HAVE

# Jahrbuch SGHVR 2018
# Annales SDRCA 2018

Stephan Fuhrer (Hrsg.)

SGHVR
SDRCA
Schweizerische Gesellschaft für Haftpflicht und Versicherungsrecht
Société suisse du droit de la responsabilité civile et des assurances

Schulthess §

Schweizerische Gesellschaft für Haftpflicht- und Versicherungsrecht
Société suisse du droit de la responsabilité civile et des assurances

# Jahrbuch SGHVR 2018
# Annales SDRCA 2018

Stephan Fuhrer (Hrsg.)

Mit Beiträgen von

Yasmine Arasteh, Christine Chappuis, Thomas Gächter, Helmut Heiss, Gregor Huber, Sylvain Métille, Cyril Steffen, Rolf H. Weber, Oliver William und Clemens von Zedtwitz
*(Wissenschaftlicher Teil)*

Peter Beck, Guy Chappuis, Ghislaine Frésard, Stephan Fuhrer, Ulrike Mönnich, Bruno Schatzmann, Dominik Skrobala, Rolf Staub und Herbert Zech
*(Jahresbericht)*

Schulthess § 2018

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.


ISBN 978-3-7255-7860-3

www.schulthess.com

# Inhalt

*Zweiter Teil:*
*Jahresbericht 2017/2018*

Sylvain Métille* / Yasmine Arasteh**

# Le Règlement général sur la protection des données et les assureurs privés suisses

## Table des matières




* Docteur en droit, avocat au barreau, professeur associé à l'Université de Lausanne (UNIL).

** Avocate au barreau.

# I. Introduction

Le Règlement général sur la protection des données (RGPD)[1] est applicable depuis le 25 mai 2018. S'il concerne principalement les données personnelles traitées par des entités présentes dans l'Union Européenne (UE) et cela que les personnes concernées soient ou non dans l'UE, il a aussi des effets extraterritoriaux et peut s'appliquer à certaines entreprises en Suisse également, y compris un assureur privé suisse. A l'heure où la révision de la Loi suisse sur la protection des données (LPD) s'enlise[2], même les entreprises qui ne sont pas dans le champ d'application du RGPD ont tendance à s'en inspirer à titre de bonnes pratiques[3]. Nous allons donc voir d'abord à qui s'applique ce règlement, puis les nouvelles obligations qu'il impose au responsable de traitement (et corollairement les droits qu'il donne aux personnes concernées).

1 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 personnelles et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données, RGPD).

2 Le Conseil fédéral a approuvé le projet de révision totale de la LPD le 15 septembre 2017 (FF 2017 6565), mais la CIP-N a décidé en janvier de scinder en deux parties la révision de la loi et de ne traiter dans un premier temps que des adaptations nécessaires en lien avec le développement de l'acquis de Schengen. Le Conseil National a adopté le 12 juin 2018 la Loi fédérale sur la protection des données personnelles dans le cadre de la mise en œuvre de l'acquis de Schengen dans le domaine pénal (Loi sur la protection des données Schengen, LPDS) et la révision de fond de la LPD devrait être traitée en hiver 2018 ou printemps 2019.

3 PHILIPPE GILLIÉRON, Basic steps towards a privacy management program for Swiss SMEs, Bulletin CEDIDAC n°73.

# II. Champ d'application

## A. Matériel

Le RGPD s'applique à tout traitement de données personnelles, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données personnelles qui sont contenues ou pourraient être contenues dans un fichier[4].

Par données à caractère personnel ou données personnelles pour reprendre la terminologie du droit suisse, il faut entendre toute information se rapportant à une personne physique identifiée ou identifiable (« personnes concernée »). Contrairement au droit suisse actuellement en vigueur, les données de personnes morales ne sont pas des données personnelles au sens du RGPD. La notion de personne identifiable est large et inclut toute personne pouvant être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale[5].

Certaines activités sont toutefois exclues du champ d'application matériel du RGPD, notamment le traitement de données aux fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre des menaces pour la sécurité publique et la prévention de telles menaces[6].

Le responsable du traitement, soit celui qui détermine les finalités et les moyens du traitement, peut être un individu, une personne morale de droit privé ou une institution de droit public[7], ce qui inclut évidemment les assureurs[8].

4 Art. 2 (1) RGPD.

5 Art. 4 (1) RGPD. L'adresse IP dynamique d'un visiteur, enregistrée lors de la consultation d'un site web accessible au public, est une donnée personnelle pour le site web, même s'il ne peut pas identifier directement le visiteur mais qu'il a des moyens légaux de le faire identifier grâce à des informations supplémentaires dont dispose par exemple le fournisseur d'accès à Internet de cette personne (CJUE Patrick Breyer c. Bundesrepublik Deutschland [C-582/14]).

6 Art. 2 (2) RGPD.

7 Art. 4 (7) RGPD. Lorsque les finalités et les moyens de ce traitement ne sont pas librement déterminées par le responsable du traitement mais qu'elles lui sont imposées par le droit de l'UE ou le droit d'un État membre, le responsable du traitement est alors désigné par ce droit (ou les critères spécifiques applicables à sa désignation qu'il contient).

