Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

GDK Schweizerische Konferenz der kantonalen Gesundheitsdirektorinnen und -direktoren
CDS Conférence suisse des directrices et directeurs cantonaux de la santé
CDS Conferenza svizzera delle direttrici e dei direttori cantonali della sanità

eHealth Suisse

Applicabilité aux communautés de référence et aux communautés de la législation de l'UE en matière de protection des données

Une aide à la mise en œuvre

Berne, mai 2019

ehealthsuisse
Kompetenz- und Koordinationsstelle
von Bund und Kantonen

Centre de compétences et de coordination
de la Confédération et des cantons

Centro di competenza e di coordinamento
di Confederazione e Cantoni

Impressum
© eHealth Suisse, Centre de compétences et de coordination de la Confédération et des cantons

Licence : Ce résultat appartient à eHealth Suisse (Centre de compétences et de coordination de la Confédération et des cantons). Le résultat final sera publié par les canaux d'information appropriés sous la licence Creative Commons de type « Attribution – Partage dans les mêmes conditions 4.0 ». Texte de la licence : https://creativecommons.org/licenses/by-sa/4.0

Autres informations et sources : www.e-health-suisse.ch

Identification du présent document
OID : 2.16.756.5.30.1.127.1.2.5.1.1

Autres informations et sources :
www.e-health-suisse.ch

Objectif et positionnement du présent document
La présente aide à la mise en œuvre contient une présentation générale de l'application aux communautés de référence et aux communautés de la législation de l'UE en matière de protection des données au sens de l'art. 2, let. d et e, en relation avec l'art. 10 LDEP. Il est à noter que le présent guide n'est pas destiné à remplacer une analyse approfondie du cas d'espèce et que son application se fait toujours aux risques et périls de son utilisateur. En cas de doute, il est recommandé de s'adresser à un spécialiste de la protection des données.

La présente aide à la mise en œuvre a été élaborée par Barbara Widmer, docteur en droit, LL.M, CIA, en collaboration avec eHealth Suisse et avec le concours du groupe de travail temporaire Applicabilité du règlement général sur la protection des données de l'UE aux communautés (de référence), des groupes de coordination Communautés de référence et cantons ainsi que du comité consultatif des acteurs de la mise en œuvre et des utilisateurs. La présente aide à la mise en œuvre est disponible sur www.e-healthsuisse.ch. Les aides à la mise en œuvre d'eHealth Suisse donnent aux acteurs concernés des conseils sur la manière de remplir une mission dans l'environnement des réseaux numériques. Ces acteurs peuvent décider eux-mêmes s'ils veulent suivre ou non ces propositions et recommandations. Le présent document n'est pas juridiquement contraignant. Il appartient dans tous les cas aux organismes de certification de juger en dernier ressort de la conformité avec les prescriptions légales.

Afin de faciliter la lecture de ce document, il a été renoncé à utiliser systématiquement les formes masculine et féminine. En l'absence de mention contraire, le masculin désigne les deux sexes.

Table des matières

1 Contexte

Contexte

Dans le cadre de la constitution de communautés de référence et de communautés, la question s'est posée, compte tenu de l'entrée en vigueur en mai 2018 de la nouvelle législation de l'UE en matière de protection des données, de savoir dans quelle mesure les traitements de données effectués par les communautés de référence et communautés pourraient entrer dans le champ d'application de cette législation de l'UE.

But du guide

Le présent guide explique à quel moment la législation de l'UE en matière de protection des données trouve application hors de l'UE, ce dont il faut tenir compte à ce sujet et quelles sont les conséquences qui en découlent pour les communautés de référence et communautés. Il montre, par ailleurs, comment il est possible à certaines conditions d'éviter que la législation de l'UE en matière de protection des données ne soit applicable.

2 Nouvelle législation de l'UE en matière de protection des données

Nouvelle législation de l'UE en matière de protection des données

La législation de l'UE en matière de protection des données est entrée en vigueur le 25 mai 2018. Elle se compose actuellement du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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, abrégé RGPD)[1].

