspondance (sous réserve des indications au paragraphe suivant). Si les données sont anonymes, elles ne sont plus personnelles et peuvent donc être partagées.

Pour déterminer si des données sont bien anonymes, l'ensemble des circonstances doivent être prises en compte. Même si une seule donnée ne permet pas d'identifier une personne, la combinaison de différentes données collectées peut permettre de l'identifier : par exemple, dans la liste des patient·e·s d'un hôpital, [ID 8128136, Femme, 42 ans, habite (petit village), traitée pour le SIDA, date d'opération 12.07.2021] ne remplit pas les conditions d'anonymité, car cette personne pourrait être identifiée sans efforts disproportionnés. Il est particulièrement important de vérifier si la combinaison de données peut conduire à l'identification de personnes lorsque des recherches très précises sont effectuées (qui mentionne, par exemple, l'âge ou l'année de naissance au lieu d'utiliser une fourchette d'âge) et lorsqu'une collecte de données est effectuée auprès d'un cercle fermé de personnes (par exemple les collaborateurs et collaboratrices d'une certaine entreprise, les habitant·e·s d'une certaine commune, etc.). Dans ce cas, les cas isolés méritent une attention particulière (personnes particulièrement jeunes ou âgées, nationalités rarement rencontrées dans le pays où se déroule la recherche, etc.). Un risque important de réidentification existe également lorsque des données personnelles publiquement accessibles concernent les mêmes personnes.

Plusieurs méthodes existent pour anonymiser des données ; les chercheurs et chercheuses pourront notamment se référer à la page « Anonymisation des données » proposée par l'EPFL :

https://www.epfl.ch/campus/services/data-protection/fr/en-pratique/le-respect-de-la-vie-privee-dans-la-recherche/anonymisation-des-donnees/.

Dürfen pseudonymisierte Daten bekanntgegeben werden, wenn der Verschlüsselungscode in der Universität oder Hochschule aufbewahrt wird, welche ursprünglich die Forschung durchgeführt hat?

Daten sind anonym, wenn sie nicht oder nur mit unverhältnismässigem Aufwand die Identifizierung einer betroffenen Person ermöglichen. Pseudonymisierte Daten – d. h. Daten, bei denen die identifizierenden Informationen durch ein Pseudonym ersetzt wurden (z. B. Ersetzen des Vor- und Nachnamens durch eine Nummer) – gelten rechtlich als anonym für eine Person, die sie erhält und die weder über den Schlüssel oder die Zuordnungstabelle noch über andere Möglichkeiten zur Re-Identifizierung verfügt (vorbehaltlich der Ausführungen im nächsten Absatz). Wenn Daten anonym sind, sind sie nicht mehr personenbezogen und können daher bekanntgegeben werden.

Um festzustellen, ob Daten tatsächlich anonym sind, müssen alle Umstände berücksichtigt werden. Selbst wenn ein einzelner Datensatz nicht zur Identifizierung einer Person führt, kann die Kombination verschiedener gesammelter Daten eine Identifizierung ermöglichen: Beispielsweise erfüllen die folgenden Daten in der Patientenliste eines Krankenhauses [ID 8128136, weiblich, 42 Jahre, wohnhaft (kleines Dorf), wird wegen AIDS behandelt, Operationsdatum 12.07.2021] nicht die Anforderungen der Anonymität, da diese Person ohne unverhältnismässigen Aufwand identifiziert werden kann. Es ist deshalb besonders wichtig zu prüfen, ob die Kombination von Daten zur Identifizierung von Personen führen kann. Dies kann insbesondere der Fall sein, wenn sehr genaue Abfragen durchgeführt werden (z. B. Angabe des Alters oder des Geburtsjahrgangs anstelle einer Altersspanne) und wenn Daten von einer geschlossenen Gruppe von Personen erhoben werden (z. B. Mitarbeitende eines bestimmten Unternehmens, Einwohner einer bestimmten Gemeinde usw.). In diesem Fall verdienen Einzelfälle besondere Aufmerksamkeit (besonders junge oder alte Personen, Nationalitäten, die in dem Land, in dem die Forschung durchgeführt wird, selten sind usw.). Ein erhebliches Risiko der Re-Identifizierung besteht auch, wenn öffentlich zugängliche Personendaten dieselben Personen betreffen.

Es gibt verschiedene Methoden, um die Anonymisierung der Daten zu gewährleisten; Forschende finden hierzu auf der Seite «Anonymisation des données» der EPFL weitere Informationen: https://www.epfl.ch/campus/services/data-protection/fr/en-pratique/le-respect-de-la-vie-privee-dans-la-recherche/anonymisation-des-donnees/.

Question / Frage 68

Si des données sont pseudonymisées, comment stocker les différentes parties (données anonymisées, table de correspondance et données brutes) ? Dans différents espaces de stockage ?

Lors du stockage de données pseudonymisées, il est essentiel que les différentes parties – données anonymisées, table de référence (clé de correspondance) et données brutes – soient conservées dans des espaces de stockage séparés et sécurisés afin de garantir la protection des données :

- Données anonymisées : Elles doivent être stockées dans un dépôt de données central mais sécurisé.
- Table de référence (clé d'attribution) : La table de référence doit être stockée dans un système de stockage séparé, idéalement dans un endroit accessible uniquement à un nombre très limité de personnes autorisées. Une bonne pratique consiste à la conserver auprès d'une personne fiable n'ayant pas participé à la recherche (par exemple, le délégué à la protection des données de l'établissement) afin de s'assurer que très peu de personnes ont accès à ces informations.
- Données brutes : Les données brutes devraient être protégées par des droits d'accès stricts et un cryptage.

Mesures supplémentaires recommandées :

- Chiffrement : la table de référence et les données brutes devraient être protégées dans les espaces de stockage par un chiffrement fort (par exemple AES-256) afin d'empêcher tout accès non autorisé.
- Séparation des espaces de stockage : au moins deux serveurs différents devraient être utilisés (un pour les données pseudonymisées et un pour la table de référence et les données brutes, avec des droits d'accès différents) et le tableau de référence peut également être stocké hors ligne pour assurer une protection supplémentaire (évaluation de la recherche...).
- Restrictions d'accès : Seul le personnel autorisé qui effectue la pseudonymisation ou la collecte de données devrait avoir accès au tableau de référence et aux données brutes.

Wenn Daten pseudonymisiert werden, wie sollen die verschiedenen Teile (die anonymisierten Daten, die Zuordnungstabelle und die Rohdaten) gespeichert werden? In verschiedenen Speicherbereichen?

Bei der Speicherung pseudonymisierter Daten ist von entscheidender Bedeutung, dass die verschiedenen Teile – die anonymisierten Daten, die Referenztabelle (Matching Keys) und die Rohdaten – in getrennten und gesicherten Speicherbereichen aufbewahrt werden, um den Datenschutz zu gewährleisten:

- Anonymisierte Daten: Sie müssen in einem zentralen, aber gesicherten Datenspeicher abgelegt werden.
- Referenztabelle (Zuordnungsschlüssel): Die Referenztabelle sollte in einem separaten Speichersystem gespeichert werden, idealerweise an einem Ort, zu dem nur eine sehr begrenzte Anzahl befugter Personen Zugang hat. Eine gute Praxis ist es, sie bei einer vertrauenswürdigen Person aufzubewahren, die nicht an der Forschung beteiligt ist (z. B. dem*der Datenschutzbeauftragten der Institution), um sicherzustellen, dass nur sehr wenige Personen Zugang zu diesen Informationen haben.
- Rohdaten: Rohdaten sollten durch strenge Zugriffsrechte und Verschlüsselung geschützt werden.

Zusätzlich werden folgende Massnahmen empfohlen:

- Verschlüsselung: Die Daten sollten in Speicherbereichen durch eine starke Verschlüsselung (z. B. AES-256) vor unbefugtem Zugriff geschützt werden.
- Getrennte Speicherbereiche: Es sollten mindestens zwei verschiedene Server verwendet werden (einen für die pseudonymisierten Daten und einen für die Referenztabelle und die Rohdaten, mit unterschiedlichen Zugriffsrechten), und die Referenztabelle kann zudem offline gespeichert werden, um zusätzlichen Schutz zu gewährleisten (Forschungsevaluierung usw.).
- Zugriffsbeschränkungen: Nur autorisierte Personen, welche die Pseudonymisierung oder die Datenerhebung durchführen, sollten Zugriff auf die Referenztabelle und auf die Rohdaten haben.

