INFRASTRUCTURE BIOBANQUES

Règlement Général sur la Protection des Données - F.A.Q v.2.0

Traduit et adapté du document préparé par le Service Commun ELSI de BBMRI-ERIC (21/03/2017)

L'EQUIPE DU SERVICE ETHIQUE ET REGLEMENTATION

Responsable du service : Emmanuelle Rial-Sebbag

Juristes : Frédéric Le Corre
Gauthier Chassang

Document en version originale rédigé par le Common Service on Ethical Legal and Social Implications of biobanking (CS-ELSI) de l'Infrastructure pan-Européenne BBMRI-ERIC, disponible en anglais à cette adresse :

http://www.bbmri-eric.eu/news-events/answers-to-faqs-on-eu-gdpr-new-version-available-now/

1. INTRODUCTION

Le 24 mai 2016, le Règlement du Parlement Européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la Directive 95/46/CE (Règlement Général sur la Protection des Données Personnelles ou « RGDP ») est entré en vigueur. Le Règlement deviendra obligatoire dans son intégralité et sera directement applicable dans tous les Etats Membres à partir du 25 mai 2018.

Vous trouverez ci-dessous une mise à jour des réponses à la Foire Aux Questions (FAQ) sur l'impact du Règlement Général sur la Protection des Données Personnelles sur les activités des biobanques, sur les collections d'échantillons biologiques et sur les données de santé associées, dans l'Union Européenne. La FAQ n'a pas valeur de conseils juridiques et peut être sujette à des changements, résultant d'analyses ultérieures ou lorsque des dispositions du RGDP seront mises en œuvre. En application du RGPD, le chevauchement des obligations contenues dans d'autres législations nationales et européennes telles que figurant dans le Règlement (UE) n°536/2014 du Parlement Européen et du Conseil du 16 avril 2014 relatif aux essais cliniques de médicaments à usage humain et abrogeant la directive 2001/20/CE devraient être également prises en compte.

Cette FAQ étend la version publiée par le Service Commun ELSI de BBMRI-ERIC dans le cadre de sa Task Force sur le Règlement Général sur la Protection des Données en 2016. Les membres suivants de la Task Force ont participé à la conception de cette FAQ : Jasper Bovenberg (Pays-Bas), Martin Boeckhout (Pays-Bas), Gauthier Chassang (France), Irene Schlünder (Allemagne), Olga Tzortzatou (Grèce) et Ruth Vella Falzon (Malte).

2. QU'EST-CE QUE LE REGLEMENT GENERAL SUR LA PROTECTION DES DONNEES (RGPD) ?

Le Règlement Général sur la Protection des Données de l'Union Européenne est le nouveau cadre juridique à l'échelle de l'Union Européenne pour la protection des données personnelles. Les objectifs du Règlement sont de protéger les droits et libertés individuelles, en lien avec le traitement des données à caractère personnel, tout en facilitant la libre circulation de ces données dans l'Union Européenne. Cette libre circulation ne doit être ni limitée ou interdite pour des raisons tenant à la protection des personnes physiques au regard du traitement de leurs données personnelles. Le Règlement peut être téléchargé en différentes langues ici. Le texte officiel du Règlement été publié au Journal Officiel de l'Union Européenne dans toutes les langues officielles le 4 mai 2016 et peut être téléchargé ici.

3. COMMENT ET QUAND LE REGLEMENT VA-T-IL S'APPLIQUER ?

Le Règlement qui a été adopté en avril 2016, sera obligatoire dans son intégralité et sera directement applicable dans tous les Etats membres de l'Union européenne à partir du 25 mai 2018. Le Règlement abroge la Directive sur la Protection des Données (95/46/CE) et il surpassera les législations nationales relatives à la protection des données basées sur la Directive. Cependant, le Règlement fournit également une possibilité pour des dérogations au niveau national et européen et des spécificités pour certains domaines, ce qui comprend l'utilisation des données à caractère personnel à des fins de recherche scientifique.

4. EST-CE QUE LE RGPD AFFECTE L'ACTIVITE DES BIOBANQUES ?

Oui, en ce qui concerne les activités de collecte, de stockage et/ou de traitement d'échantillons biologiques humains, associés à des données personnelles, comprenant les données sensibles, telles que les données génétiques et de santé.

5. EST-CE QUE LE RGPD AFFECTE LE TRANSFERT DE DONNEES ENTRE LES BIOBANQUES EN EUROPE ?

Le RGPD dispose que la libre circulation des données personnelles ne doit être ni limitée ni interdite pour des raisons tenant à la protection des personnes physiques au regard du traitement de leurs données personnelles. Le RGPD autorise les Etats membres à maintenir ou à introduire d'autres conditions, y compris des limitations, au regard du traitement des données génétiques, des données biométriques ou des données qui concernent la santé. Cependant, ceci ne doit pas entraver la libre circulation des données personnelles dans l'UE, lorsque ces conditions s'appliquent au traitement transfrontalier de ces données.

6. QUELLES SONT LES NOUVEAUTES DU RGPD ?

Les principaux changements opérés par le RGPD par rapport à la précédente Directive européenne sur la protection des données sont les suivants :

- La transparence et la responsabilité (principe *d'accountability*) sont désormais des principes essentiels de la protection des données,
- Des dispositions spéciales viennent préciser les règles pour la recherche scientifique,
- Des droits enrichis pour les personnes concernées par le traitement de leurs données personnelles, tels que le droit à l'oubli et le droit à la portabilité des données,
- Des procédures obligatoires pour la gestion des violations de données à caractère personnel,
- Des dispositions particulières pour la protection des données des mineurs,
- Des procédures obligatoires relatives à des évaluations d'impact sur la protection des données,
- L'obligation de nommer un délégué à la protection des données (en France le Correspondant Informatique et Libertés, CIL) (sous réserve d'exceptions),
- Procédure de validation des Codes de Conduite Européens pour les organisations sans but lucratif,
- La certification de mécanismes spécifiques à la protection des données,
- Des dispositions sur des recours, sanctions et amendes.

7. QUELS SONT LES ELEMENTS PRINCIPAUX DU RGPD ?

Le RGPD contient un certain nombre de principes relatifs au traitement des données personnelles, aux droits des personnes concernées, et aux obligations des responsables du traitement et sous-traitants.