Règlement « vie privée et communications électroniques »

Il est prévu qu'entre 2020 et 2022, un deuxième acte législatif réglant en particulier les communications électroniques, la publicité électronique et le suivi sur internet entre en vigueur. Il s'agit de la Proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques, et abrogeant la directive 2002/58/CE (règlement « vie privée et communications électroniques », abrégé règlement ePrivacy)[2].

Champ d'application

La législation de l'UE en matière de protection des données s'applique en premier lieu aux traitements des données réalisées par des institutions qui se trouvent à l'intérieur de l'UE. Elle contient toutefois des normes qui peuvent conduire à ce que des traitements de données réalisés par des institutions qui se trouvent à l'extérieur de l'UE (p. ex. en Suisse) se trouvent également régis par cette même législation de l'UE.

[1] JO L 119/1 du 4.5.2016
[2] COM(2017) 10 final

3 Conditions d'application

Application extraterritoriale

Il existe en particulier deux situations dans lesquelles la législation de l'UE en matière de protection des données est applicable à des institutions à l'extérieur de l'UE et donc également en Suisse (application extraterritoriale)[3] :

- Situation 1 : La législation de l'UE en matière de protection des données s'applique lorsqu'une institution qui se trouve en Suisse offre des biens ou des services à des personnes qui se trouvent au sein de l'UE.

ou

- Situation 2 : La législation de l'UE en matière de protection des données s'applique lorsque des personnes qui se trouvent au sein de l'UE sont observées au moyen d'outils d'analyse lors de leur visite du site internet d'une institution qui se trouve en Suisse (2).

3.1 Situation 1 : Offre de biens et de services à des personnes au sein de l'UE

3.1.1 Aspects juridiques

Conditions à remplir pour la première situation

Le premier cas d'application extraterritoriale de la législation de l'UE en matière de protection des données implique qu'une institution qui se trouve en Suisse offre (cf. 3.1.1.1) des biens ou des services (cf. 3.1.1.2) à des personnes au sein de l'UE (cf. 3.1.1.3). Pour être considérée comme une offre de biens et de services à des personnes au sein de l'UE entrant dans le champ d'application de la législation de l'UE en matière de protection des données, celle-ci doit donc remplir trois conditions :

3.1.1.1 Offre

Il convient de vérifier dans tous les cas s'il s'agit d'une offre au sens de la législation de l'UE en matière de protection des données. Toutes les formes d'offres ne remplissent pas cette condition.

Offre au sens du RGPD de l'UE

Une offre au sens de la législation de l'UE en matière de protection des données ne nécessite pas de comportement actif de la part de l'institution prestataire. Le fait de mettre passivement à disposition une offre de biens ou de services peut également constituer une offre au sens de la législation de l'UE en matière de protection des données. On partira toutefois du principe que le simple fait de permettre aux personnes dans l'Union d'accéder à un site internet ne constitue pas une offre au sens de la législation de l'UE en matière de protection des données. Il faut une combinaison d'éléments supplémentaires comme, p. ex., des offres en euros et/ou l'utilisation de langues spécifiques à des pays de l'UE (en Suisse, l'utilisation des langues nationales que sont l'allemand, le français et l'italien ne constitue toutefois pas un indice), des noms de domaine avec un domaine de premier niveau de pays autres que celui dans lequel l'institution se trouve (pas .ch, mais par exemple .de, .pl, .at) ou la description d'itinéraires d'accès depuis l'étranger jusqu'au lieu en Suisse où se trouvent les biens ou les services.

[3] Cf. art. 3, al. 2, let. a et b, RGPD

Prise en compte du cas d'espèce

On retiendra globalement que pour déterminer dans quelle mesure il s'agit d'une offre au sens de la législation de l'UE en matière de protection des données, il faut toujours s'en référer au cas d'espèce, et que cette évaluation n'est pas toujours possible avec une certitude absolue.