Question / Frage 69

Quel niveau précis d'anonymisation est-il attendu suivant chaque type de données ? La question se pose, par exemple, pour les données de la recherche en médecine où une radio ou un scanner peuvent permettre d'identifier la personne.

Des données sont considérées comme anonymes lorsqu'elles ne permettent pas d'identifier la personne concernée ou uniquement en déployant des efforts disproportionnés.

Pour déterminer si des données sont bien anonymes, l'ensemble des circonstances doivent être prises en compte. Même si une seule donnée ne permet pas d'identifier une personne, la combinaison de différentes données collectées peut permettre de l'identifier : par exemple, dans la liste des patient·e·s d'un hôpital, [ID 8128136, Femme, 42 ans, habite (petit village), traitée pour le SIDA, date d'opération 12.07.2021] ne remplit pas les conditions d'anonymité, car cette personne pourrait être identifiée sans efforts disproportionnés. Il est particulièrement important de vérifier si la combinaison de données peut conduire à l'identification de personnes lorsque des recherches très précises sont effectuées (qui mentionne, par exemple, l'âge ou l'année de naissance au lieu d'utiliser une fourchette d'âge) et lorsqu'une collecte de données est effectuée auprès d'un cercle fermé de personnes (par exemple les collaborateurs et collaboratrices d'une certaine entreprise, les habitant·e·s d'une

certaine commune, etc.). Dans ce cas, les cas isolés méritent une attention particulière (personnes particulièrement jeunes ou âgées, nationalités rarement rencontrées dans le pays où se déroule la recherche, etc.). Un risque important de réidentification existe également lorsque des données personnelles publiquement accessibles concernent les mêmes personnes.

Plusieurs méthodes existent pour anonymiser des données ; les chercheurs et chercheuses pourront notamment se référer à la page « Anonymisation des données » proposée par l'EPFL : https://www.epfl.ch/campus/services/data-protection/fr/en-pratique/le-respect-de-la-vie-privee-dans-la-recherche/anonymisation-des-donnees/.

En matière d'imagerie médicale, les principes suivants devraient être suivis :

- Suppression des métadonnées : élimination des informations intégrées dans les fichiers d'images qui pourraient identifier le/la patient.e.
- Masquage des zones identifiables : floutage ou suppression des parties de l'image qui pourraient permettre l'identification (par exemple, les parties du visage sur une radiographie).

Welches Mass an Anonymisierung wird je nach Art der Daten erwartet? Diese Frage stellt sich zum Beispiel bei medizinischen Forschungsdaten, bei denen ein Röntgenbild oder ein CT-Scan die Person identifizieren kann.

Daten gelten als anonym, wenn sie nicht oder nur mit unverhältnismässigem Aufwand die Identifizierung einer betroffenen Person ermöglichen

Um festzustellen, ob Daten tatsächlich anonym sind, müssen alle Umstände berücksichtigt werden. Selbst wenn ein einzelner Datensatz nicht zur Identifizierung einer Person führt, kann die Kombination verschiedener gesammelter Daten eine Identifizierung ermöglichen: Beispielsweise erfüllen die folgenden Daten in der Patientenliste eines Krankenhauses [ID 8128136, weiblich, 42 Jahre, wohnhaft (kleines Dorf), wird wegen AIDS behandelt, Operationsdatum 12.07.2021] nicht die Anforderungen der Anonymität, da diese Person ohne unverhältnismässigen Aufwand identifiziert werden kann. Es ist deshalb besonders wichtig zu prüfen, ob die Kombination von Daten zur Identifizierung von Personen führen kann. Dies kann insbesondere der Fall sein, wenn sehr genaue Abfragen durchgeführt werden (z. B. Angabe des Alters oder des Geburtsjahrgangs anstelle einer Altersspanne) und wenn Daten von einer geschlossenen Gruppe von Personen erhoben werden (z. B. Mitarbeitende eines bestimmten Unternehmens, Einwohner einer bestimmten Gemeinde usw.). In diesem Fall verdienen Einzelfälle besondere Aufmerksamkeit (besonders junge oder alte Personen, Nationalitäten, die in dem Land, in dem die Forschung durchgeführt wird, selten sind usw.). Ein erhebliches Risiko der Re-Identifizierung besteht auch, wenn öffentlich zugängliche Personendaten dieselben Personen betreffen.

Es gibt verschiedene Methoden, um die Anonymisierung der Daten zu gewährleisten; Forschende finden hierzu auf der Seite «Anonymisation des données» der EPFL weitere Informationen: https://www.epfl.ch/campus/services/data-protection/fr/en-pratique/le-respect-de-la-vie-privee-dans-la-recherche/anonymisation-des-donnees/.

Im Zusammenhang mit der medizinischen Bildgebung sollten die folgenden Grundsätze befolgt werden:

- Löschung der Metadaten: Entfernung von in Bilddateien eingebetteten Informationen, die eine Identifizierung des Patienten ermöglichen.
- Ausblenden identifizierbarer Bereiche: Unkenntlichmachung oder Entfernung von Bildteilen, die eine Identifizierung ermöglichen könnten (z. B. Gesichtsteile auf einem Röntgenbild).

Question / Frage 70

Si des données personnelles (voire sensibles) sont pseudonymisées et que la table de correspondance est conservée exclusivement au sein d'une haute école, peuvent-elles être considérées comme anonymisées lorsqu'elles sont transmises et traitées par d'autres hautes écoles ?

La réponse a été donnée (en allemand) par privatim, la Conférence des Préposé·e·s suisses à la protection des données.

Oui et non. Une véritable « anonymisation » signifie qu'il n'y a plus de possibilité d'attribution à qui que ce soit, au sens de l'ATF 136 II 508 consid. 3.2 : « Toute possibilité théorique d'identification ne suffit toutefois pas à l'identification. Si l'effort à fournir est tel qu'il ne faut pas s'attendre, selon l'expérience générale de la vie, à ce qu'une personne intéressée s'en charge, il n'y a pas de déterminabilité (FF 1988 II 444 s. ch. 221.1). La réponse à cette question doit être donnée en fonction du cas concret, en tenant compte notamment des possibilités offertes par la technique, comme par exemple les outils de recherche disponibles sur Internet. Ce qui importe, ce n'est pas seulement l'effort objectivement nécessaire pour pouvoir attribuer une information déterminée à une personne, mais aussi l'intérêt que le responsable du traitement des données ou un tiers a à l'identifier ».

Le même critère doit être appliqué à la question de savoir si les données ont été efficacement pseudonymisées avant leur transmission. C'est le cas lorsque les destinataires n'ont pas accès à la clé d'attribution qui continue d'exister et qu'ils ne peuvent pas établir l'identifiabilité d'une autre manière moyennant des efforts raisonnables.

Le « oui » dans la réponse signifie que les données efficacement pseudonymisées peuvent être traitées par les destinataires comme des données anonymes. De leur point de vue, ce ne sont pas des données personnelles et ils peuvent en principe les traiter librement. Il y a toutefois une exception : s'ils transmettent les données (par ex. enrichies des résultats de leur propre activité) à la haute école d'origine ou à d'autres tiers qui ont accès à la clé de répartition, cette transmission est considérée comme une communication de données personnelles selon la pratique du Tribunal fédéral, cf. ATF 136 II 508 consid. 3.4 : « En cas de transmission d'informations, il suffit à cet égard que le destinataire soit en mesure d'identifier la personne concernée ».

Voir aussi la réponse donnée à la Question / Frage 63.

Wenn persönliche (oder sogar besonders schützenswerte) Daten pseudonymisiert werden und die Zuordnungstabelle ausschliesslich innerhalb einer Hochschule aufbewahrt wird, können diese Daten dann als anonymisiert betrachtet werden, wenn sie an andere Hochschulen übermittelt und dort bearbeitet werden?

Die Antwort wurde von privatim, der Konferenz der Schweizer Datenschutzbeauftragten, zur Verfügung gestellt:

Jein. Eine echte «Anonymisierung» bedeutet, dass für niemanden mehr eine Zuordnungsmöglichkeit mehr besteht, im Sinne von BGE 136 II 508 E. 3.2: „Für die Bestimmbarkeit genügt jedoch nicht jede theoretische Möglichkeit der Identifizierung. Ist der Aufwand derart gross, dass nach der allgemeinen Lebenserfahrung nicht damit gerechnet werden muss, dass ein Interessent diesen auf sich nehmen wird, liegt keine Bestimmbarkeit vor (BBl 1988 II 444 f. Ziff. 221.1). Die Frage ist abhängig vom konkreten Fall zu beantworten, wobei insbesondere auch die Möglichkeiten der Technik mitzuberücksichtigen sind, so zum Beispiel die im Internet verfügbaren Suchwerkzeuge. Von Bedeutung ist indessen nicht nur, welcher Aufwand objektiv erforderlich ist, um eine bestimmte Information einer Person zuordnen zu können, sondern auch, welches Interesse der Datenbearbeiter oder ein Dritter an der Identifizierung hat».

Der gleiche Massstab ist auch anzuwenden auf die Frage, ob die Daten vor der Weitergabe wirksam pseudonymisiert wurden. Dies ist dann der Fall, wenn die Empfänger weder Zugang zum nach wie vor existenten Zuordnungsschlüssel haben noch mit zumutbarem Aufwand auf anderem Weg die Bestimmbarkeit herstellen können.

Das «J» in der Antwort bedeutet, dass wirksam pseudonymisierte Daten von den Empfängern wie anonyme Daten bearbeitet werden können. Aus ihrer Sicht sind es keine Personendaten und sie können diese grundsätzlich frei bearbeiten. Es gibt jedoch eine Ausnahme: Falls sie die Daten (z.B. angereichert mit den Ergebnissen ihrer eigenen Tätigkeit) an die ursprüngliche Hochschule oder andere Dritte übermitteln, die Zugang zum Zuordnungsschlüssel haben, gilt diese Übermittlung nach der Praxis des Bundesgerichts als Bekanntgabe von Personendaten, vgl. BGE 136 II 508 E. 3.4: «Im Falle der Weitergabe von Informationen ist dabei ausreichend, wenn der Empfänger die betroffene Person zu identifizieren vermag»).

Siehe hierzu auch die Antwort auf Question / Frage 63.

Question / Frage 71

Est-ce que des données pseudonymisées, qui ont été traitées dans le cadre de recherches menées par une haute école suisse, sont considérées comme des données personnelles si elles sont partagées dans un data repository (par conséquent sans une clé d'identification) ? Si oui, qu'est-ce que cela signifie juridiquement ? La réponse est-elle identique si les données sont soumises à la LRH ?

Voir la réponse donnée à la Question / Frage 63.

Werden pseudonymisierte Daten, die im Rahmen von Forschungsarbeiten an einer Schweizer Hochschule bearbeitet werden, als Personendaten betrachtet, wenn sie in einem Repositorium (also ohne einen Identifikationsschlüssel) veröffentlicht werden? Wenn ja, was bedeutet dies rechtlich gesehen? Ist die Antwort dieselbe, wenn die Daten dem Humanforschungsgesetz unterliegen?

Siehe hierzu die Antwort auf Question / Frage 63.

XI. Secret de fonction / Amtsgeheimnis

Question / Frage 72

Est-ce que tous les cas où aucun secret spécifique n'est applicable sont « par défaut » couverts par le secret de fonction ? En d'autres termes, est-ce que les données de recherche comportant des données personnelles collectées par des chercheurs et chercheuses d'une haute école dans le cadre de leurs projets sont soumises au secret de fonction (ce qui aurait des conséquences importantes en matière de partage) ? Concernant la portée du secret de fonction, est-il possible d'appliquer une méthode autre qu'une appréciation qu'au cas par cas ?

Les membres du personnel des hautes écoles et des universités sont des fonctionnaires soumis au secret de fonction au sens de l'art. 320 du Code pénal suisse (CP). Le secret porte sur toutes les informations apprises dans la fonction, qui ne doivent pas être connues ou qui ne sont pas accessibles au public, et qui doivent être gardées secrètes en raison d'un intérêt légitime, privé ou public. S'il n'existe pas d'intérêt légitime à garder des données personnelles confidentielles, le secret de fonction ne s'oppose pas à la divulgation.

Les informations qui peuvent être communiquées sur la base des lois sur la transparence ne tombent pas sous le secret de fonction.

L'analyse de l'intérêt légitime doit tenir compte des circonstances des données concernées, de sorte qu'un examen au cas par cas est recommandé.

Par ailleurs, les règles cantonales définissent les conditions de levée du secret de fonction. Une procédure de levée du secret de fonction doit être initiée avant toute divulgation et l'autorisation ou le refus de la levée du secret de fonction est objet d'une décision formelle.

Wenn keine spezifische Geheimhaltungspflicht zur Anwendung kommt, findet dann «standardmässig» das Amtsgeheimnis Anwendung? Mit anderen Worten: fallen Forschungsdaten mit Personendaten, die von Forschern einer Hochschule im Rahmen ihrer Projekte gesammelt werden, unter das Amtsgeheimnis (was erhebliche Konsequenzen für die Bekanntgabe hätte)? Ist es in Bezug auf den Umfang des Amtsgeheimnisses möglich, eine andere Methode als eine Einzelfallbeurteilung anzuwenden?

Das Hochschul- und Universitätspersonal untersteht dem Amtsgeheimnis nach Art. 320 StGB. Das Amtsgeheimnis bezieht sich auf alle in Ausübung des Amtes bekannt gewordenen Tatsachen, die nicht bekannt werden dürfen oder der Öffentlichkeit nicht zugänglich sind und wegen eines berechtigten privaten oder öffentlichen Interesses geheim gehalten werden müssen. Liegt kein berechtigtes Interesse an der Geheimhaltung von Personendaten vor, steht das Amtsgeheimnis einer Offenbarung nicht entgegen.

Nicht unter das Amtsgeheimnis fallen Informationen, die nach dem Öffentlichkeitsprinzip bekannt gegeben werden dürfen.

Bei der Prüfung des berechtigten Interesses sind die Umstände der betreffenden Daten zu berücksichtigen, so dass sich eine Einzelfallprüfung jedenfalls empfiehlt.

Im Übrigen legen die kantonalen Vorschriften die Bedingungen für die Aufhebung des Amtsgeheimnisses fest. Ein entsprechendes Verfahren zur Aufhebung des Amtsgeheimnisses, muss vor jeder Offenlegung eingeleitet werden, und die Genehmigung oder Verweigerung zur Aufhebung des Amtsgeheimnisses ist Gegenstand einer formellen Entscheidung.

XII. Archives / Archivierung

Question / Frage 73

Est-il possible d'archiver des données dans des dépôts de données (conformément à la Loi sur l'archivage) ?

Il convient de distinguer l'archivage au sens juridique du dépôt durable dans des dépôts ou référentiels (repositories) :

- L'archivage est régi par la Loi fédérale sur l'archivage (LAr) ou par l'une des lois cantonales sur l'archivage. Cet archivage s'effectue par le transfert d'informations dignes d'être archivées aux Archives nationales ou cantonales, ou à un service chargé de l'archivage (Archives universitaires).
- En revanche, le dépôt durable dans des repositories est un stockage des données. En principe, les données de recherche peuvent être mises à disposition de manière durable dans les dépôts. L'obligation de proposer les données aux archives d'État ou aux archives universitaires doit être évaluée séparément (voir à ce sujet la Question / Frage 76).

Ist es möglich, Daten in Repositorien zu archivieren (gemäss dem Archivierungsgesetz)?

Die Archivierung im rechtlichen Sinne ist zu unterscheiden von der dauerhaften Aufbewahrung von Forschungsdaten in Repositorien:

- Die Archivierung ist im Bundesgesetz über die Archivierung oder in einem der kantonalen Archivierungsgesetze geregelt. Die Archivierung erfolgt durch die Übergabe der archivwürdigen Informationen an das nationale oder kantonale Archiv oder an eine mit der Archivierung beauftragte Stelle (bspw. Universitätsarchiv).
- Im Gegensatz dazu handelt es sich bei der dauerhaften Ablage in Repositorien um die Speicherung von Daten. Grundsätzlich können Forschungsdaten in Repositorien dauerhaft verfügbar gemacht werden. Ob die Daten dem Staatsarchiv oder dem Universitätsarchiv angeboten werden sollen, ist gesondert zu beurteilen (siehe dazu auch Question / Frage 76).

Question / Frage 74

La responsabilité des données change-t-elle avec la remise du processus et des données aux archives de l'État ?

Le transfert de données aux Archives d'État implique également le transfert de la responsabilité des données aux Archives d'État ; les Archives d'État doivent assumer la responsabilité de la communication de données et les informations dignes de protection (p. ex. les données personnelles) restent en général sous clé.

En règle générale, il n'est pas prévu d'archiver les données de recherche. Si des données de recherche sont néanmoins proposées, les informations sensibles (données personnelles sensibles) doivent être signalées.

Ändert sich die Verantwortung für die Daten mit der Übergabe des Prozesses und der Daten an das Staatsarchiv?

Mit der Übergabe von Daten an das Staatsarchiv geht auch die Verantwortung für diese Daten an das Staatsarchiv über; das Staatsarchiv muss die Verantwortung für die übergebenen Daten übernehmen und schutzwürdige Informationen (z.B. Personendaten) bleiben in der Regel unter Verschluss.

Eine Archivierung von Forschungsdaten ist in der Regel nicht vorgesehen. Wenn Forschungsdaten dennoch angeboten werden, müssen sensible Informationen (besonders schützenswerte Personendaten) gekennzeichnet werden.

Question / Frage 75

Qu'entend-on par « archives » au sens juridique du terme ? Comment le terme est-il utilisé dans le domaine de la recherche, notamment dans le contexte des dépôts ?

Sur cette problématique, voir Question / Frage 73.

Was versteht man unter "Archiven" im rechtlichen Sinne? Wie wird der Begriff in der Forschung verwendet, insbesondere im Zusammenhang mit Datenablagen?

Zu dieser Problematik siehe Question / Frage 73.

Question / Frage 76

Dans quelle mesure les résultats de la recherche doivent-ils être confiés aux archives d'État ?

Les hautes écoles et universités suisses sont en principes tenues, en vertu des lois sur l'archivage qui s'appliquent à elles (Loi fédérale sur l'archivage pour les écoles fédérales ; lois cantonales pour les hautes écoles cantonales (universités, hautes écoles spécialisées et hautes écoles pédagogiques)) de proposer aux archives les documents dont elles n'ont plus l'utilité. En général, les archives décident ensuite si les documents présentent un intérêt et doivent être archivés.

Même si les données de recherche elles-mêmes ne seront pas forcément considérées comme dignes d'être archivées, elles doivent quand même être proposées aux archives.

In welchem Umfang sollten die Forschungsergebnisse den Staatsarchiven angeboten werden?

Die Schweizer Hochschulen und Universitäten sind aufgrund der für sie geltenden Archivierungsgesetze (Bundesgesetz über die Archivierung der Eidgenössischen Hochschulen; kantonale Gesetze für die kantonalen Hochschulen (Universitäten, Fachhochschulen und Pädagogischen Hochschulen)) grundsätzlich verpflichtet, ihre nicht mehr benötigten Unterlagen den Archiven anzubieten. Die Archive entscheiden dann in der Regel, ob die Unterlagen von Interesse sind und archiviert werden sollen.

Auch wenn Forschungsdaten selbst nicht zwingend als archivwürdig gelten, sollten sie dennoch den Archiven angeboten werden.

XIII. Durée de conservation et destruction des données / Speicherdauer und Datenvernichtung

Question / Frage 77

Combien de temps puis-je conserver des données personnelles ?

Sauf obligation légale, les données personnelles ne doivent pas être conservées plus longtemps que nécessaire pour atteindre le but visé. Il n'est pas possible d'indiquer, dans l'absolu, la durée pendant laquelle les données doivent être conservées. Cette durée va dépendre des circonstances du cas d'espèce et doit répondre au principe de proportionnalité : ainsi, les données personnelles doivent être détruites ou anonymisées dès qu'elles ne sont plus nécessaires pour le traitement. Dans certains cas, la loi peut fixer un délai de conservation (voir par exemple art. 45 de l'Ordonnance sur les essais cliniques hors essais cliniques de dispositifs médicaux, qui fixe un délai de conservation de 10 ans au promoteur et à l'investigateur de l'essai clinique).

Wie lange dürfen Personendaten aufbewahrt werden?

Sofern keine gesetzliche Verpflichtung besteht, dürfen Personendaten nicht länger aufbewahrt werden, als es zur Erreichung des Zwecks erforderlich ist. Wie lange Daten aufbewahrt werden müssen, kann nicht absolut gesagt werden. Die Dauer hängt von den Umständen des Einzelfalls ab und muss dem Grundsatz der Verhältnismässigkeit entsprechen: So müssen Personendaten vernichtet oder anonymisiert werden, sobald sie für die Bearbeitung nicht mehr erforderlich sind. In bestimmten Fällen kann das Gesetz indes eine Aufbewahrungsfrist vorsehen (siehe z.B. Art. 45 der Verordnung über klinische Versuche mit Ausnahme von klinischen Versuchen mit Medizinprodukten, der eine Aufbewahrungsfrist von 10 Jahren für den Sponsor und die Studienleitung des klinischen Versuchs vorsieht).

Question / Frage 78

Dans quelles conditions un délai de rétention exprimé sans une fin déterminée (qui reviendrait à conserver les données personnelles « tant qu'elles représentent un intérêt pour la recherche scientifique ») est-il acceptable ?

Une période de conservation sans objectif spécifique, qui conduit à la conservation à long terme de données à caractère personnel, n'est acceptable dans la recherche scientifique que dans certaines conditions :

- La conservation devrait être réglementée sur la base des politiques d'archivage institutionnelles et des déclarations de consentement avec les personnes concernées.
- Une fois un projet de recherche terminé, il convient de procéder à une évaluation minutieuse des données afin de déterminer les besoins ultérieurs. Cette évaluation peut être répétée après une période donnée (par exemple 10 ans) afin de vérifier la pertinence des données.
- L'anonymisation doit être régulièrement vérifiée et, le cas échéant, mise à jour.

Unter welchen Bedingungen ist eine Speicherfrist, die ohne ein bestimmtes Ende festgelegt wird (was darauf hinauslaufen würde, dass Personendaten so lange gespeichert werden, «wie sie für die wissenschaftliche Forschung von Interesse sind»), akzeptabel?

Eine Aufbewahrungsfrist ohne Zweckbindung, die zu einer langfristigen Speicherung von Personendaten führt, ist in der wissenschaftlichen Forschung nur unter bestimmten Bedingungen akzeptabel:

- Die Aufbewahrung ist auf der Grundlage von institutionellen Archivierungsrichtlinien und Einverständniserklärungen mit den betroffenen Personen geregelt.
- Nach Abschluss eines Forschungsprojekts wird eine sorgfältige Evaluierung der Daten durchgeführt, um den weiteren Bedarf zu ermitteln. Diese Bewertung kann nach einem bestimmten Zeitraum (z.B. 10 Jahre) wiederholt werden, um die Relevanz der Daten zu überprüfen.

- Die Anonymisierung wird regelmässig überprüft und gegebenenfalls aktualisiert.

Question / Frage 79

Quelles sont les mesures techniques pour garantir la destruction des données ?

Comme cela ressort de l'article 6 al. 4 de la Loi fédérale sur la protection des données (LPD), les données personnelles n'ont pas pour vocation à être conservées sans aucune limite de temps. Leur durée de conservation doit être définie et des mécanismes pour la destruction définitive de ces données doivent être établis. Ainsi, il ne suffit pas d'effacer simplement ses données d'un disque dur pour considérer qu'elles sont détruites. Il faut véritablement s'assurer qu'elles ne seront plus jamais accessibles. Il en va de même pour les données qui sont contenues sur papier ou sur des supports mobiles. Les copies de sauvegardes doivent également être détruites (Guide relatif aux mesures techniques et organisationnelles de la protection des données [TOM] du Préposé fédéral à la protection des données et à la transparence - PFPDT).

Mesures à envisager :

- Définir une stratégie de suppression de manière appropriée pour assurer une destruction graduelle et complète des données personnelles, y compris dans les sauvegardes après la fin de leur utilité.
- Effacer les données à l'aide de programmes spéciaux qui garantissent un effacement total et définitif des données (en nettoyant les espaces vides, par exemple).
- Les données papier sont détruites par une déchiqueteuse de papiers.
- Les CD-ROM et autres supports mobiles sont également détruits physiquement s'ils ne peuvent pas être complètement nettoyés d'une autre manière.

Welche technischen Massnahmen gibt es, um die Vernichtung von Daten zu gewährleisten?

Wie aus Art. 6 Abs. 4 des Bundesgesetzes über den Datenschutz hervorgeht, sind Personendaten nicht dazu bestimmt, unbefristet aufbewahrt zu werden. Ihre Aufbewahrungsdauer muss festgelegt und es müssen Mechanismen für ihre endgültige Vernichtung geschaffen werden. Es reicht also nicht aus, die Daten einfach von einer Festplatte zu löschen, damit sie als vernichtet gelten. Es muss tatsächlich sichergestellt sein, dass sie nie wieder zugänglich sind. Gleiches gilt für Daten, die auf Papier oder mobilen Datenträgern gespeichert sind. Sicherungskopien sind ebenfalls zu vernichten (siehe hierzu den Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes [TOM] des EDÖB).

Massnahmen sind:

- Erarbeiten einer Löschstrategie, die eine schrittweise und vollständige Vernichtung der Personendaten, einschliesslich der Sicherungskopien, nach Ablauf ihrer Zweckbestimmung sicherstellt.
- Löschen der Daten mit speziellen Programmen, die eine vollständige und endgültige Löschung gewährleisten (z. B. durch Löschen von Leerzeichen).
- Vernichtung von Papierdaten durch einen Aktenvernichter.
- Vernichtung von CD-ROMs und anderen Datenträgern ebenfalls physikalisch, wenn sie nicht auf andere Weise vollständig gelöscht werden können.

Question / Frage 80

Qui devrait prendre la décision de détruire des données ou de lever un embargo ? Si, par exemple, des données ont été déposées sous embargo pour 20 ans et que les chercheurs et chercheuses en charge ne travaillent plus dans la haute école ou l'université, sont décédés ou retraités, qui doit prendre cette décision et en assumer la responsabilité ?

Du point de vue juridique, la haute école ou l'université est responsable du traitement des données personnelles et donc responsable de respecter les règles en matière de protection des données et de sécurité de l'information.

En pratique, l'institution doit veiller à ce que son personnel connaisse et applique les exigences légales dans ce domaine. Les chercheurs et chercheuses responsables d'un projet doivent s'assurer que leur recherche respecte la protection des données, en suivant notamment les éventuelles instructions ou lignes directrices de l'institution. De plus, les collaborateurs et collaboratrices sont soumis au secret de fonction à titre individuel.

Il est recommandé d'établir un processus interne permettant de définir à l'avance qui prendra les décisions relatives aux données personnelles en cas de changement dans le personnel.

En outre, il convient de distinguer la problématique de l'embargo de celle de la destruction des données :

- Un embargo ne devrait pas être levé tant que des données personnelles sont contenues dans les données de recherche, étant donné que la protection des données ne prend fin qu'avec le décès d'une personne et qu'ensuite (post mortem), le droit général de la personnalité s'applique toujours. Dans ce sens, les anonymisations devraient être effectuées avant la levée d'un embargo.
- Les données personnelles doivent être supprimées lorsqu'elles ne sont plus nécessaires à la traçabilité des résultats de la recherche (pas de nécessité) ; toutes les autres données doivent être définitivement supprimées lorsqu'on peut supposer qu'elles ne sont plus pertinentes.

Wer muss die Entscheidung über die Vernichtung von Daten oder die Aufhebung eines Embargos treffen? Wenn beispielsweise Daten für 20 Jahre mit einem Embargo versehen wurden und die verantwortlichen Forschenden nicht mehr an der Hochschule oder Universität arbeiten, verstorben oder pensioniert sind, wer sollte diese Entscheidung treffen und die Verantwortung dafür übernehmen?

Aus rechtlicher Sicht ist die Hochschule für die Bearbeitung von Personendaten und damit für die Einhaltung der Datenschutz- und Informationssicherheitsvorschriften verantwortlich.

In der Praxis muss die Institution sicherstellen, dass ihre Mitarbeitenden die rechtlichen Anforderungen in diesem Bereich kennen und anwenden. Die für ein Projekt verantwortlichen Forschenden müssen dann sicherstellen, dass bei ihrer Forschung der Datenschutz eingehalten wird, indem sie insbesondere etwaige Anweisungen oder Richtlinien der Institution befolgen. Darüber hinaus sind die Mitarbeitenden individuell an das Amtsgeheimnis gebunden.

Es wird empfohlen, ein internes Verfahren einzurichten, das im Voraus festlegt, wer bei Personalwechseln über Personendaten entscheidet.

Darüber hinaus ist die Sperrfristproblematik von der Problematik der Datenvernichtung zu unterscheiden:

- Eine Sperrfrist (Embargo) sollte nicht aufgehoben werden, solange Personendaten in den Forschungsdaten enthalten sind, da der Datenschutz erst mit dem Tod einer Person endet und auch danach (post mortem) das allgemeine Persönlichkeitsrecht gilt. Insofern muss vor der Aufhebung einer Sperrfrist eine Anonymisierung erfolgen.
- Personendaten müssen gelöscht werden, wenn sie für die Nachvollziehbarkeit der Forschungsergebnisse nicht mehr erforderlich sind (no need); alle anderen Daten sind endgültig zu löschen, wenn davon auszugehen ist, dass sie nicht mehr relevant sind.

Question / Frage 81

Combien de temps les données de recherche confidentielles (par exemple, les données personnelles et leur cryptage ; les déclarations de consentement), qui sont encore disponibles dans une haute école ou une université en plus des données de recherche ouvertes, doivent-elles rester disponibles ?

La durée de conservation des données personnelles va dépendre des circonstances du cas d'espèce et doit répondre au principe de proportionnalité, qui implique que le traitement de données personnelles doit se limiter à ce qui est nécessaire : ainsi, les données personnelles doivent être détruites ou anonymisées dès qu'elles ne sont plus nécessaires pour le traitement. Dans certains cas, la loi peut fixer un délai de conservation (voir par exemple art. 45 de l'Ordonnance sur les essais cliniques hors essais cliniques de dispositifs médicaux, qui fixe un délai de conservation de 10 ans au promoteur et à l'investigateur de l'essai clinique).

Il convient de se référer aux règles internes de la haute école ou de l'université en matière de conservation et d'archivage.

Dans la mesure où des données de recherche publiées sont concernées, il faut tenir compte des exigences spécifiques à la recherche en matière de disponibilité des données (thème de la « traçabilité » des résultats de recherche). Les données personnelles doivent être supprimées dès qu'elles ne sont plus nécessaires à la traçabilité des résultats de la recherche. Cela peut déjà être le cas lorsque les données de recherche sont rendues anonymes. En règle générale, les données liées à une publication (même lorsqu'elles sont anonymes et donc plus personnelles) doivent être disponibles aussi longtemps que la publication elle-même.

Wie lange müssen vertrauliche Forschungsdaten (z. B. Personendaten und deren Verschlüsselung; Einwilligungserklärungen), die an einer Hochschule oder Universität zusätzlich zu den veröffentlichten Forschungsdaten noch verfügbar sind, verfügbar bleiben?

Die Dauer der Aufbewahrung von Personendaten hängt von den Umständen des Einzelfalls ab und muss dem Grundsatz der Verhältnismässigkeit im Sinne der Erforderlichkeit entsprechen: Personendaten sind zu vernichten oder zu anonymisieren, sobald sie für die Bearbeitung nicht mehr notwendig sind. In einigen Fällen kann das Gesetz eine Aufbewahrungsfrist vorsehen (siehe z.B. Art. 45 der Verordnung über klinische Versuche mit Ausnahme von klinischen Versuchen mit Medizinprodukten, der eine Aufbewahrungsfrist von 10 Jahren für den Sponsor und den Prüfer des klinischen Versuchs vorsieht).

Es sei zudem auf die internen Regelungen der Hochschule oder Universität zur Aufbewahrung und Archivierung verwiesen werden.

Soweit publizierte Forschungsdaten betroffen sind, sind zudem die forschungsspezifischen Anforderungen an die Verfügbarkeit der Daten zu berücksichtigen (Thema «Nachvollziehbarkeit» von Forschungsergebnissen). Personendaten sind zu löschen, sobald sie für die Nachvollziehbarkeit von Forschungsergebnissen nicht mehr erforderlich sind. Dies kann bereits bei der Anonymisierung der Forschungsdaten der Fall sein. Generell gilt, dass Daten, die im Zusammenhang mit einer Publikation stehen (auch wenn sie anonymisiert und damit nicht mehr personenbezogen sind), so lange verfügbar sein müssen, wie die Publikation selbst verfügbar ist.

Question / Frage 82

Pour combien d'années devons-nous garantir qu'un fichier soit ouvrable et lisible ? Qui doit se charger de maintenir les fichiers accessibles (ouvrables et lisibles) ? Qu'en est-il des logiciels pour que ces fichiers soient ouvrables ?

- S’agissant de la responsabilité, voir Question / Frage 6, Question / Frage 8 et Question / Frage 9.

- S’agissant des formats de documents, l'EPFL a publié un guide sur la gestion des données de recherche, qui liste (notamment) les formats appropriés pour que les données puissent rester lisibles (https://zenodo.org/records/3327830#.Y9eLyy9XaZB).

Für wie viele Jahre muss garantiert sein, dass eine Datei geöffnet und lesbar ist? Wer muss sich darum kümmern, dass die Dateien zugänglich (zu öffnen und lesbar) bleiben? Was ist mit der Software, die notwendig ist, damit diese Dateien geöffnet werden können?

- Zur Haftung siehe Question / Frage 6, Question / Frage 8 und Question / Frage 9.
- Bezüglich der Dokumentenformate hat die EPFL einen Leitfaden zur Verwaltung von Forschungsdaten veröffentlicht, der (unter anderem) geeignete Formate auflistet, damit die Daten lesbar bleiben (siehe https://zenodo.org/records/3327830#.Y9eLyy9XaZB).

Question / Frage 83

Est-ce que le devoir d’information pour chaque communication ne s’applique plus si l’on a un consentement pour le partage des données en ORD ?

Les lois sur la protection des données (Loi fédérale sur la protection des données (LPD) applicable aux hautes écoles fédérales et lois cantonales applicables aux hautes écoles cantonales (universités, hautes écoles spécialisées et hautes écoles pédagogiques)) prévoient généralement un devoir d'information, qui requiert d'informer les personnes concernées sur « les destinataires ou les catégories de destinataires auxquels des données personnelles sont transmises ».

En cas de partage de données en ORD, il est donc suffisant d'informer les personnes concernées des catégories de destinataires (par exemple, « les données personnelles peuvent être transmises à des autres institutions ou à des entreprises privées pour des projets de recherche nationaux et internationaux »). Il n'y a pas d'obligation d'informer pour chaque téléchargement.

Le consentement doit porter sur le libre accès aux données et leur réutilisation - c'est-à-dire que la personne concernée doit accepter que ses données personnelles soient rendues librement accessibles et puissent être utilisées par des tiers.

Il existe généralement des exceptions au devoir d'informer dans les lois de protection des données, par exemple si l'information est impossible à donner ou nécessiterait des efforts disproportionnés. Ces exceptions sont susceptibles de s'appliquer lorsque les données de contact de personnes ne sont pas disponibles ; dans chaque situation concrète, il convient toutefois de vérifier dans la loi applicable si une telle exception existe et si ses conditions peuvent être considérées comme remplies.

Lorsque la Loi fédérale relative à la recherche sur l’être humain (LRH) s’applique, il convient en outre de vérifier si les exigences de cette loi sont également remplies en cas de réutilisation des données.

Gilt die Pflicht zur Information für jede Bekanntgaben von Personendaten nicht mehr, wenn eine Einwilligung zur Weiterverwendung von Daten im Rahmen von ORD vorliegt?

Die Datenschutzgesetze (das für die Eidgenössischen Hochschulen geltende Bundesgesetz über den Datenschutz und die für die kantonalen Hochschulen (Universitäten, Fachhochschulen und Pädagogischen Hochschulen) geltenden kantonalen Gesetze) sehen in der Regel eine Informationspflicht vor, die verlangt, dass die betroffenen Personen über die «Empfänger oder Kategorien von Empfängern, an die Personendaten bekannt gegeben werden» informiert werden.

Bei der Bekanntgabe von Daten im Rahmen von ORD reicht es daher aus, die betroffenen Personen über die Kategorien von Empfängern zu informieren (z. B. «Personendaten können an andere Institutionen oder private Unternehmen für nationale und internationale Forschungsprojekte bekanntgegeben werden»). Eine Informationspflicht für jeden einzelnen Download besteht nicht.

Die Einwilligung muss sich auf den freien Zugang zu den Daten und deren Weiterverwendung beziehen, d.h. die betroffene Person muss zustimmen, dass ihre Personendaten frei zugänglich sind und von Dritten verwendet werden dürfen.

Die Datenschutzgesetze sehen in der Regel Ausnahmen von der Informationspflicht vor, z. B. wenn die Information unmöglich ist oder einen unverhältnismässigen Aufwand erfordern würde. Diese Ausnahmen sind wohl anwendbar, wenn die Kontaktdaten einer Person nicht verfügbar sind; in der konkreten Situation muss jedoch anhand des anwendbaren Rechts geprüft werden, ob eine solche Ausnahme besteht und die jeweiligen Bedingungen als erfüllt angesehen werden können.

Wenn das Humanforschungsgesetz anwendbar ist, muss ausserdem geprüft werden, ob die Anforderungen dieses Gesetzes an die Weiterverwendung der Daten erfüllt sind.

XIV. Autres / Weitere

Question / Frage 84

Dans le cadre d'un projet de recherche dans le domaine de la santé, nous souhaitons utiliser le numéro AVS comme donnée d'identification. Le numéro AVS fait-il l'objet de dispositions particulières en matière de protection des données ? Est-il une donnée sensible ? Comment traiter cette donnée ?

Le numéro AVS est une donnée personnelle dont l'utilisation est soumise à des règles particulières figurant aux art. 153b et suivants de la Loi fédérale sur l'assurance-vieillesse et survivants (LAVS). L'art. 153c LAVS dresse la liste des autorités pouvant utiliser le numéro AVS, étant précisé que cela est possible seulement si l'exécution d'une tâche légale l'exige. Il n'existe pas de base légale autorisant l'utilisation du numéro AVS pour la recherche.

En raison des limites posées par l'art. 153c LAVS, le numéro AVS ne doit pas être utilisé comme donnée d'identification dans un projet de recherche. Il faut utiliser un autre identifiant (par exemple, nom et prénom, date de naissance).

Im Rahmen eines Forschungsprojekts im Gesundheitsbereich sollen die AHV-Nummern als Identifikationsdaten verwendet werden. Unterliegt die AHV-Nummer besonderen Datenschutzbestimmungen? Handelt es sich um besonders schützenswerte Personendaten? Wie soll mit diesen Daten umgegangen werden?

Die AHV-Nummer ist ein Personendatum, dessen Verwendung besonderen Regeln unterliegt, die in Art. 153b ff AHV-Gesetz aufgeführt sind. Art. 153c AHVG listet die Behörden auf, die die AHV-Nummer verwenden dürfen, wobei dies nur möglich ist, wenn es für die Erfüllung einer gesetzlichen Aufgabe erforderlich ist. Es gibt keine gesetzliche Grundlage, die die Verwendung der AHV-Nummer zu Forschungszwecken erlaubt.

Aufgrund der durch Art. 153c AHVG gesetzten Grenzen darf die AHV-Nummer nicht als Identifikationsmerkmal in einem Forschungsprojekt verwendet werden. Es muss ein anderer Identifikator (z.B. Vor- und Nachname, Geburtsdatum) verwendet werden.

Question / Frage 85

Qui peut signer un NDA professionnel pour données de recherche, par exemple pour le mode *restricted* d'un dépôt de données ?

Un *Non-Disclosure Agreement* (NDA ou accord de confidentialité) étant un contrat, il doit être signé par une personne ayant la faculté d'engager la haute école ou l'université sur le plan juridique par sa signature. Le droit de signature découle des lois et ordonnances sur les hautes écoles et les universités, mais peut également résulter en partie de prescriptions internes.

Wer kann ein berufsbezogenes NDA für Forschungsdaten unterzeichnen, z. B. für den *Restricted* Mode eines Repositoriums?

Da es sich bei einem NDA um einen Vertrag handelt, muss er von einer Person unterzeichnet werden, die befugt ist, die Hochschule durch ihre Unterschrift rechtlich zu verpflichten. Die Zeichnungsberechtigung ergibt sich aus den Hochschulgesetzen und -verordnungen, kann sich aber zum Teil auch aus internen Regelungen ergeben.

Question / Frage 86

La maintenance des données doit-elle être réalisée régulièrement en vue de vérifier l'exactitude, l'exhaustivité, le respect des dispositions légales, la durée de conservation, etc. des données de recherche collectées ? Qui en a la responsabilité ?

Tant la Loi fédérale sur la protection des données (LPD) (applicable aux écoles fédérales) que les lois cantonales sur la protection des données (applicables aux hautes écoles cantonales (universités, hautes écoles spécialisées et hautes écoles pédagogiques)) prévoient une obligation de s'assurer que les données personnelles sont exactes. La portée de cette obligation dépend des circonstances ; de manière générale, en matière de recherche, les conseils suivants peuvent être suivis :

- Une vérification doit être effectuée au moment de la publication.
- Un contrôle doit être effectué au moment du dépôt dans un référentiel.

Il n'existe en revanche pas d'obligation de vérifier régulièrement si les données sont toujours à jour (à condition que le dépôt indique clairement la date à laquelle les données ont fait l'objet de la dernière vérification).

Du point de vue juridique, la haute école ou l'université est responsable du traitement des données personnelles et donc responsable de respecter les règles en matière de protection des données. En pratique, l'institution doit veiller à ce que son personnel connaisse et applique les exigences légales dans ce domaine. Les chercheurs et chercheuses responsables d'un projet doivent s'assurer que leur recherche respecte la protection des données, en suivant notamment les éventuelles instructions ou lignes directrices de l'institution.

Muss die Datenpflege regelmässig durchgeführt werden, um die Richtigkeit, Vollständigkeit, Einhaltung der gesetzlichen Bestimmungen, Aufbewahrungsdauer usw. der gesammelten Forschungsdaten zu überprüfen? Wer ist dafür verantwortlich?

Sowohl das Bundesgesetz über den Datenschutz (anwendbar auf die Eidgenössischen Hochschulen) als auch die kantonalen Datenschutzgesetze (anwendbar auf die kantonalen Hochschulen (Universitäten, Fachhochschulen und Pädagogischen Hochschulen)) sehen die Pflicht vor, die Richtigkeit der Personendaten zu gewährleisten. Der Umfang dieser Verpflichtung hängt von den Umständen ab; im Allgemeinen sollten die folgenden Empfehlungen für die Forschung befolgt werden:

- Zum Zeitpunkt der Veröffentlichung muss eine Überprüfung erfolgen.
- Bei der Ablage in einem Repositorium muss eine Überprüfung erfolgen.

Es besteht jedoch keine Verpflichtung, regelmässig zu überprüfen, ob die Daten noch aktuell sind (vorausgesetzt, aus dem Repositorium geht klar hervor, wann die Daten zuletzt überprüft wurden).

Aus rechtlicher Sicht ist die Hochschule für die Bearbeitung der Personendaten und damit für die Einhaltung der Datenschutzbestimmungen verantwortlich. In der Praxis muss die Institution sicherstellen, dass ihre Mitarbeitenden die rechtlichen Anforderungen in diesem Bereich kennen und anwenden. Die für ein Projekt verantwortlichen Forschenden müssen sicherstellen, dass bei ihrer Forschungstätigkeit der Datenschutz eingehalten wird, indem sie insbesondere etwaige Weisungen oder Richtlinien der Institution befolgen.

Question / Frage 87

Dans quelles situations la Loi relative à la recherche sur l'être humain (LRH) s'applique-t-elle ?

La Loi fédérale relative à la recherche sur l'être humain (LRH) s'applique à la recherche sur les maladies humaines et sur la structure et le fonctionnement du corps humain, pratiquée sur des personnes, sur des personnes décédées, sur des embryons et des fœtus, sur du matériel biologique et sur des données personnelles liées à la santé. Elle pose des conditions en matière d'information et de consentement, ainsi que des exigences pour la

réutilisation de matériel biologique, de données génétiques et de données personnelles (non génétiques) liées à la santé.

In welchen Situationen gilt das Humanforschungsgesetz (HFG)?

Das Humanforschungsgesetz (HFG) gilt für die Forschung zu Krankheiten des Menschen sowie zu Aufbau und Funktion des menschlichen Körpers mit Personen, mit verstorbenen Personen, mit Embryonen und Föten, mit biologischem Material sowie mit gesundheitsbezogenen Personendaten. Es legt die Voraussetzungen für die Aufklärung und Einwilligung sowie die Anforderungen an die Weiterverwendung von biologischem Material, genetischen Daten und gesundheitsbezogenen (nicht genetischen) Personendaten fest.

Question / Frage 88

Les données vidéo, qui contiennent des données personnelles, peuvent-elles être utilisées pour la formation et la formation continue ?

L'utilisation de données vidéo contenant des données à caractère personnel pour des formations est possible sous certaines conditions :

- **Consentement :** Tout d'abord, il est important de s'assurer que toutes les personnes identifiables dans les données vidéo ont donné leur consentement à l'utilisation de leurs données à des fins de formation (à moins qu'il existe une base légale autorisant le traitement de données, auquel cas un consentement n'est pas nécessaire). Ce consentement doit être transparent, informé et volontaire.
- **Dispositions relatives à la protection des données :** Les lois nationales et cantonales sur la protection des données doivent être respectées. Cela implique de respecter les règles relatives à la protection des données à caractère personnel et de veiller à ce que le traitement de ces données soit conforme aux exigences légales correspondantes. En particulier, des mesures de sécurité appropriées doivent être prises pour garantir la confidentialité et l'intégrité des données.
- **Limitation de la finalité :** L'utilisation des données vidéo à des fins d'éducation et de formation devrait être compatible avec la finalité initiale de la collecte des données. Il convient d'éviter d'utiliser les données à d'autres fins sans obtenir un consentement supplémentaire.
- **Anonymisation :** dans la mesure du possible, les données à caractère personnel contenues dans les données vidéo devraient être anonymisées ou pseudonymisées afin de protéger la vie privée des personnes concernées.
- **Sensibilité :** lors de l'utilisation de données vidéo à des fins d'éducation et de formation, il est important de tenir compte de la sensibilité des informations et de veiller à ce que les données soient protégées de manière adéquate.

Dürfen Videodaten, die Personendaten enthalten, für die Aus- und Weiterbildung verwendet werden?

Die Verwendung von Videodaten, die Personendaten enthalten, ist zu Ausbildungszwecken unter bestimmten Voraussetzungen möglich:

- **Einwilligung:** Zunächst ist es wichtig sicherzustellen, dass alle Personen, die in den Videodaten identifiziert werden können, ihre Einwilligung zur Verwendung ihrer Daten für Schulungszwecke gegeben haben (es sei denn, es gibt eine Rechtsgrundlage, die die Datenbearbeitung erlaubt; in diesem Fall ist keine Einwilligung erforderlich). Diese Einwilligung muss transparent, informiert und freiwillig sein.
- **Datenschutzbestimmungen:** Die nationalen und kantonalen Datenschutzgesetze müssen eingehalten werden. Dies bedeutet, dass die Vorschriften zum Schutz von Personendaten eingehalten werden müssen und dass die Bearbeitung dieser Daten in Übereinstimmung mit den entsprechenden gesetzlichen Anforderungen erfolgen muss. Insbesondere sind angemessene Sicherheitsmassnahmen zu treffen, um die Vertraulichkeit und Integrität der Daten zu gewährleisten.

- **Zweckbindung:** Die Verwendung von Videodaten für Aus- und Weiterbildungszwecke sollte mit dem ursprünglichen Zweck der Datenerhebung vereinbar sein. Die Verwendung der Daten für andere Zwecke ohne zusätzliche Einwilligung ist zu vermeiden.
- **Anonymisierung:** Soweit möglich, sind die in den Videodaten enthaltenen Personendaten zu anonymisieren oder zu pseudonymisieren werden, um die Privatsphäre der betroffenen Personen zu schützen.
- **Sensibilität:** Bei der Verwendung von Videodaten für Ausbildungs- und Weiterbildungszwecke ist es wichtig, die Sensibilität der Informationen zu berücksichtigen und sicherzustellen, dass die Daten angemessen geschützt werden.

Question / Frage 89

Si une haute école (Data Processor) héberge des données médicales de patient·e·s d'un prestataire de soins (Data Controller), peut-elle les réutiliser à des fins de recherche ?

Un sous-traitant ne peut pas utiliser dans son propre intérêt les données hébergées pour le compte du responsable du traitement. Un tel traitement est toutefois envisageable si les données reprises sont véritablement anonymes et que le responsable du traitement a donné son accord.

Wenn eine Hochschule als Auftragsdatenbearbeiter medizinische Patientendaten eines Gesundheitsdienstleisters (Datencontroller) hostet, darf sie diese dann zu Forschungszwecken weiterverwenden?

Ein Auftragsdatenbearbeiter darf die im Auftrag des Verantwortlichen gehosteten Daten nicht im eigenen Interesse (als Datenverantwortlicher) verwenden. Eine solche Bearbeitung ist nur möglich, wenn die Daten anonym übernommen werden und der für die Bearbeitung Verantwortliche seine Einwilligung gegeben hat.

Question / Frage 90

Que faut-il entendre par un traitement ou une communication « à des fins de recherche » ? Comment traiter les différentes réglementations dans les lois cantonales sur la protection des données et dans la Loi fédérale sur la protection des données ?

Dans les lois cantonales sur la protection des données ainsi que dans la Loi fédérale sur la protection des données (art. 39 LPD), il existe des réglementations qui autorisent le traitement ou la communication de données personnelles dans un but non personnel, notamment (entre autres) pour la recherche. Il n'y a toutefois pas d'unanimité sur la question de savoir si cela supprime la finalité du traitement des données ainsi que d'autres exigences relatives au traitement/à la communication (par exemple, l'exigence du consentement). Les interprétations divergentes de ce privilège de la recherche fragmentent ainsi le paysage suisse de la recherche et compliquent l'échange intra-cantonal et intra-fédéral ainsi que la communication des données au sein de la Suisse. Dans cette mesure, il convient de mettre en évidence les différences cantonales, d'en tenir compte et, en cas de doute, de consulter l'autorité cantonale de protection des données /le·la préposé·e cantonal·e à la protection des données.

Was ist unter einer Bearbeitung bzw. Bekanntgaben «zu Forschungszwecken» zu verstehen? Wie ist mit den unterschiedlichen Regelungen in den kantonalen Datenschutzgesetzen bzw. dem Bundesgesetz über den Datenschutz umzugehen?

In den kantonalen Datenschutzgesetzen sowie im Bundesgesetz über den Datenschutz (Art. 39) existieren Regelungen, welche eine Bearbeitung bzw. eine Bekanntgabe von Personendaten zu einem nicht personenbezogenen Zweck, insbesondere (unter anderem) für die Forschung, zulassen. Ob hierdurch die Zweckbindung der Datenbearbeitung sowie sonstige Anforderungen an die Bearbeitung / Bekanntgabe (bspw. das Einwilligungserfordernis) aufgehoben werden, wir indes nicht einheitlich gesehen. Die divergierende Auslegung dieses sog. Forschungsprivilegs zersplittert damit die schweizerische Forschungslandschaft und

erschwert den innerkantonalen und innerföderalen Austausch sowie die Datenkommunikation innerhalb der Schweiz. Insofern gilt, die kantonalen Unterschiede herauszuarbeiten, zu beachten und im Zweifel die Kantonale Datenschutzbehörde / den kantonalen Datenschutzbeauftragten zu konsultieren.

Question / Frage 91

Peut-on considérer que les hautes écoles sont toutes « soumises à la même loi » lorsqu'il s'agit de traiter des données de recherche sous le « privilège de la recherche » ?

Les écoles fédérales sont soumises à la Loi fédérale sur la protection des données (LPD), tandis que les hautes écoles cantonales (universités, hautes écoles spécialisées et hautes écoles pédagogiques) sont soumises à la loi cantonale sur la protection des données du canton dans lequel elles se situent. Même si le privilège de la recherche est réglementé de manière similaire dans ces différentes lois, il convient de s'assurer, dans chaque cas d'espèce, que les conditions de la loi applicable sont respectées.

Kann man davon ausgehen, dass die Hochschulen alle «demselben Gesetz unterworfen» sind, wenn es darum geht, Forschungsdaten unter dem sog. Forschungsprivileg zu bearbeiten?

Die Eidgenössischen Hochschulen unterstehen dem Bundesgesetz über den Datenschutz, die kantonalen Hochschulen (Universitäten, Fachhochschulen und Pädagogischen Hochschulen) dem Datenschutzgesetz ihres Standortkantons. Auch wenn das Forschungsprivileg in diesen verschiedenen Gesetzen ähnlich geregelt ist, muss im Einzelfall geprüft werden, ob die Voraussetzungen des anwendbaren Gesetzes erfüllt sind.

Question / Frage 92

Quelle est l'autorité cantonale de protection des données compétente lorsque plusieurs hautes écoles de différents cantons travaillent ensemble sur un projet de recherche ?

La réponse a été donnée (en allemand) par privatim, la Conférence des Préposé·e·s suisses à la protection des données.

L'autorité de protection des données de chaque canton impliqué pour les traitements de données personnelles effectués par « sa » haute école. Dans la mesure où il y a un traitement commun des données, il est judicieux d'attribuer une responsabilité globale à un service, ce qui ne change toutefois rien à la responsabilité de chaque haute école pour ses traitements de données.

Welche Kantonale Datenschutzbehörde ist zuständig, wenn mehrere Hochschulen aus verschiedenen Kantonen gemeinsam an einem Forschungsprojekt arbeiten?

Die Antwort wurde von privatim, der Konferenz der Schweizer Datenschutzbeauftragten, zur Verfügung gestellt:

Die Datenschutzbehörde jedes beteiligten Kantons für die Personendatenbearbeitungen durch «seine» Hochschule. Soweit eine gemeinsame Datenbearbeitung stattfindet, wird sinnvollerweise einer Stelle eine Gesamtverantwortung zugewiesen, die jedoch nichts an der Verantwortung jeder Hochschule für ihre Datenbearbeitungen ändert.