Le principe essentiel est que les données personnelles doivent être traitées « de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence) ». Pour la recherche

scientifique et les activités des biobanques, cela requerra un consentement éclairé des individus dont les données à caractère personnel sont traitées, à moins que la loi ne prévoit d'autres bases légales alternatives pour le traitement des données à caractère personnel (ex : permissions spécifiques prévues par la loi). Par ailleurs, les principes de minimisation de données et de limitation de la conservation sont particulièrement importants pour les activités de biobanques de recherche.

Les personnes concernées (ex : patients et participants contribuant à la recherche au travers de leurs données et échantillons) ont un certain nombre de droits face au(x) responsable(s) du traitement et sous-traitant(s) de leurs données. Ceux-ci incluent le droit de consentir, le droit d'être informé sur le traitement des données, le droit d'accéder aux données à caractère personnel, de rectifier ou de demander l'effacement de celles-ci (dit « droit à l'oubli »), ou de limiter le traitement des données relatives à la personne concernée, ainsi que le droit de s'opposer au traitement et le droit à la portabilité des données. Un certain nombre de ces droits peuvent être sujets à des limitations dans le cadre de la recherche scientifique lorsque cela est prévu par le droit des Etats membres ou par le droit de l'Union.

Les obligations du responsable du traitement et du sous-traitant englobent l'obligation d'établir des procédures claires et transparentes pour la protection des données, de veiller à la sécurité et la confidentialité des données, ainsi que d'assurer leur responsabilité (principe *d'accountability*) et d'être en mesure de démontrer la conformité aux règles du RGPD. La recherche scientifique peut connaitre certaines exceptions à ces obligations (voir ci-dessous).

8. LE RGPD CONTIENT-IL DES EXCEPTIONS POUR LES BIOBANQUES ?

Les biobanques peuvent être exemptées d'un certain nombre des principes généraux du RGPD, d'obligations et du respect des droits des personnes concernées, lorsqu'est effectué un traitement de données personnelles à des fins de recherche scientifique. Par exemple, par dérogation au principe de la limitation de la conservation des données, les données personnelles peuvent être conservées pour des durées plus longues lorsque celles-ci font l'objet d'un traitement à des fins de recherche scientifique en application des dispositions de l'article 89(1) du RGPD, et sujettes à l'implantation de mesures techniques et organisationnelles requises par le RGPD. En outre, le RGPD retient une présomption de compatibilité de l'utilisation des données à des fins de recherche, permettant ainsi davantage de traitements de données personnelles à des fins de recherche, initialement traitées à des fins différentes, à condition qu'il existe un fondement juridique valable pour le traitement initial dans l'Union européenne ou dans les législations des Etats membres.

Par ailleurs, le RGPD prévoit des exceptions à certains droits des personnes concernées dès lors que l'exercice de ces droits rendrait impossible, ou impacterait sérieusement la réalisation de la recherche, et à condition que ces dérogations soient nécessaires à l'accomplissement des objectifs de cette recherche. Ces dérogations étant nécessaires à l'accomplissement de ces objectifs. Un certain nombre de ces exceptions peuvent directement s'appliquer au cas-par-cas, alors que d'autres doivent être prévues par le droit de l'Union Européenne ou par les législations des Etats membres. Toutes ces exceptions sont assujetties à la mise en place de mesures techniques et organisationnelles devant assurer en particulier le respect du principe de la minimisation des données (comprenant par exemple des techniques d'anonymisation ou de pseudonymisation), telles que mentionnées à l'article 89, et le respect des standards éthiques pertinents. Pour d'autres exemples, se référer aux réponses en lien avec les différents principes, droits et obligations découlant du Règlement.

9. QUELLE RELATION Y'A-T-IL ENTRE LA PROTECTION DES DONNEES ET LA VIE PRIVEE

La « protection des données » est la terminologie juridique centrale du Règlement. La « vie privée » englobe la protection des données personnelles, mais comprend également les droits des individus à la vie privée et familiale ainsi que le respect de la confidentialité des correspondances et des communications.

10. QUELLE RELATION Y'A-T-IL ENTRE LA PROTECTION DES DONNEES ET LA SECURITE DES DONNEES ?

La « sécurité des données » est un élément de sauvegarde des droits et doit permettre de s'acquitter des obligations énoncées dans les lois de protection des données. Plus largement : la sécurité des données est une condition nécessaire (mais pas suffisante à elle seule) pour parvenir aux fins de protection des données. Des mesures de sécurité peuvent servir d'autres finalités qui ne sont pas nécessairement en lien avec la protection des données à caractère personnel, telle que la protection des intérêts commerciaux.

11. QUE SONT LES DONNEES ANONYMISEES/ANONYMES ?

Le RGPD s'applique seulement aux données personnelles, et non pas aux données anonymisées/anonymes (non-personnelles). Le Règlement ne fait pas la distinction entre les données anonymes et anonymisées.

Les données anonymisées/anonymes sont définies comme étant à l'opposer des données personnelles : « *informations ne concernant pas une personne physique identifiée ou identifiable, ni aux données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable* ».

L'anonymat n'est pas un état statique, cela dépend du contexte des connaissances et de « tous les moyens raisonnablement susceptibles d'être utilisés » afin de ré-identifier la personne derrière les enregistrements de données. Le fait de déterminer s'il faut qualifier des données de données anonymes doit être établi au cas par cas, ce qui requiert une évaluation des risques. Des « facteurs d'objectifs », (tels que le coût de l'identification et le temps nécessaire à celle-ci, la disponibilité des technologies au moment du traitement et l'évolution de celles-ci), doivent être pris en compte afin de décider de la qualification de ces données en pratique.

12. DE QUELLE FAÇON EST ACCOMPLIE L'ANONYMISATION ?

Il existe différentes méthodes, techniques et stratégies afin d'anonymiser les données à caractère personnel. Le RGPD ne se prononce pas en faveur d'une méthode spécifique.

En substance, le Règlement ne change pas la définition des données à caractère personnel et anonymes. Par conséquent, les méthodes qui rencontrent les standards établis par la Directive de 1995 sur la Protection des Données devraient toujours être pertinentes d'un point de vue légal, bien qu'elles doivent toujours faire l'objet d'évaluations face aux développements constant de la technique. Il existe de nombreuses techniques qui peuvent être utilisées, telles la suppression, les techniques de généralisation ou d'agrégation, de perturbation ou de dissociation des informations identifiantes. Voir notamment,

l'Avis publié par le Groupe de l'Article 29 sur les techniques d'anonymisation qui demeure pertinent avec le Règlement.

13. L'ANONYMISATION EST-ELLE UNE NECESSITE POUR LA RECHERCHE SCIENTIFIQUE ?

Le principe de la minimisation des données est une exigence du RGPD. Cela signifie que les données doivent être autant que possible dé-identifiées dans la mesure où les objectifs de la recherche peuvent être accomplis. Cependant, l'anonymisation ne sera pas toujours requise. D'autres moyens comme la pseudonymisation peuvent être également envisagés. Dans la mise en œuvre du principe de minimisation, les utilisations futures des données à des fins de recherche ainsi que le respect des droits des participants à la recherche devraient être pris en compte. En effet, l'anonymisation rend impossible la communication ultérieure avec les individus dont les données ont été enregistrées, afin par exemple de faire un retour sur les résultats de recherche ou pour demander un suivi d'informations. Par ailleurs, cela prive le participant du droit de retirer son consentement. Les analyses au cas par cas sont nécessaires.

14. QU'EST-CE QUE LA PSEUDONYMISATION DES DONNEES ?

Le RGPD définit la pseudonymisation comme « *le traitement de données à caractère personnel de telles façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable* ».

15. QUELLE DIFFERENCE Y'A-T-IL ENTRE ANONYMISATION ET PSEUDONYMISATION ?

Avec la pseudonymisation, l'attribution de données à des individus reste possible en utilisant des « informations additionnelles » (par exemple une clé ou un code de cryptage). Les données pseudonymisées restent *a priori* des données à caractère personnel. Pour les données anonymisées, de telles informations ne sont plus disponibles. Ces dernières ne sont donc pas à considérer comme des données à caractère personnel au sens du RGPD.

Les données pseudonymisées restent donc considérées comme des données à caractère personnel, alors que les données anonymisées ne le sont plus.

16. EST-CE QUE LE REGLEMENT REQUIERT LA PSEUDONYMISATION DES DONNEES POUR LA RECHERCHE SCIENTIFIQUE ?

La pseudonymisation est favorisée dans le Règlement comme étant l'une des méthodes principales pour réduire les risques associés au traitement des données personnelles et « aider les responsables du traitement et les sous-traitants à remplir leurs obligations en matière de protection des données ». Cependant, d'autres garanties (comme le cryptage) devront être envisagés et mises en œuvre

(Considérant 28 du préambule). Dans le même temps, la pseudonymisation n'est pas requise si cela empêche de poursuivre des objectifs particuliers de la recherche scientifique (article 89(1)).

17. QU'EST-CE QUE LE CONSENTEMENT ?

Le RGPD définit le « consentement » de la personne concernée comme « *l'acte positif clair par lequel la personne concernée manifeste de façon libre, spécifique, éclaire et univoque son accord au traitement des données à caractère personnel la concernant, par exemple au moyen d'une déclaration écrite, y compris par voie électronique, ou d'une déclaration orale* ». Le consentement est l'un des moyens de respecter les exigences du RGPD afin que le traitement des données à caractère personnel soit effectué de manière légale.

Le RGPD spécifie les conditions selon lesquelles les personnes concernées peuvent valablement donner leur consentement pour le traitement de leurs données à caractère personnel.

18. DE QUELLE MANIERE LE CONSENTEMENT DES PERSONNES CONCERNEES DOIT-IL ETRE OBTENU ?

Lorsque le traitement des données à caractère personnel est basé sur le consentement :

- Si le consentement de la personne concernée est donné dans le contexte d'une déclaration écrite qui concerne également d'autres matières, la demande afin d'obtenir le consentement devrait être présentée de manière à ce qu'elle soit clairement distinguée de ces autres matières.
- Le consentement doit être requis de manière intelligible et sous une forme accessible, utilisant un langage clair et commun.
- Le consentement doit être donné de façon libre.
- Le consentement doit être éclairé comme indiqué dans le RGPD (voir la FAQ sur les droits à l'information).
- Le consentement doit être fourni de façon claire par un acte positif (le silence, des cases pré-remplies ou l'inactivité ne sont pas considérées comme des formes valides de consentement au regard du RGPD).
- Le consentement peut être fourni sous la forme écrite, par des moyens électroniques, ou de manière orale.
- Le consentement doit comporter l'indication spécifique, éclairée et non équivoque de l'accord de la personne concernée au traitement des données.
- Le responsable du traitement doit être en mesure de démontrer que le traitement a été recueilli de manière de licite, même si le consentement a été fourni de manière orale.
- Les lois nationales peuvent maintenir ou introduire d'autres conditions relatives au consentement des personnes concernées dans des contextes spécifiques, par exemple au regard du traitement des données génétiques.

19. LES BIOBANQUES PEUVENT-ELLES AVOIR RECOURS A UN « CONSENTEMENT LARGE » AVEC LE REGLEMENT ?

Le Règlement reconnait que les finalités de la recherche scientifique ne peuvent pas toujours être spécifiées au moment de la collecte initiale des données. Cela permet donc aux biobanques de demander aux individus un consentement pour « certains domaines de la recherche scientifique, dans le respect des normes éthiques reconnues en matière de recherche scientifique ». Cependant, le Règlement indique que « *les personnes concernées devraient pouvoir donner leur consentement uniquement pour ce qui est de certains domaines de la recherche ou de certaines parties de projets de recherche, dans la mesure où la finalité visée le permet* » (considérant 33 du RGPD).

20. LES BIOBANQUES ONT ELLES BESOIN D'UN CONSENTEMENT POUR LE TRAITEMENT DE DONNEES SENSIBLES ?

Le RGPD dispose que le traitement de données personnelles sensibles (telles que les données génétiques ou de santé) est interdit. Cependant, le Règlement prévoit un certain nombre d'exceptions à cette interdiction. L'une de ces exceptions à cette interdiction est si la personne concernée a donné son consentement explicite au traitement. Mais le consentement ne constitue pas la seule exception. L'interdiction ne s'applique pas non plus lorsque le traitement est nécessaire pour des finalités de recherche scientifique conformément à l'article 89(1°) basé sur le droit de l'Union ou des membres ; traitement qui doit être proportionné au but poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour protéger les droits fondamentaux et les intérêts des personnes concernées.