3.1.1.2 Biens ou services

Définition des biens et des services

La deuxième condition est que des biens et des services doivent être offerts. La législation de l'UE en matière de protection des données ne définit pas ce qu'il faut entendre par biens et services. Il est possible en recourant à d'autres actes législatifs de l'UE de définir les **biens** comme étant tous les biens meubles corporels qui ont une valeur monétaire et qui peuvent faire l'objet de transactions commerciales. En font également partie, outre les marchandises conventionnelles, les sources d'énergie (pétrole, gaz, électricité), les semences, les animaux, les déchets, les objets d'art ou les supports de biens immatériels (p. ex. les supports de sons ou d'images). Selon la doctrine, la notion de **services** doit être comprise au sens large. Elle comprend notamment tous les types de services internet tels que les plateformes de réservation (p. ex. en matière de voyages), les offres de cloud, d'applications, de réseaux sociaux ou les services de streaming. Le fait qu'un service soit proposé à titre onéreux ou gratuit ne joue aucun rôle.

3.1.1.3 Personnes qui se trouvent au sein de l'UE

L'UE en tant que lieu de séjour du client

La dernière condition est que l'offre de biens et de services doit s'adresser à des personnes qui, au moment du traitement des données, se trouvent au sein de l'UE. La nationalité de ces personnes ne joue aucun rôle.

3.1.2 Signification pour les communautés de référence et communautés

Tâches des communautés (de référence)

Les tâches des communautés de référence et communautés sont réglées à l'art. 10 LDEP[4] et aux art. 9 ss ODEP[5]. Selon l'art. 10 LDEP, elles comprennent en particulier les activités suivantes :

- s'assurer que les données du DEP[6] soient accessibles (al. 1, let. a)
- consigner dans un historique chaque traitement de données (al. 1, let. b)

Les communautés de référence doivent par ailleurs :

- gérer les déclarations de consentement et de révocation des patients (al. 2, let. a)
- donner aux patients la possibilité de gérer les droits d'accès des professionnels de la santé ou d'accéder à leur propre DEP et de pouvoir y saisir eux-mêmes des données (al. 2, let. a et b)

Organisation des tâches

Les tâches des communautés de référence et communautés sont donc essentiellement de nature administrative. Les communautés de référence et communautés sont chargées de l'infrastructure et de l'exploitation des DEP, mais pas de leur commercialisation. Les communautés de référence et communautés disposent certes de leurs propres sites internet, mais ceux-ci ne poursuivent dans la mesure où il est possible d'en juger qu'un but purement informatif et illustratif. Ces sites internet permettent aux

---

4 Loi fédérale du 19 juin 2015 sur le dossier électronique du patient (LDEP), RS **816.1**
5 Ordonnance du 22 mars 2017 sur le dossier électronique du patient (ODEP), RS **816.11**
6 Abréviation pour « dossier électronique du patient » (DEP)

communautés de référence ou aux communautés de se présenter (organisation, activités, membres, etc.). Les sites internet fournissent par ailleurs des indications quant à l'utilisation et au fonctionnement du DEP.

Ouverture d'un DEP

En ce qui concerne l'ouverture d'un DEP, tout porte à croire en l'état actuel des connaissances soit qu'une personne prendra elle-même l'initiative d'ouvrir un DEP, soit que les institutions de soins (p. ex. des hôpitaux, des médecins) lui signaleront à l'occasion d'un traitement concret la possibilité d'ouvrir un DEP. La possibilité d'ouvrir un DEP est en principe également ouverte aux personnes au sein de l'UE pour autant qu'elles disposent d'un numéro AVS et qu'elles se fassent soigner en Suisse (notamment les frontaliers). Pour cette catégorie de personnes également, tout porte à croire que soit elles prendront elles-mêmes l'initiative d'ouvrir un DEP, soit que les institutions de soins (p. ex. des hôpitaux, des médecins) leur signaleront à l'occasion d'un traitement concret la possibilité d'ouvrir un DEP. Les communautés de référence et communautés ne devraient donc en règle générale pas être directement impliquées dans l'ouverture des dossiers électroniques des patients.