8 Lorsque cela n'est pas précisé, le terme « assureur » dans cet article vise les entreprises proposant des assurances privées, par opposition à l'assurance sociale (à laquelle des règles supplémentaires ou différentes peuvent parfois s'appliquer en raison de son statut de droit public).

## B. Assureurs suisses avec une présence dans l'UE

Le RGPD s'applique d'abord aux organisations établies dans l'UE et qui traitent des données personnelles dans le cadre des activités de leur établissement, indépendamment du fait que le traitement des données ait effectivement lieu ou non dans l'UE, de la nationalité ou de la résidence des personnes concernées[9]. Conformément à la jurisprudence rendue sous l'égide de la Directive 95/46/CE et du Traité sur le fonctionnement de l'UE[10], il faut retenir une conception souple de la notion d'établissement, qui écarte toute approche formaliste selon laquelle une entreprise ne serait établie que dans le lieu où elle est enregistrée[11].

Un établissement requiert un dispositif stable, mais sa forme juridique n'est pas déterminante[12]. Il peut par exemple s'agir d'une succursale ou d'une filiale ayant la personnalité juridique. Un rattachement purement technique, comme des serveurs ou des boîtes aux lettres ne suffit pas[13]. Il faut au contraire que soient disponibles en permanence des moyens humains et techniques nécessaires à la fourniture de services particuliers[14]. Un bureau de vente ou un seul courtier peut remplir cette condition[15]. L'établissement suppose encore l'exercice effectif et réel d'une activité, même minime[16].

L'établissement doit finalement traiter des données personnelles dans le cadre de ses activités, ce qui n'implique pas pour autant qu'il traite lui-même les données[17]. La CJUE a d'ailleurs déjà retenu que la présence en Espagne de Google Spain, filiale chargée de vendre des espaces publicitaires au profit de la société

9 Art. 3 (1) RGPD; considérant 22 RGPD ; NICOLAS PASSADELIS/SIMON ROTH, Weisser Rauch über Brüssel, Jusletter du 4 avril 2016, 5.

10 PHILIPP MITTELBERGER, Der Extraterritoriale Ansatz der Datenschutzgrundverordnung (DSGVO), Berne 2018, 21 ; PASSADELIS/ROTH (n. 9), 5.

11 CJUE Weltimmo c. NAIH (C-230/14) point 29 et Verein für Konsumenteninformation c. Amazon (C-191/15) point 77.

12 Considérant 22 RGPD; MITTELBERGER (n. 10), 8.

13 MANUEL KLAR, in: Kühling/Buchner (édit.), Kommentar zur DS-GVO, München 2017, art. 3 N 46.

14 BRENDAN VAN ALSENOY, in: Vermeulen/Lievens (édit.), Reconciling the (extra)territorial reach of the GPDR with public international law, Antwerp 2017, 80.

15 S'il agit avec un degré de stabilité suffisant et à l'aide de moyens nécessaires à la fourniture des services concrets concernés (CJUE Weltimmo c. NAIH [C-230/14] point 30).

16 Considérant 22 RGPD, CJUE Weltimmo c. NAIH (C-230/14), points 28 et 29 ; MITTELBERGER (n. 10), 8.

17 CJUE Google Spain SL, Google Inc. c. AEPD, Mario Costeja González (C-131/12) point 52 ; MITTELBERGER (n. 10), 29.

américaine Google Inc. suffisait à exiger que Google Inc. qui effectue la majeure partie des traitements de données personnelles soit soumise à la législation européenne en matière de protection des données[18].

## C. Assureurs suisses qui visent les résidents de l'UE

### 1. Lieu du marché

Afin d'éviter qu'un responsable de traitement ne se délocalise hors de l'UE pour se soustraire à ses obligations, le RGPD prévoit un champ d'application extraterritorial lié au principe du lieu du marché (*« Marktort-Prinzip »*)[19]. L'article 3 (2) RGPD vise le traitement de données relatif à des personnes qui se trouvent sur le territoire de l'UE[20]. Le critère de localisation du traitement est ainsi mis en arrière-plan, pour retenir celui de la localisation du public cible[21].

Deux cas sont visés. Le premier est celui du traitement de données de personnes qui se trouvent dans l'UE par une organisation qui n'est pas établie dans l'UE mais dont les activités de traitement sont liées à l'offre de biens ou de services à des personnes dans l'UE, qu'un paiement soit exigé ou non[22]. Le second est plus limité et vise l'organisation hors UE qui effectue un suivi du comportement de résidents de l'UE[23].

18 Le traitement de données personnelles qui est fait pour les besoins du service d'un moteur de recherche tel que Google Search, lequel est exploité par une entreprise ayant son siège dans un État tiers mais disposant d'un établissement dans un État membre, est effectué « dans le cadre des activités » de cet établissement si celui-ci est destiné à assurer, dans cet État membre, la promotion et la vente des espaces publicitaires proposés par ce moteur de recherche, qui servent à rentabiliser le service offert par ce moteur (CJUE Google Spain SL, