国内外の個人情報保護法制が日本の学術研究活動にもたらす影響

第３回バイオバンク・ネットワークウェビナー

『個人情報保護法改正とバイオバンクへの影響を考える』

2021年12月7日（火）

隅藏 康一（政策研究大学院大学　教授）

日本における個人情報保護法制の抜本的な再構築(2021)

2021年個人情報保護法改正

- ① 個人情報保護法、行政機関個人情報保護法、独立行政法人等個人情報保護法の3本の法律を1本の法律に統合するとともに、地方公共団体の個人情報保護制度についても統合後の法律において全国的な共通ルールを規定し、全体の所管を個人情報保護委員会に一元化
- ② 医療分野・学術分野の規制を統一するため、国公立の病院、大学等には原則として民間の病院、大学等と同等の規律を適用
- ③ 学術研究分野を含めたGDPR（EU一般データ保護規則）の十分性認定への対応を目指し、学術研究に係る適用除外規定について、一律の適用除外ではなく、義務ごとの例外規定として精緻化
- ④ 個人情報の定義等を国・民間・地方で統一するとともに、行政機関等での匿名加工情報の取扱いに関する規律を明確化

2021年改正前は3つの法律と地方自治体の個人情報保護条例が存在（2000個問題）

改正後個人情報保護委員会に一元化

個人情報の保護に関する法律・・・個人情報保護委員会所管
（個人情報保護法：民間企業や私立大学が対象）
平成15年法律第57号

行政機関の保有する個人情報の保護に関する法律・・・総務大臣所管
（行政機関個人情報保護法：法人化されていない国立の研究所などが対象）
平成15年法律第 58号

独立行政法人等の保有する個人情報の保護に関する法律・・・総務大臣所管
（独立行政法人等個人情報保護法：国立大学法人や国立研究開発法人などが対象）
平成15年法律第59 号

個人情報保護法（2021年改正後）

- 第1章　総則（1条～3条）
- 第2章　国及び地方公共団体の責務等（4条～6条）
- 第3章　個人情報の保護に関する施策等（7条～15条）
- 第4章　個人情報取扱事業者等の義務等（16条～59条）
- 第5章　行政機関等の義務等（60条～129条）
- 第6章　個人情報保護委員会（130条～170条）
- 第7章　雑則（171条～175条）
- 第8章　罰則（176条～185条）

個人情報（2条1項）

- 生存する個人に関する情報であって、
- ①当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）
- ②個人識別符号が含まれるもの

個人識別符号（2条2項）

- ①特定の個人の身体の一部の特徴を電子計算機の用に供するために変換した文字、番号、記号その他の符号であって、当該特定の個人を識別できるもの
- ②個人に提供されるサービスの利用若しくは個人に販売される商品の購入に関し割り当てられ、又は個人に発行されるカードその他の書類に記載され、若しくは電磁的方式により記録された文字、番号、記号その他の符号であって、その利用者若しくは購入者又は発行を受ける者ごとに異なるものとなるように割り当てられ、又は記載され、若しくは記録されることにより、特定の利用者若しくは購入者又は発行を受ける者を識別することができるもの

個人識別符号（1号）

- イ　細胞から採ったデオキシリボ核酸（DNA）を構成する塩基配列
- ロ　顔の骨格および皮膚の色ならびに目、鼻、口その他の顔の部位の位置および形状によって定まる容貌
- ハ　虹彩の表面の突起により形成される線上の模様
- ニ　発声の際の声帯の振動、声紋の開閉ならびに声道の形状およびその変化
- ホ　歩行の際の姿勢および両腕の動作、歩幅その他の歩行の態様
- ヘ　手のひらまたは手の甲もしくは指の皮下の静脈の分岐および端点によって定まるその静脈の形状
- ト　指紋または掌紋
- チ　以上の組み合わせ

要配慮個人情報（2条3項）

- 本人の
- ①人種
- ②信条
- ③社会的身分
- ④病歴
- ⑤犯罪の経歴
- ⑥犯罪により害を被った事実
- ⑦その他本人に対する不当な差別、偏見その他の不利益が生じないように、その取扱いに配慮を要するものとして政令で定める記述等
- が含まれる個人情報をいう。

仮名加工情報（2条5項）

- 次の各号に掲げる個人情報の区分に応じて当該各号に定める措置を講じて他の情報と照合しない限り特定の個人を識別できないように個人情報を加工して得られる個人に関する情報をいう。
- 二　当該個人情報に含まれる個人識別符号の全部を削除すること（当該個人識別符号を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）。

- ※　個人情報に該当。

匿名加工情報（2条6項）

- 次の各号に掲げる個人情報の区分に応じて当該各号に定める措置を講じて特定の個人を識別できないように個人情報を加工して得られる個人に関する情報であって、当該個人情報を復元することができないようにしたものをいう。
- 二　当該個人情報に含まれる個人識別符号の全部を削除すること（当該個人識別符号を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む）

- ※　個人情報にはあたらない

個人情報に関する、個人情報取扱事業者の義務（17-21条）

- 利用目的をできる限り特定しなければならない。利用目的を変更する場合には、変更前の利用目的と関連性を有すると合理的に認められる範囲を超えて行ってはならない。（※　それ以外の場合は、本人の事前同意が必要。変更前の利用目的と関連性を有すると合理的に認められる範囲内の変更である場合も、変更された利用目的を本人に通知し又は公表する必要がある。）
- 本人の事前同意を得ずに、利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない。（※　目的外利用には本人の事前同意が必要。）
- 違法又は不当な行為を助長し、又は誘発するおそれがある方法により個人情報を利用してはならない
- 偽りその他不正の手段により個人情報を取得してはならない。本人の事前同意を得ずに要配慮個人情報を取得してはならない。
- 個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を本人に通知し又は公表しなくてはならない。

本人の事前同意なしに個人情報を目的外利用できる場合（18条3項）

- 法令に基づく場合
- 人の生命、身体又は財産の保護のために必要がある場合で、本人の同意を得ることが困難なとき
- 公衆衛生の向上又は児童の健全育成の推進のために特に必要がある場合で、本人の同意を得ることが困難なとき
- 国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに協力する必要がある場合であって、本人の同意を得ることにより当該事務遂行に支障を及ぼすおそれがあるとき
- 学術研究機関等が、個人情報を学術研究目的で取り扱う必要があるとき
- 学術研究機関等に個人データを提供する場合であって、当該学術機関等が当該個人データを学術研究目的で取り扱う必要があるとき

本人の事前同意なしに要配慮個人情報を取得できる場合（20条2項）

- 法令に基づく場合
- 人の生命、身体または財産の保護のために必要がある場合で、本人の同意を得ることが困難なとき
- 公衆衛生の向上または児童の健全育成の推進のために特に必要がある場合で、本人の同意を得ることが困難なとき
- 国の機関もしくは地方公共団体またはその委託を受けた者が法令の定める事務を推敲することに協力する場合で、本人の同意を得ることにより当該事務遂行に支障を及ぼすおそれがあるとき
- 学術研究機関等が、当該要配慮個人情報を学術研究目的で取り扱う必要があるとき
- 学術研究機関等から当該要配慮個人情報を取得する場合であって、当該要配慮個人情報を学術研究目的で取得する必要があるとき
- 当該要配慮個人情報が、本人、国の機関、地方公共団体、学術研究機関等、57号1項各号に掲げる者その他委員会規則で定める者により公開されている場合
- その他前各号に掲げる場合に準ずるものとして政令で定める場合

個人データに関する、個人情報取扱事業者の義務（22-28条）

- 正確性の確保、不要となった個人データの消去
- 安全管理措置、従業者の監督、委託先の監督、漏えい等の報告等
- 第三者提供の制限（本人の事前同意が必要）、外国にある第三者への提供の制限（本人の事前同意が必要）、第三者提供に係る記録の作成等、第三者提供を受ける際の確認等

第三者提供における本人の事前同意取得の例外（27条1項）

- 法令に基づく場合
- 人の生命、身体または財産の保護のために必要がある場合で、本人の同意を得ることが困難なとき
- 公衆衛生の向上または児童の健全育成の推進のために特に必要がある場合で、本人の同意を得ることが困難なとき
- 国の機関もしくは地方公共団体またはその委託を受けた者が法令の定める事務を推敲することに協力する場合で、本人の同意を得ることにより当該事務遂行に支障を及ぼすおそれがあるとき
- 学術研究機関等による当該個人データの提供が、学術研究の成果の公表又は教授のためやむを得ないとき
- 学術研究機関等が当該個人データを学術研究目的で提供する必要があるとき
- 提供を受ける第三者が学術研究機関等であり、当該第三者が当該個人データを学術研究目的で取り扱う必要があるとき

第三者提供における本人の事前同意取得の例外（27条2項、5項）

- オプトアウト制度
  所定の事項をあらかじめ本人に通知し、又は容易に知り得る状態に置くとともに、
  個人情報保護委員会に届け出たときは、
  ⇒個人データを第三者に提供できる
  （ただし、①要配慮個人情報、②不正な手段で取得されたもの、③他の事業者からオプトアウト方式で提供されたもの、は除外）
- 第三者にあたらない場合
  委託先への提供
  事業承継に伴う提供
  共同利用（所定の事項をあらかじめ本人に通知し、又は容易に知り得る状態に置いているとき）

外国にある第三者に提供する場合（28条）

- 本人の事前同意が必要
- 27条1項に記されたのと同じ例外が適用される
- 27条2項、5項の記載内容については、例外が適用されない。すなわち「オプトアウト制度」や「第三者にあたらない場合」の規定は適用されない。
- ただし、個人情報保護委員会の認定国（現在は、EEAと英国）、ならびに、基準適合体制整備者は、国内の第三者と同様に扱われる。

学術研究機関の扱いについて（2021年改正前）

- 私立大学は個人情報保護法の対象であり、学術研究の用に供する目的で個人データが取り扱われる場合は、同法76条により、同法4章に記された個人情報取扱事業者の義務規定の適用除外とされていた。
- 国立大学法人や国立研究開発法人や国立の研究所は、個人情報保護法の適用対象ではないため、上記の適用除外の対象となっていなかった。

学術研究機関の扱いについて（2021年改正後）

- 官民を問わず「学術研究機関等」を位置付け。国公立大学、私立大学、国立研究開発法人、国立研究所、国公立病院、私立病院、いずれも含まれる。
- 学術研究目的については、以下の義務を免除。

  利用目的による制限：本人の事前同意なしに個人情報を目的外利用できる（18条3項）

  要配慮個人情報の取得制限：本人の事前同意なしに要配慮個人情報を取得できる（20条2項）

  第三者提供の制限：本人の事前同意なしに第三者提供できる（27条1項）

学術研究機関等の責務（59条）

- 個人情報取扱事業者である学術研究機関は、学術研究目的で行う個人情報の取扱いについて、この法律の規定を遵守するとともに、その適正を確保するために必要な措置を自ら講じ、かつ、当該措置の内容を公表するよう努めなくてはならない。

国立大学法人政策研究大学院大学（2021）『国立研究開発法人及び国立大学法人等が研究目的により国内外の個人データを取り扱う場合の動向及び今後の課題等に関する調査分析　報告書』.

https://www.mext.go.jp/content/20210510-mxt_chousei01-100000404.pdf

EUの一般データ保護規則（GDPR）

- 欧州においては、2016年4月に欧州議会本会議でRegulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) が採択された。
- それまでのEUにおけるDirective 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such dataに替わり、EU域内における新たな個人データ保護のルールとなった。
- GDPRは約2年後の2018年5月から全面適用されており、対象となる国は、EU加盟国（現時点で全27か国）にノルウェー、リヒテンシュタイン、アイスランドを含めた30か国（EEA: European Economic Area, 欧州経済領域）。

個人データの処理（取扱い）

- 自動的な手段によるか否かを問わず、
- 収集、記録、編集、構成、記録保存、修正若しくは変更、検索、参照、使用、送信による開示、配布、
- 又は、それら以外に利用可能なものとすること、整列若しくは結合、制限、消去若しくは破壊のような、
- 個人データ若しくは一群の個人データに実施される業務遂行又は一群の業務遂行を意味する（GDPR4条2項）。

管理者、処理者、共同管理者

- 管理者（controller）とは、「自然人又は法人、公的機関、部局又はその他の組織であって、単独で又は他の者と共同で、個人データの取扱いの目的及び方法を決定する者」を指す（GDPR第4条第7項）。
- 処理者（processor）とは、「管理者の代わりに個人データを取扱う自然人若しくは法人、公的機関、部局又はその他の組織」を指す（GDPR第4条第8項）。
- 共同管理者（joint controller）とは、二者以上の管理者が共同して取扱いの目的及び方法を決定する場合、それらの者をいう（GDPR第26条第1項）。

European Data Protection Board (EDPB) “Guidelines 07/2020 on the concepts of controller and processor in the GDPR”

- 「いくつかの研究機関は、特定の共同研究プロジェクトに参加し、そのためにプロジェクトに関与する研究機関の1つの既存のプラットフォームを使用することを決定します。各研究機関は、共同研究の目的で保有する個人データをプラットフォームに供給し、プラットフォームを通じて他の人が提供したデータを使用して研究を行います。この場合、すべての研究機関は、処理の目的と使用手段（既存のプラットフォーム)を一緒に決定したため、このプラットフォームから情報を保存および開示することによって行われる個人データ処理の共同管理者に該当します。ただし、各研究機関は、それぞれの意図する目的のためにプラットフォームの外部で実行する可能性のある他の処理については、それぞれが別途管理者となります。」

日本の大学・研究機関のGDPRとの関わり

- 欧州に拠点を有する場合
- 欧州の組織から個人データの移転を受ける場合
- 欧州の機関と共同研究を行う場合　など

- 共同プロジェクトとして計画策定から参加し、情報収集するような場合には共同管理者となり得る。
- 他方、共同管理者として収集された個人データであったとしても、収集後の処理が分離可能であって相互に補助するものではない場合は、独立した処理については、それぞれが管理者として別個に対応する余地がある。
- また、単に欧州の研究機関が運営するデータプラットフォームを利用する場合については、共同管理者ではなく独立の管理者と評価し得る。
- 関与の仕方、役割によっては、処理者と整理されることも考えられる。
- 実態を踏まえていずれに該当するか判断し、必要な措置を講ずることとなる。

GDPRの基本原則

- 個人データの処理については、
- ①適法性・公平性・透明性、
- ②目的の限定、
- ③データの最小化、
- ④正確性、
- ⑤記録保存の制限、
- ⑥完全性及び機密性、
- の6つの基本原則を遵守しなくてはならない（GDPR5条第1項）。

適法性根拠

個人データの処理に当たっては、以下の少なくとも一つの法的根拠が求められる（GDPR第6条第1項）。そのいずれかの事由が認められない場合は、個人データを処理することはできない。

- データ主体が、一つ又は複数の特定の目的のための自己の個人データの処理に関し、同意を与えた場合（同項(a)）
- データ主体が契約当事者となっている契約の履行のために処理が必要となる場合、又は、契約締結の前に、データ主体の要求に際して手段を講ずるために処理が必要となる場合（同項(b)）
- 管理者が服する法的義務を遵守するために取扱いが必要となる場合（同項(c)）
- データ主体又は他の自然人の生命に関する利益を保護するために取扱いが必要となる場合（同項(d)）
- 公共の利益において、又は、管理者に与えられた公的な権限の行使において行われる職務の遂行のために取扱いが必要となる場合（同項(e)）
- 管理者によって、又は、第三者によって求められる正当な利益の目的のために取扱いが必要となる場合。ただし、その利益よりも、個人データの保護を求めるデータ主体の利益並びに基本的な権利及び自由のほうが優先する場合、特に、そのデータ主体が子どもである場合を除く（同項(f)）

データ主体が持つ権利

- GDPRにおいて個人データとは、識別された自然人又は識別可能な自然人（「データ主体」）に関する情報を意味する（4条1項）。
- GDPRはデータ主体が持つ権利を中心に構成されており、
- ①情報提供を受ける権利（GDPR13条、14条）、
- ②アクセスの権利（GDPR15条）、
- ③訂正の権利（GDPR16条）、
- ④消去の権利（忘れられる権利）（GDPR17条）、
- ⑤処理制限の権利（GDPR18条）、
- ⑥個人データの訂正若しくは消去又は処理制限に関する通知義務（GDPR19条）、
- ⑦データポータビリティの権利（GDPR20条）、
- ⑧異議を述べる権利（GDPR21条）、
- ⑨プロファイリングを含む個人に対する自動化された意思決定に関する権利（GDPR22条）
- が認められている。

特別な種類のデータの取扱いの原則禁止

- GDPR第9条第1項は、「人種的若しくは民族的な出自、政治的な意見、宗教上若しくは思想上の信条、又は、労働組合への加入を明らかにする個人データの取扱い、並びに、遺伝子データ（※１）、自然人を一意に識別することを目的とする生体データ（※２）、健康に関するデータ（※３）、又は、自然人の性生活若しくは性的指向に関するデータの処理は、禁止される。」と規定し、特別な類型のデータの処理を原則として禁止している。
- ※１　自然人の、先天的な又は後天的な遺伝的特性に関連する個人データであって、自然人の生理状態又は健康状態に関する固有な情報を与えるものであり、かつ、特に、当の自然人から得られた生化学資料の分析結果から生ずるもの（GDPR第4条第13項）
- ※２　自然人の身体的、生理的又は行動的な特性に関連する特別な技術的取扱いから得られる個人データであって、顔画像や指紋データのように、当該自然人を一意に識別できるようにするもの、又はその識別を確認するもの（GDPR第4条第14項）
- ※３　医療サービスの提供を含め、健康状態に関する情報を明らかにする、自然人の身体的又は精神的な健康と関連する個人データ（GDPR第4条第15項）

特別な種類のデータの取扱いの原則禁止の例外

- データ主体が、一つ又は複数の特定された目的のためのその個人データの処理に関し、明確な同意を与えた場合（同項（a））
- データ主体によって明白に公開のものとされた個人データに関する取扱いの場合（同項(e)）
- 求められる目的と比例的であり、データ保護の権利の本質的部分を尊重し、また、データ主体の基本的な権利及び利益の安全性を確保するための適切かつ個別の措置を定めるEU 法又は加盟国の国内法に基づき、重要な公共の利益を理由とする取扱いが必要となる場合（同項(g)）
- EU法又は加盟国の国内法に基づき、又は医療専門家との契約により、かつ、同条第3項に定める条件及び保護措置に従い、予防医学若しくは産業医学の目的のために、労働者の業務遂行能力の評価、医療上の診断、医療若しくは社会福祉又は治療の提供、又は医療制度若しくは社会福祉制度及びそのサービス提供の管理のために取扱いが必要となる場合（同項（h））
- 健康に対する国境を越える重大な脅威から保護すること、又は医療及び医薬品若しくは医療機器の高い水準の品質及び安全性を確保することのような、公衆衛生の分野において、公共の利益を理由とする取扱いが必要となる場合（同項（i））
- 求められる目的と比例的であり、データ保護の権利の本質的部分を尊重し、また、データ主体の基本的な権利及び利益の安全性を確保するための適切かつ個別の措置を定めるEU法又は加盟国の国内法に基づき、第89条第1項に従い、公共の利益における保管の目的、科学的研究若しくは歴史的研究の目的又は統計の目的のために取扱いが必要となる場合（同項（j））

GDPRにおける、学術上の活動や科学研究に関連する条文

- 85条第2項には、報道の目的、又は、学術上の表現、芸術上の表現又は文学上の表現の目的のために行われる取扱いに関し、加盟国は、個人データの保護の権利と表現の自由及び情報伝達の自由との調和を保つ必要がある場合、GDPRにおけるいくつかの規程の例外又は特例を認める、との記載がある。
- 89条2項は、個人データが科学調査若しくは歴史調査の目的又は統計の目的で取扱われる場合、EU法又は加盟国の国内法は、そのような権利が、個別具体的な目的を達成できないようにしてしまうおそれがある場合、又は、その達成を深刻に阻害するおそれがある場合であり、かつ、そのような特例がそれらの目的を果たすために必要である場合に限り、データの最小化や仮名化を施した上で、アクセスの権利、訂正の権利、処理制限の権利、ならびに異議を述べる権利の特例を定めることができるとしている。
- 9条1項は、「特別な種類の個人データ」について：前掲

EUからのデータの越境移転

- GDPRは44条以下で越境移転について定めているが、なかでも45条は、十分性認定に基づく移転について定めている。
- 十分性認定は、「第三国、第三国内の地域又は一若しくは複数の特定の部門、又は、国際機関」に対して行うことができ、十分性認定がなされた場合、当該第三国又は国際機関への個人データの移転にはいかなる個別の許可も必要ではない。
- 一方、移転しようとする第三国等が十分性認定を受けていない場合は、「管理者又は処理者は、その管理者又は処理者が適切な保護措置を提供しており、かつ、データ主体の執行可能な権利及びデータ主体のための効果的な司法救済が利用可能なことを条件としてのみ、第三国又は国際機関への個人データを移転することができる」とされる（GDPR46条1項）。
- この場合の具体的な手段は同条2項に定められている。

GDPRの十分性認定（2021年日本の法改正前）

- 日本は、欧州委員会による十分性認定を受けており、個人データ保護について十分な水準を満たしていると判断されている。（Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information）
- 2021年個人情報保護法改正以前は、この十分性認定は、個人情報保護法の適用範囲に限られているため、国立大学法人や国立研究開発法人はその対象から外れていた。
- さらに、私立大学は個人情報保護法の対象であるが、学術研究の用に供する目的で個人データが取り扱われる場合は、同法76条により、同法4章に記された個人情報取扱事業者の義務規定の適用除外とされているため、GDPRに基づく十分性認定の対象に含まれない。
- すなわち、日本の大学や公的研究機関は、欧州在住のデータ主体に関する個人データの越境移転を受けようとすれば、各大学・機関において個別に、個人情報の適切な保護措置を取る必要があった。

GDPRの十分性認定（2021年日本の法改正後）

- 個人情報保護法の令和3年改正後は、民間事業者だけでなく大学・公的研究機関を含むすべての機関がGDPR第45条による日本への十分性認定の範囲に含まれるようになり、個人データの越境移転が容易になると期待される。
- ただし、十分性認定はあくまでも欧州委員会の判断によるものとなる。
- 欧州以外との越境データ移転についても、GDPRが参考にされているところは大であり、十分性認定の対象が拡大すれば、波及も想定される。

GDPRの十分性認定以外の枠組みによる、EU域内からの越境データ移転の可能性

- GDPR前文26項によると、匿名情報の処理はGDPRの適用を受けるものではないものの、どのような措置を講じ、また、どのような状態のデータであれば匿名情報となるかは必ずしも明確ではない。
- 今後、事例の積み重ねにより、匿名情報となるための条件が明確になってくれば、欧州委員会からの十分性認定が大学・公的研究機関に及ぶようになる前であっても、日本の大学・公的研究機関がEU域内の機関と共同で研究のために個人データの収集を行い、EU域内で個人データの保有及び処理（分析を含む）を完了させ、個人データではない状態にまで加工してから日本の大学・公的研究機関への移転を行うというスキーム上の工夫が可能となるものと期待される。
- しかしながら、国際共同研究等において、やはり日本の大学・公的研究機関においても、生のデータを見て分析したいという場面は生じるであろう。そのような場合は、越境移転制限において個別の移転を許すスキームを検討することになる。
- 例えば、GDPR第46条第2項には、十分性認定がない場合の適切な保護措置を条件とした個人データの移転について、監督機関からの個別の承認を必要としない6つの類型を挙げる。民間企業においてはBinding Corporate Rule（BCR）によるグループ企業間の包括的な移転も想定し得るが、日本の大学・公的研究機関においては認証を得るためのコストがかかりすぎるため、現実的な選択肢にはなり得ない。他方、欧州の研究機関と日本の大学・公的研究機関の間で、欧州委員会が決定したSCC（Standard Contractual Clause：標準契約条項）を含む契約を締結したうえで、個人データを移転することは検討され得る。

データ主体の同意の取得

- GDPR第6条第1項には、GDPRに係る個人データの処理の適法化要件が6つ記されているが、研究活動においては、ほぼすべての場合に、これらの要件のうちの「データ主体が1つ以上の特定の目的のために自己の個人データの処理に同意を与えた場合」(a)を根拠とすることになるだろう。
- 上記のSCCによる個人データの越境移転を行う場合であっても、処理の適法化根拠は必要であるため、個人データを第三国に移転することが予定されていること、ならびに、その個人データが第三国でどのように取り扱われるかについて、データ主体に示して同意を得ておく必要がある。
- そして、このような同意と、研究のためのインフォームド・コンセント（特に臨床研究によるもの）をどのように取得するか、についても気を配る必要がある。GDPRでは、ガイドライン等も見られるところである。

GDPR: 大学に対する執行事例はあるか？

- GDPRはそもそも、巨大プラットフォーム企業等が個人データをデータ主体の意に反して取得・利用してビジネスを展開することに歯止めをかけるために制定されたのであり、大学・公的研究機関の研究活動がGDPRによる罰則の適用対象となることはないであろう、という見方もありうる。
- 実際、我々が調査した範囲では、欧州においても、大学・公的研究機関の研究活動そのものに関してGDPR違反が指摘されたというケースは、まだ知られていない。
- もっとも、大学に対しての執行事例は知られている。例えば、ポーランドのデータ保護機関が、大学が、オンラインプラットフォーム上で行った試験についてのデータを漏洩したにもかかわらず、データ侵害通知を行わなかったことについてGDPRを執行した事例として、“Polish DPA: University Fined for the lack of Data Breach Notifications,” https://edpb.europa.eu/news/national-news/2021/polish-dpa-university-fined-lack-data-breach-notifications_en
- 学術上の活動や科学研究に関する特例や適用除外は、大学・公的研究機関において取扱われている個人データのうち、研究活動において取扱われる個人データを対象としており、事務系の部局で取扱われる個人データは対象としていないことに注意が必要である。

大学や公的研究機関の日常の業務・活動に関して、取り扱われる個人データには、様々なものがある

事務系で取扱われる個人データ	大学・公的研究機関に共通	研究活動において取扱われる個人データ
入試志願者のデータ	当該機関が主催するシンポジウムで招聘した講演者の個人データ（自宅住所、銀行口座、マイナンバーなど）	特定の地域の住民の医療データや遺伝子データ
学生の成績データ	当該機関に在籍するあるいは時限付きで受け入れた研究者の個人データ	脳をはじめとする身体の測定データ
教員の人事データ		人文・社会科学研究におけるアンケート調査の個票データ

交換留学プログラムにおける海外からの学生受け入れ、海外からの講演者の受け入れ、海外からのポストドクターの受け入れ、海外の特定地域の住民に関する生命科学的あるいは社会科学的な調査などにより、海外に在住する個人のデータが含まれることもある。こうした個人データが欧州に在住する個人のものである場合、GDPRに関連して、特段の配慮が必要である。

出典：国立研究開発法人及び国立大学法人等が研究目的により国内外の個人データを取り扱う場合の動向及び今後の課題等に関する調査分析　調査報告書

国立研究開発法人及び国立大学法人等が研究目的により
国内外の個人データを取り扱う場合の動向及び今後の課題等に関する調査分析

（有識者）

石井 夏生利	中央大学　教授	(2.5)
板倉 陽一郎	ひかり総合法律事務所　弁護士	(3)
小泉 周	自然科学研究機構　特任教授	(2.6)
長神 風二	東北メディカル・メガバンク機構　特任教授	
日置 巴美	三浦法律事務所　弁護士	(2.1, 2.2)

（政策研究大学院大学）

隅藏 康一	教授	(代表者, 調査・報告書作成)
大﨑 章弘	客員研究員	(調査・報告書作成支援)
加藤 春香	研究補佐員	(2.4, 調査・報告書作成支援)
天元 志保	客員研究員	(2.3, 調査・報告書作成支援)
藤原 奈保子	研究補佐員	(調査・報告書作成支援)

Ana Nordberg (2021) “Biobank and Biomedical Research: Responsibilities of Controllers and Processors Under the EU General Data Protection Regulation.”

In Santa Slokenberga et al. (2021), “GDPR and Biobanking,” Springer. https://link.springer.com/book/10.1007/978-3-030-49388-2

Geographical Scope of the GDPR

- Biobanks often collect, receive, keep or analyse transnational samples or data, which raises the question of the geographic scope of applicability of data protection rules. Generally, there are two factors that are relevant to determine the territorial scope of application: the establishment criterion, and the targeting criterion.
- Concerning the establishment criterion, the European Data Protection Board (EDPB) recommends consideration of three aspects: (a) establishment in the EU; (b) processing of personal data carried out 'in the context of the activities of' an establishment; and (c) application of the GDPR to the establishment of a controller or a processor in the EU regardless of whether the processing takes place in the EU or not.
- In regards to the targeting criterion, Article 3 contains international private law rules that extend the jurisdiction of the GDPR to data controllers and processors not established in the EU and regardless of where the data processing activities take place. The connecting factor here is the location of the data subject and the purpose of the data processing activities. The GDPR applies to data subjects located in the EU independently of their legal status concerning nationality or residence.

Ana Nordberg (2021) "Biobank and Biomedical Research: Responsibilities of Controllers and Processors Under the EU General Data Protection Regulation." in Santa Slokenberga et al., "GDPR and Biobanking," Springer. https://link.springer.com/book/10.1007/978-3-030-49388-2

Notion of Controller and Processor in Biobanking

- In a biobanking context the controller is whichever entity decides on issues pertaining to those substantial questions which are essential to the core of lawfulness of processing, for example, decisions on the legal basis for processing (e.g. consent or an exception), length of time a biological sample and related data are to be stored and who has access to the personal data processed.
- The concept of processor is dependent on the organisational decisions and structure of the controller.

Ana Nordberg (2021) "Biobank and Biomedical Research: Responsibilities of Controllers and Processors Under the EU General Data Protection Regulation." in Santa Slokenberga et al., "GDPR and Biobanking," Springer. https://link.springer.com/book/10.1007/978-3-030-49388-2

Joint-Controllers and Joint-Processors

- In biobanking practice, situations involving putative joint-controllers and joint-processors present challenges, in particular when different entities submit samples and data to a biobank and/or when such data are shared, used and re-used by a diverse number of research institutions.
- … Applying this reasoning to a biobanking research context, both biobanks, researchers and entities conducting, sponsoring or financially supporting research, may be considered data controllers either by themselves or jointly.

Ana Nordberg (2021) "Biobank and Biomedical Research: Responsibilities of Controllers and Processors Under the EU General Data Protection Regulation." in Santa Slokenberga et al., "GDPR and Biobanking," Springer. https://link.springer.com/book/10.1007/978-3-030-49388-2

Relationship Between Controllers and Processors

- Territorial scope is also relevant here as often biobanking activities are conducted in collaboration with international research institutions and repositories.
- Firstly, the EDPB takes the view that the existence of a relationship between a controller and a processor does not necessarily trigger the application of the GDPR to both if one is not established in the Union. This means that 'when it comes to the identification of the different obligations triggered by the applicability of the GDPR, the processing by each entity must be considered separately'.
- Secondly, when an EU biobank acting as a controller uses a processor located outside the EU, it will be necessary for the controller to ensure by contract or other legal act that the processor will conduct its activities in accordance with the GDPR. This will include imposing on the processors by contract clauses all the relevant obligations placed by the GDPR on processors, and thus extending by contractual means the GDPR scope of application to processors outside the EU.
- Thirdly, the opposite situation— a biobank processing data on behalf of an institution/controller outside of the EU—is also a recurrent one. In such cases, while the provisions of the GDPR do not apply to the data controller, the biobank, as a processor established in the EU, will still continue to be required to comply with the GDPR obligations imposed on data processors provided that such activities are carried out in the context of its activities.

Ana Nordberg (2021) "Biobank and Biomedical Research: Responsibilities of Controllers and Processors Under the EU General Data Protection Regulation." in Santa Slokenberga et al., "GDPR and Biobanking," Springer. https://link.springer.com/book/10.1007/978-3-030-49388-2

Lawfulness of Data Processing

- The main restriction imposed on data controllers and processors is the duty to ensure the lawfulness of such activities.
- The GDPR contains two main legal bases for data processing of interest to biobanks: consent-based model and necessity-based model.
- It will remain critical to carefully consider which to apply to each data set because combining data sets based on different lawfulness grounds may generate increased compliance complexity.

Ana Nordberg (2021) "Biobank and Biomedical Research: Responsibilities of Controllers and Processors Under the EU General Data Protection Regulation." in Santa Slokenberga et al., "GDPR and Biobanking," Springer. https://link.springer.com/book/10.1007/978-3-030-49388-2

参考文献

- 国立大学法人政策研究大学院大学（2021）『国立研究開発法人及び国立大学法人等が研究目的により国内外の個人データを取り扱う場合の動向及び今後の課題等に関する調査分析報告書』. https://www.mext.go.jp/content/20210510-mxt_chousei01-100000404.pdf
- 岡村久道（2021）『個人情報保護法の知識』（第5版）日経文庫.
- 冨安泰一郎・中田響編著（2021）『一問一答　令和3年改正　個人情報保護法』商事法務.
- Santa Slokenberga et al. (2021), “GDPR and Biobanking,” Springer. https://link.springer.com/book/10.1007/978-3-030-49388-2