Le DEP en tant que service

Au vu de ce qui précède, rien ne donne à penser que les communautés de référence et communautés offrent le DEP en tant que service à des personnes qui se trouvent au sein de l'UE. La première situation qui pourrait conduire à l'application de la législation de l'UE en matière de protection des données ne devrait donc pas concerner les communautés de référence et communautés.[7]

Examen distinct en cas d'offre de services complémentaires

Si une communauté de référence ou une communauté offre des services complémentaires (p. ex. une plateforme de prise de rendez-vous) par le biais de son infrastructure, elle doit toutefois examiner dans quelle mesure leur mise en œuvre pourrait constituer une « offre de biens ou de services à l'attention de personnes au sein de l'UE » au sens de la législation de l'UE en matière de protection des données. Ces services complémentaires sont offerts par les communautés de référence et communautés en dehors de la législation concernant le DEP et ils n'ont donc aucun lien avec les tâches qui découlent des art. 10 LDEP et 9 ss ODEP. Le fait que ces services complémentaires peuvent également être utilisés par des personnes au sein de l'UE ne devrait toutefois en soi pas encore conduire à l'applicabilité de la législation de l'UE en matière de protection des données.

Prise en compte séparée des services complémentaires par la législation de l'UE en matière de protection des données

Si l'examen des services complémentaires devait aboutir à la conclusion que ceux-ci conduisent à l'applicabilité de la législation de l'UE en matière de protection des données, seuls les traitements de données effectués dans le cadre des services complémentaires correspondants seraient toutefois concernés par la législation de l'UE en matière de protection des données, et non l'ensemble des traitements de données réalisés par la communauté de référence ou la communauté. Dans un tel cas, le domaine des DEP ne serait donc pas concerné par l'applicabilité de ladite législation de l'UE.

---

[7] On signalera au sujet de cette affirmation qu'elle ne peut pas être formulée avec une sécurité absolue et que, dans un cas concret, il n'est donc pas exclu que l'autorité de protection des données d'un État membre de l'UE ou qu'un tribunal saisi de la cause puisse aboutir à une autre appréciation.

3.2 Situation 2 : Observation du comportement (suivi et profilage)

3.2.1 Aspects juridiques

La législation de l'UE en matière de protection des données s'applique par ailleurs lorsqu'une institution qui se trouve en Suisse traite des données au sujet de personnes physiques afin d'observer le comportement de ces personnes (cf. 3.2.1.1.) dans la mesure où le comportement a lieu au sein de l'UE (cf. 3.2.1.2.). Deux conditions doivent donc être réunies pour qu'un suivi et un profilage soient soumis à la législation de l'UE en matière de protection des données :

Conditions à remplir pour la deuxième situation

3.2.1.1 Observation du comportement des personnes

La deuxième situation se réfère exclusivement aux traitements des données qui servent à **observer les activités sur internet d'une personne physique** (suivi), y compris l'utilisation de techniques de création d'un profil de la personne concernée grâce auquel il est possible d'analyser ou de prédire ses préférences ou ses comportements (profilage).

Observation par le biais d'un suivi et d'un profilage

Pour être considérée comme une observation, celle-ci doit présenter une certaine durée et une certaine intensité. Le recours à des outils d'analyse tels que des cookies ou des plugins sociaux (p. ex. le bouton « J'aime » de Facebook) ainsi que le recours à des services à valeur ajoutée (qui complètent de manière individuelle les services de base) servent en particulier toujours à l'observation au sens de la législation de l'UE en matière de protection des données.

En ce qui concerne les sites internet qui utilisent des outils de suivi et de profilage, il faut partir de l'idée que pour que cela soit considéré comme une observation au sens de la législation de l'UE en matière de protection des données, le fait que le site internet s'adresse ou non concrètement à des personnes qui se trouvent au sein de l'UE ne joue pas de rôle (contrairement à ce qui se passe en matière d'offre de biens et de services (cf. 3.1.1.1 ci-dessus). Tout exploitant de site internet qui utilise ces outils est donc assujetti à la législation de l'UE en matière de protection des données dans la mesure où l'utilisateur, au moment de sa visite du site internet, se trouve au sein de l'UE et que les outils de suivi et de profilage utilisés conduisent à un traitement de ses données personnelles. Si le suivi et le profilage se font de façon anonymisée ou pseudonymisée, cela ne constitue pas un traitement des données personnelles et cela n'entraîne donc pas en soi d'applicabilité de la législation de l'UE en matière de protection des données.

Le suivi et le profilage anonymisés n'entrent pas dans le champ d'application du RGPD

3.2.1.2 Comportement au sein de l'UE

La deuxième condition d'applicabilité de la législation de l'UE en matière de protection des données est que les personnes concernées doivent se trouver physiquement au sein de l'UE au moment de l'observation de leur utilisation d'internet. Cela peut être déterminé à l'aide de l'adresse IP du terminal de la personne concernée.

La personne doit se trouver au sein de l'UE au moment de l'observation

3.2.2 Signification pour les communautés de référence et communautés

Si une personne qui se trouve au sein de l'UE au moment où elle consulte le site internet d'une communauté de référence ou d'une communauté et que cette communauté de référence ou cette communauté utilise des outils de suivi et de profilage qui ne sont pas anonymisés, cela est considéré

Signification pour les sites internet des communautés (de référence)

comme une observation du comportement qui relève de la législation de l'UE en matière de protection des données. Comme déjà expliqué plus haut (cf. 3.2.1.1), dans la deuxième situation, le fait que le site internet s'adresse ou non à des personnes au sein de l'UE ne joue aucun rôle. Tout site internet qui utilise des outils de suivi et de profilage non anonymisés et qui est visité par des personnes qui se trouvent au sein de l'UE entre dans le champ d'application de la législation de l'UE en matière de protection des données.

Points à examiner en ce qui concerne les sites internet

Toutes les communautés de référence ou communautés devraient donc vérifier les points suivants concernant la conception de leur site internet :

- est-il possible de renoncer à l'utilisation des instruments de suivi et de profilage, p. ex. sur le bouton « J'aime » de Facebook ?
- le suivi et le profilage peuvent-ils être réalisés de façon anonymisée, p. ex. en recourant à Google Analytics ?
- les personnes avec une adresse IP dans l'espace européen peuvent-elles être exclues du suivi et du profilage au moyen d'outils de géolocalisation ? – cet examen n'est nécessaire que s'il n'est pas possible de renoncer au suivi ou que celui-ci ne peut pas être réalisé de manière anonymisée.

Conception recommandée des sites internet

Si la réalisation des démarches susmentionnées (prises isolément ou combinées) s'avère difficile ou que celles-ci ne sont pas compatibles avec les objectifs poursuivis, il faudra conclure à l'applicabilité de la législation de l'UE en matière de protection des données en ce qui concerne les visiteurs qui se trouvent au sein de l'UE au moment de l'utilisation du site internet. Pour des raisons de sécurité et de coûts, il est recommandé aux communautés de référence et aux communautés de concevoir leurs sites internet de manière à ce que ceux-ci n'entrent pas dans le champ d'application de la législation de l'UE en matière de protection des données.

4 Conclusion et résumé

C'est en fin de compte le cas d'espèce qui est déterminant

La législation de l'UE en matière de protection des données peut dans certaines conditions être applicable aux communautés de référence et aux communautés. Les communautés de référence et communautés peuvent toutefois se soustraire à cette applicabilité en prenant les mesures appropriées. C'est toujours le cas d'espèce concret qui est déterminant. Si une communauté de référence ou une communauté a l'intention d'offrir des services complémentaires par le biais de son infrastructure, il faut qu'elle examine de manière distincte si ces services complémentaires sont susceptibles de conduire à l'applicabilité de la législation de l'UE en matière de protection des données.