21. QUELLES SONT LES DISPOSITIONS SPECIFIQUES RELATIVES AU CONSENTEMENT CONCERNANT LES ENFANTS ?

Les enfants méritent une protection spécifique vis-à-vis de leurs données à caractère personnel, parce qu'ils peuvent être moins conscient des risques, des conséquences et des garanties concernées et de leurs droits liés au traitement des données à caractère personnel. En ce qui concerne l'offre de services des sociétés d'information directement à un enfant, à moins que le droit d'un Etat membre spécifie un âge inférieur, le traitement des données personnelles relatives à un enfant est licite lorsque l'enfant est âgé d'au moins 16 ans. Lorsque l'enfant est âgé de moins de 16 ans, ce traitement n'est licite que si, et dans la mesure où, le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant.

22. EXISTE-T-IL DES DISPOSITIONS PARTICULIERES CONCERNANT LE TRAITEMENT DES DONNEES DE PERSONNES DECEDEES ?

Le Règlement ne s'applique pas aux données à caractère personnel des personnes décédées. Néanmoins, cette question peut être abordée dans les législations nationales, par exemple dans le cadre de la législation relative au secret professionnel. Par ailleurs, il est nécessaire de garder à l'esprit les considérations relatives aux droits constitutionnels ainsi qu'aux droits des personnes qui peuvent être avoir un intérêt quant au traitement relatif aux données à caractère personnel des personnes décédées.

23. EST-CE QUE LE RGPD REGLEMENTE LE SECRET PROFESSIONNEL ?

Le droit relatif au secret professionnel (pour les professionnels de santé tels que les médecins, les infirmières, etc.) peut fournir des dispositions légales additionnelles à respecter, en sus de la législation sur la protection des données [ex : article 9(2°, i)]. Le Règlement n'affecte pas les obligations relatives au secret professionnel. Lorsqu'elles sont applicables, le secret professionnel comme la législation sur la protection des données doivent être toutes les deux respectées.

24. QUELLES OBLIGATIONS SONT A RESPECTER AFIN DE FOURNIR L'INFORMATION AUX PERSONNES CONCERNEES ?

Différentes obligations sont impliquées selon la situation : si les données sont collectées auprès de la personne concernée (article 13) ; si les données sont collectées auprès d'un tiers (article 14) ; ou encore si les personnes concernées invoquent leur droit d'accès (article 15).

En vertu du Règlement, les biobanques qui collectent des données à caractère personnel relatives à leurs participants, doivent fournir à ces derniers des informations détaillées sur la manière dont sont traitées ces données. Ces obligations de fournir aux personnes concernées des informations sur le traitement des données existaient déjà en vertu de la législation précédente relative à la protection des données. Le RGPD complète ces obligations.

L'obligation de fournir cette information ne s'applique pas dans certains cas :

- Lorsque le participant a déjà reçu l'information ;
- Lorsque l'enregistrement ou la divulgation des données à caractère personnel est expressément prévu par la loi ;
- Si les données à caractère personnel ont été obtenues d'un tiers : lorsque la fourniture de l'information à la personne concernée se révèle impossible ou impliquerait des efforts disproportionnés. A cet égard, l'adoption de garanties appropriées devrait être prise en compte.

25. QUELLES INFORMATIONS DEVRAIENT ETRE FOURNIES AUX PERSONNES CONCERNEES SI LES DONNEES SONT COLLECTEES AUPRES DE LA PERSONNE CONCERNEE ?

Comme indiqué à l'article 13, les biobanques doivent fournir à leurs participants les informations suivantes au moment où les données sont obtenues *et* lorsque ces informations sont mises à jour (en application des principes généraux d'un traitement équitable et transparent) :

- L'identité et les coordonnées du responsable du traitement et, le cas échéant, du représentant du responsable du traitement ;
- Le cas échéant, les coordonnées du délégué à la protection des données ;
- Les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement ;

- Les destinataires ou les catégories de destinataires des données à caractère personnel, s'ils existent :
- Le cas échéant, le fait que le responsable du traitement a l'intention d'effectuer un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale, et l'existence ou l'absence d'une décision d'adéquation rendue par la Commission, ou, selon le cas, la référence aux garanties appropriées ou adaptées et les moyens par lesquels les participants peuvent en obtenir une copie ou l'endroit où elles ont été mises à disposition ;
- La durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée.
- L'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, la rectification ou l'effacement de celles-ci, ou une limitation du traitement relatif à la personne concernée, ou du droit de s'opposer au traitement et du droit à la portabilité des données ;
- Lorsque le traitement des données à caractère personnel par les biobanques est fondé, entre autres, sur le consentement, l'existence du droit de retirer son consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci ;
- Le droit des participants d'introduire une réclamation auprès d'une autorité de contrôle ;
- L'information de tout traitement de données à caractère personnel avec une autre finalité que celle pour laquelle les données ont été collectées en premier lieu, et toute autre information pertinente comme mentionné plus haut.

26. QUELLES INFORMATIONS DEVRAIENT ETRE FOURNIES AUX PERSONNES CONCERNEES SI LES DONNEES ONT ETE COLLECTEES AUPRES DE TIERS ?

Comme indiqué à l'article 14, les biobanques doivent fournir à leurs participants les informations suivantes :

- L'identité et les coordonnées du responsable du traitement, et, le cas échéant, du représentant du responsable du traitement ;
- Le cas échéant, les coordonnées du délégué à la protection des données ;
- Les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement ;
- Le cas échéant, les destinataires ou les catégories de destinataires des données à caractère personnel ;
- Le cas échéant, le fait que le responsable du traitement a l'intention d'effectuer un transfert de données à caractère personnel à un destinataire dans un pays tiers ou une organisation internationale, et l'existence ou l'absence d'une décision d'adéquation rendue par la Commission, ou, selon le cas, la référence aux garanties appropriées ou adaptées et les moyens

par lesquels les participants peuvent en obtenir une copie ou l'endroit où elles ont été mises à disposition ;

- La durée pendant laquelle les données à caractère personnel seront conservées ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;
- L'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, la rectification ou l'effacement de celles-ci, ou une limitation du traitement relatif à la personne concernée, ainsi que du droit de s'opposer au traitement et du droit à la portabilité des données ;
- Lorsque le traitement des données à caractère personnel par les biobanques est fondé, entre autres, sur le consentement, l'existence du droit de retirer son consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci ;
- Le droit des participants d'introduire une réclamation auprès d'une autorité de contrôle ;
- Lorsque le traitement est basé sur des intérêts légitimes plutôt que sur le consentement (par exemple dans certains cas d'utilisations résiduelles ou secondaires de données), les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers ;
- Si les données ont été collectées auprès de tiers : la source d'où proviennent les données à caractère personnel et, le cas échéant, une mention indiquant qu'elles sont issues ou non de sources accessibles au public.

27. QUELLES INFORMATIONS DOIVENT ETRE FOURNIES AUX PERSONNES CONCERNEES LORSQU'ELLES INVOQUENT LEUR DROIT D'ACCES ?

Comme indiqué à l'article 15, lorsque les personnes concernées invoquent leur droit d'accès aux données, les biobanques doivent fournir aux participants la confirmation de savoir si oui ou non des données à caractère personnel les concernant font l'objet d'un traitement, et, lorsque c'est le cas, les biobanques doivent fournir l'accès aux données à caractère personnel et les informations suivantes :

- Les finalités du traitement ;
- Les catégories de données à caractère personnel concernées ;
- Les destinataires ou catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, en particulier les destinataires qui sont établis dans des pays tiers ou les organisations internationales ;
- Lorsque cela est possible, la durée de conservation des données à caractère personnel envisagée, ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;
- L'existence du droit de demander au responsable du traitement la rectification ou l'effacement de données à caractère personnel, ou une limitation du traitement des données à caractère personnel relatives à la personne concernée, où du droit de s'opposer à ce traitement ;
- Le droit d'introduire une réclamation auprès d'une autorité de contrôle ;

- Lorsque les données à caractère personnel ne sont pas collectées auprès de la personne concernée, toute information disponible quant à leur source ;
- L'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 22, paragraphes 1 et 4, et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée ;
- Lorsque les données à caractère personnel sont transférées vers un pays tiers ou à une autre organisation internationale, la personne concernée a le droit d'être informée des garanties appropriées, en vertu de l'article 46, en ce qui ce concerne ce transfert ;
- Le responsable du traitement fournit une copie des données à caractère personnel faisant l'objet d'un traitement. Le responsable du traitement peut exiger le paiement de frais raisonnables basés sur les coûts administratifs pour toute copie supplémentaire demandée par la personne concernée. Lorsque la personne concernée présente sa demande par voie électronique, les informations sont fournies sous une forme électronique d'usage courant, à moins que la personne concernée ne demande qu'il en soit autrement. Ce droit d'obtenir une copie ne doit pas porter atteinte aux droits et libertés d'autrui.

A noter que, les Etats membres peuvent fournir des dérogations à ce droit dans leurs législations nationales.

28. DE QUELLE MANIERE L'INFORMATION DOIT-ELLE ETRE FOURNIE AUX PERSONNES CONCERNEES ?

Conformément à l'article 12 et selon le principe de transparence, toute information adressée à la personne concernée ou au public, doit être délivrée d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples, et en outre, le cas échéant, la visualisation doit être utilisée. En particulier pour toute information destinée spécifiquement à un enfant, l'information et la communication doivent être adressées en des termes clairs et simples que l'enfant peut aisément comprendre. Toute personne concernée devrait se voir adresser ces informations. Ces informations sont fournies par écrit ou par d'autres moyens y compris, lorsque c'est approprié, par voie électronique. Lorsque la personne concernée en fait la demande, les informations peuvent être fournies oralement, à condition que l'identité de la personne concernée soit démontrée par d'autres moyens.

Les informations peuvent être fournies accompagnées d'icônes normalisées afin d'offrir une bonne vue d'ensemble, facilement visible, compréhensible et clairement lisible, du traitement prévu.

29. A QUEL MOMENT LES INFORMATIONS PEUVENT ELLES ETRE FOURNIES AUX PERSONNES CONCERNEEES ?

Lorsque des données sont collectées auprès de la personne concernée, les informations doivent être données au moment où les données sont obtenues, ainsi qu'au moment où les informations sont mises à jour, en application des principes généraux pour un traitement équitable et transparent. Lorsque les données sont collectées auprès de tiers et/ou sont utilisées pour des finalités secondaires, les informations doivent être fournies (article 14 (3°)) :

- Dans un délai raisonnable après avoir obtenu les données à caractère personnel, mais ne dépassant pas un mois, eu égard aux circonstances particulières dans lesquelles les données à caractère personnel sont traitées ;
- Si les données à caractère personnel doivent être utilisées aux fins de la communication avec la personne concernée, au plus tard au moment de la première communication à ladite personne ;
- S'il est envisagé de communiquer les informations à un autre destinataire, au plus tard lorsque les données à caractère personnel sont communiquées pour la première fois.

30. QUELLES EXCEPTIONS AUX DROITS A L'INFORMATION PEUVENT S'APPLIQUER ?

De manière générale, l'obligation de fournir une information ne s'applique pas quand et dans la mesure où la personne concernée a déjà obtenu les informations relatives au traitement. Dans le cas où les données à caractère personnel n'ont pas été obtenues auprès de la personne concernée (mais l'ont été auprès d'un tiers), l'obligation de fournir aux individus ces informations peut être dispensée si :

- La fourniture de telles informations à la personne concernée est impossible,
- La fourniture de telles informations impliquerait des efforts disproportionnés, et/ou
- Cette obligation risque de rendre impossible ou d'impacter sérieusement l'accomplissement des objectifs (de recherche) du traitement des données à caractère personnel.

Si une biobanque souhaite invoquer l'une ou l'autre de ces exceptions, elle devra établir que ces exigences sont remplies. Par ailleurs, l'invocation de ces exceptions est soumise à des conditions appropriées et de mesures de sauvegarde conformément à l'article 89, telles que des mesures techniques et organisationnelles, y compris la pseudonymisation, ainsi que des mesures visant à protéger les droits, libertés et intérêts légitimes des personnes concernées. Quoi qu'il en soit, ces mesures impliquent de rendre ces informations disponibles au public, par exemple, via le site internet de la biobanque.

Ces exceptions ne peuvent généralement pas être invoquées avec succès par les biobanques qui communiquent régulièrement avec leurs participants. Pour d'autres formes de recherche, comme pour l'utilisation résiduelle des banques de tissus et des registres de patients, ces clauses peuvent prévoir une certaine latitude sur la base d'un système d'*opt-out*. Toutefois, tout ceci dépendra fortement sur des spécificités de l'infrastructure, des recherches concernées, ainsi que des législations nationales.

Enfin, l'obligation de fournir des informations peut ne pas s'appliquer, lorsque des données à caractère personnel obtenues auprès d'un tiers sont également assujettis au secret professionnel, comme pour les médecins.

31. EXISTE-T-IL DE NOUVEAUX DROITS POUR LES PERSONNES CONCERNEES PAR LE TRAITEMENT DE LEURS DONNEES ?

Oui. Ces nouveaux droits incluent le droit à l'oubli, qui modifie le droit à l'effacement déjà existant, et le droit à la portabilité des données. De plus, un certain nombre de droits déjà existant ont été précisés. Ce sont les droits à l'information, à la rectification, à la limitation du traitement, le droit de s'opposer au traitement des données à caractère personnel, et le droit de ne pas être soumis à des mesures juridiques fondées uniquement sur le profilage automatisé. Le RGPD reconnait également le besoin de reconnaitre

une protection spéciale s'agissant des enfants en tant que personnes concernées au regard de ces traitements de leurs données personnelles et que leur soit fourni une information renforcée et adaptée, en particulier au regard du consentement pour le traitement des données à caractère personnel sensibles (telles que les données de santé, génétique, ou biométriques). Une information plus transparente et une communication sur les finalités et les formes du traitement des données, doivent être également fournies à la personne concernée quand les données sont traitées par des tierces parties.

32. LES DROITS DES PERSONNES CONCERNEES S'APPLIQUENT-ILS AUX BIOBANQUES ?

En application de l'article 89, le droit de l'Union Européenne ou des Etats membres peut prévoir des dérogations à un certain nombre de droits des personnes concernées, comprenant le droit d'accès, de rectification, la limitation du traitement relatif à la personne concernée ou encore le droit de s'opposer au traitement des données à caractère personnel quand celles-ci font l'objet d'un traitement à des fins de recherche scientifique. Ces dérogations sont soumises à des mesures techniques et organisationnelles (ex : pseudonymisation) qui doivent être mises en place afin de s'assurer du respect du principe de minimisation des données.

Ces dérogations sont applicables seulement si l'exercice de ces droits risque de rendre impossible ou d'impacter sérieusement l'accomplissement des objectifs du traitement des données à caractère personnel. Chaque fois que ces finalités peuvent être atteintes par un traitement ultérieur ne permettant pas ou plus l'identification des personnes concernées, il convient de procéder de cette manière.

33. LE NOUVEAU « DROIT A L'OUBLI » S'APPLIQUE-T-IL AUX BIOBANQUES ?

Le « droit à l'oubli » ne s'applique pas dans la mesure où le traitement des données personnelles est nécessaire pour des fins de recherche scientifique ou historique, ou à des fins statistiques conformément à l'article 89, dès lors que l'exercice de ce droit risque de rendre impossible ou d'entraver sérieusement la réalisation des finalités de ce traitement.

34. QU'EN EST-IL DU NOUVEAU DROIT A LA PORTABILITE DES DONNEES ?

Le RGPD introduit un « droit à la portabilité des données », c'est-à-dire le droit pour la personne concernée de recevoir les données la concernant, qu'elle a fourni à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées n'y fasse obstacle. La personne concernée a également le droit d'avoir ses données transmises directement d'un responsable du traitement à un autre. Ce droit s'applique que le traitement soit basé sur un consentement ou qu'il soit basé sur un contrat et lorsque le traitement est effectué par des moyens automatisés. A noter que, le droit à la portabilité des données ne fait pas parti de la liste des droits des personnes concernées auxquels les Etats membres peuvent déroger conformément à l'article 89(2) du Règlement.

« Les données déduites » et les « données dérivées » telles que les données résultant du séquençage génétique d'échantillons pourraient être exemptées de cette obligation, comme suggéré par une ligne directrice (non-obligatoire, projet) élaborée par le Groupe de travail de l'article 29 de l'Union

Européenne. D'autres spécifications supplémentaires sur la portée de cette loi à cet effet restent encore à être définies.

35. QU'EST-CE QUE LE PRINCIPE DE RESPONSABILITE (*ACCOUNTABILITY*) DESIGNE DANS LE RGPD ?

Le principe d'*accountability* fait référence à la responsabilité du responsable de traitement visant à assurer que les principes fondamentaux relatifs au traitement des données à caractère personnel sont respectés, tout comme la capacité à pouvoir démontrer cette conformité.

36. QU'EST-CE QUE LE PRINCIPE DE TRANSPARENCE (*TRANSPARENCY* DESIGNE DANS LE RGPD ?

La transparence est l'un des principes essentiels du RGPD. Il requiert en particulier que les personnes concernées soient informées sur, comment et par qui les données les concernant sont traitées, ainsi que sur « le droit d'obtenir la confirmation et la communication que des données à caractère personnel les concernant font l'objet d'un traitement » (considérant 39), « en prenant en compte les circonstances spécifiques et le contexte dans lesquels les données à caractère personnel sont traitées » (considérant 60).

37. LES BIOBANQUES DOIVENT-ELLES DESIGNER UN DELEGUE A LA PROTECTION DES DONNEES ?

Puisque les activités de base des Biobanques consistent en des opérations de traitements qui requièrent une surveillance régulière et systématique des données des personnes concernées à une large échelle, un délégué à la protection des données doit être désigné par le responsable du traitement de la Biobanque ou le(s) sous-traitant(s) afin qu'il les assiste à contrôler la conformité avec le Règlement. Ces délégués à la protection des données, qu'ils soient ou non employés du responsable du traitement, doivent être en mesure de mener à bien leurs fonctions et tâches de manière indépendante.

Les organismes comptant moins de 250 employés sont exemptés de cette obligation en application du Règlement. A noter, cependant, que ce sont tous les employés de l'organisation à laquelle est rattaché la biobanque qui doivent être pris en compte pour calculer le nombre total d'employés. Par exemple, la biobanque peut faire partie d'un hôpital universitaire ou d'une université.

38. QUE DIT LE REGLEMENT SUR LES VIOLATIONS DE DONNEES A CARACTERE PERSONNEL ?

Selon le RGPD, la violation de données à caractère personnel est « *une violation de la sécurité entrainant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données* ».

Dès que le responsable du traitement apprend qu'une violation de données à caractère personnel s'est produite, il convient qu'il la notifie à l'autorité de contrôle dans les meilleures délais et, lorsque c'est possible, 72 heures au plus tard après en avoir pris connaissance, à moins qu'il ne puisse démontrer, conformément au principe de responsabilité, qu'il est peu probable que la violation en question engendre

un risque pour les droits et libertés des personnes physiques. Si une telle notification ne peut avoir lieu dans ce délai de 72 heures, la notification devrait être assortie des motifs du retard et des informations peuvent être fournies de manière échelonnée sans autre retard indu.

Le responsable du traitement devrait communiquer une violation de données à caractère personnel à la personne concernée dans les meilleurs délais lorsque cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés de la personne physique afin qu'elle puisse prendre les précautions qui s'imposent.

39. LES BIOBANQUES DOIVENT-ELLES PROCEDER A UNE ANALYSE D'IMPACT RELATIVE A LA PROTECTION DES DONNEES ?

Oui probablement, en supposant qu'elles s'engagent dans un type de traitement de données à caractère personnel, en particulier à l'aide de nouvelles technologies, ce qui, compte tenu de la nature, de l'étendue, du contexte et des finalités du traitement, est susceptible d'entrainer un risque élevé pour les droits et libertés des personnes physiques (par exemple quand il s'agit de traitements à une large échelle de catégories particulières de données, telles que les données de santé et les données génétiques). C'est l'autorité de surveillance d'un Etat membre qui établit et publie une liste du type d'opérations de traitements qui sont soumises à l'obligation d'une évaluation d'impact relative à la protection des données ; veuillez-vous référer à votre autorité de contrôle afin de vérifier si votre type de traitement a été inscrit. En outre, l'autorité de contrôle peut établir et rendre publique une liste du type de traitements pour lesquels aucune analyse d'impact relative à la protection des données n'est requise. Les chances que les traitements de données sensibles menés par les biobanques soient inscrits sur cette liste sont minces, mais veuillez néanmoins vous référer à votre autorité de contrôle. Une seule évaluation peut porter sur des opérations de traitements similaires et qui présentent des risques élevés similaires.

40. EST-CE QUE LE RGPD S'APPLIQUERA AU ROYAUME-UNI APRES LE BREXIT ?

Dans l'ensemble, pour assurer la sécurité juridique au Royaume-Uni après la sortie de l'Union européenne, le Libre blanc du Royaume-Uni fixant ses plans en vue de la négociation à venir avec ses partenaires européens sur la sortie de l'Union européenne, prévoit que le Gouvernement introduise le « *Great Repeal Bill* » afin de supprimer le « *European Communities Act* » de 1972 des textes de lois et de transposer le corps existant de règles européennes en droit interne. Cela signifie que, de façon pratique et éclairée, les mêmes règles et lois s'appliqueront le jour suivant le départ du Royaume-Uni de l'Union européenne, comme cela était le cas auparavant.

Le Royaume-Uni sera toujours membre de l'Union européenne le 25 mai 2018, ainsi le RGPD deviendra automatiquement obligatoire au Royaume-Uni à cette date. Le mercredi 1er février 2017, le sous-comité des affaires intérieures de l'Union européenne a recueilli des témoignages du député Matt Hancock, Ministre d'Etat chargé de la culture et des médias et du Département de la culture, des médias et des sports, sur le RGPD sur la protection des données. Il a déclaré que le que le gouvernement britannique appliquerait pleinement le RPGD pour deux raisons principales :

- « Grâce à d'importants succès de négociations durant son développement, nous pensons que c'est une bonne mesure législative en soi ».

- « Nous souhaitons assurer un flux de données sans entraves entre le Royaume-Uni et l'Union européenne post-Brexit, et nous pensons que la signature du RGPD sur les règles de protection des données est un élément important pour aider à aboutir à ce résultat ».

Même si le Royaume-Uni met pleinement en œuvre le RGPD post-Brexit, il deviendrait un « pays tiers ». A ce stade, la libre circulation des données entre le Royaume-Uni et le l'UE serait tributaire d'arrangements similaires à ceux actuellement en place pour permettre des flux de données vers d'autres pays tiers à l'extérieur de l'Union européenne. Une option serait pour le Royaume-Uni de solliciter une « décision d'adéquation » (voir plus loin).

41. COMMENT LES DONNEES PERSONNELLES PEUVENT-ELLES ETRE TRANSFEREES EN DEHORS DU TERRITOIRE DE L'UNION EUROPEENNE ?

Un transfert de données à caractère personnel vers un pays tiers peut avoir lieu lorsque la Commission a constaté par voie de décision que le pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, assure un niveau adéquat de protection. L'effet d'une telle « décision d'adéquation » est que les données à caractère personnel peuvent circuler de l'Union européenne vers des pays tiers ou des secteurs, sans autres garanties. Un tel transfert ne requiert aucune autorisation spécifique.

En l'absence d'une décision d'adéquation de la Commission, un responsable de traitement ou un sous-traitant peut transférer des données à caractère personnel vers pays tiers seulement s'il a prévu des garanties appropriées et à la condition que les personnes concernées disposent de droits opposables et de voies de droit effectives. Les garanties appropriées peuvent être fournies par des clauses types de protection des données adoptées par la Commission. Elles peuvent également être fournies par un code de conduite approuvé ou par un mécanisme de certification, assortis de l'engagement contraignant et exécutoire du responsable du traitement ou le sous-traitant dans le pays tiers, d'appliquer les garanties appropriées, y compris en ce qui concerne les droits des personnes concernées.

En l'absence d'une décision d'adéquation ou de garanties appropriées, un transfert ou un ensemble de transferts de données à caractère personnel vers un pays tiers peut avoir lieu à la condition que, la personne concernée a explicitement donné son consentement au transfert proposé, et ce, après avoir été informée des risques possibles s'agissant de tels transferts du fait de l'absence d'une décision d'adéquation et de garanties appropriées.

42. LES BIOBANQUES PEUVENT-ELLES CONTINUER A OPERER DES TRANSFERTS DE DONNEES PERSONNELLES VERS LES ETATS-UNIS ?

Oui, sous réserve du respect des dispositions générales de transfert pour le transfert des données en dehors de l'Union Européenne, discutées dans la question ci-dessus. Les transferts effectués dans le respect des principes du Safe Harbour ne sont désormais plus valides. De nouvelles règles (*Privacy Shield*) sont encore en négociations.

43. EST-CE QUE LES BIOBANQUES PEUVENT TRANSFERER DES DONNEES A CARACTERE PERSONNEL VERS LES ETATS-UNIS EN SE FONDANT SUR LE PRIVACY SHIELD « UE-US » ?

Seulement si l'organisation qui reçoit ces données est répertoriée dans le cadre du *Privacy Shield* et que les données relèvent des données couvertes par la liste.

Le 12 juillet 2016, la Commission européenne a considéré le *Privacy Shield* UE-US adéquat pour autoriser le transfert de données de l'Union européenne vers les Etats-Unis en vertu de la législation européenne (le *Privacy Shield* remplaçant les précédents accords de *Safe Harbor* entre l'Union européenne et les Etats-Unis).

Les données à caractère personnel sont transférées dans le cadre du *Privacy Shield* entre l'UE et les US, de l'Union européenne vers des entreprises aux Etats-Unis qui sont incluses dans la « liste du *Privacy Shield* », tenue et rendue publique par le Département du Commerce des Etats-Unis. Le transfert de données à caractère personnel à une telle entreprise serait alors qualifié de transfert valide en vertu du Règlement. Toute entreprise qui est soumis à la compétence de la *Federal Trade Commission* (FTC) ou au Département des Transports (*Departement of Transportation* - DOT) peut participer au *Privacy Shield*. Généralement, la compétence de la FTC couvre les actes ou les pratiques relatifs au commerce. A toutes fins pratiques, il est peu probable que les organismes de recherche universitaire et les organismes sans but lucratif soient admissibles à être inscrits dans le cadre du *Privacy Shield*. Par conséquent, les biobanques ne peuvent pas faire reposer leurs transferts de données à caractère personnel sur le *Privacy Shield*. Cela peut être différent pour les institutions commerciales, à condition bien sûr qu'elles soient répertoriées, et que les données à transférer soient couvertes par la liste (par exemple, 23andMe). La liste du *Privacy Shield* peut être consultée ici.

44. EST-CE QUE LES BIOBANQUES PEUVENT TRANSFERER DES DONNEES A CARACTERE PERSONNEL VERS LES ETATS-UNIS EN SE FONDANT SUR LE PRIVACY SHIELD « SUISSE-US » ?

En ce qui concerne la Suisse (pays non-membre de l'UE), en janvier 2017, le Conseil Fédéral a indiqué qu'un nouveau cadre, le *Privacy Shield*, a été établi pour le transfert de de données à caractère personnel de la Suisse vers les Etats-Unis. Avec l'introduction du *Privacy Shield*, les mêmes normes s'appliquent aux exportations suisses de données à caractère personnel vers les Etats-Unis que pour les exportations de données depuis l'Union européenne. Le Commissaire fédéral à la protection des données à l'information (FDPIC), comme les autres autorités de surveillance des Etats membres de l'UE, servira de point de contact pour les personnes en Suisse en cas de problèmes liés aux transferts de données vers les Etats-Unis.

En ce qui concerne le transfert des données à caractère personnel sensibles (telles que définies à l'article 9(1°), comprenant par exemple les données médicales, génétiques et génomiques) à des fins de recherche, bien que cela ne soit pas obligatoire au titre du RGPD, il est recommandé d'utiliser des mesures contractuelles supplémentaires, afin de définir spécifiquement les activités en termes de finalités, de méthodologies, de gestion des données confidentielles et de protection des droits des personnes concernées. Un tel contrat peut prendre la forme d'un accord de transfert de données (DTA) ou d'un accord de matériel (MTA)

45. COMMENT LE NON-RESPECT DE LA REGLEMENTATION VA-T-IL ETRE SANCTIONNE ?

Le Règlement prévoit trois types de mécanismes pour appliquer ses dispositions : des mesures correctives, des amendes et des pénalités.

Toute autorité de contrôle dispose d'un ensemble de mesures correctives, lesquelles incluent : l'émission d'avertissements ou de réprimandes, l'imposition d'une limitation ou même d'une interdiction de traitement, pouvoir ordonner la rectification ou l'effacement de données à caractère personnel, et pouvoir imposer des amendes administratives au responsable de traitement ou au sous-traitant.

Les violations des principes de base d'un traitement, y compris les conditions applicables au consentement, mais également les violations des droits dont bénéficient les personnes concernées et les transferts de données à caractère personnel à un destinataire situé dans un pays tiers ou à une organisation internationale peuvent faire l'objet d'amendes administratives pouvant aller jusqu'à 20.000.000€.

Les Etats membres déterminent le régime des autres sanctions applicables en cas de violations du présent Règlement en particulier pour les violations qui ne font pas l'objet des amendes administratives prévues à l'article 83, et prennent toutes les mesures nécessaires pour garantir leur mise en œuvre.

Changements apportés par rapport à la précédente version de la F.A.Q :

- Modifications apportées en introduction ;
- Modifications apportées au point 2 « Qu'est-ce que le règlement général sur la protection des données (RGPD) ? » ;
- Création d'un point 3 « Comment et quand le règlement va-t-il s'appliquer ? » ;
- Modifications apportées au point 7 « Quels sont les éléments principaux du RGPD ? » ;
- Modifications apportées au point 8 « Le RGPD contient-il des exceptions pour les biobanques ? » ;
- Création d'un point 9 « Quelle relation y'a-t-il entre la protection des données et la vie privée ? » ;
- Création d'un point 10 « Quelle relation y'a-t-il entre la protection des données et la sécurité des données ? » ;
- Modifications apportées au point 12 « De quelle façon est accomplie l'anonymisation ? » ;
- Modifications apportées au point 15 « Quelle différence y'a-t-il entre anonymisation et pseudonymisation ? » ;
- Création des points 17 et 18 sur le consentement ;
- Modifications apportées aux points 19, 20 et 21 sur le consentement ;
- Création des points 22 à 30 ;
- Modifications apportées au point 34 sur le droit à la portabilité des données ;
- Création des points 35 et 36 sur les principes de responsabilité et de transparence ;
- Création des points 39 et 40 ;
- Modifications apportées au point 41 sur le transfert des données personnelles en dehors du territoire de l'Union européenne ;
- Création des points 43 et 44 sur le transfert des données vers les Etats-Unis et la Suisse ;

Pour toute demande d'information liée à une question éthique ou juridique concernant l'interprétation du RGPD, vous pouvez vous adresser au service éthique et règlementation de l'Infrastructure BIOBANQUES en suivant l'adresse suivante :

http://www.biobanques.eu/fr/demande-de-prestations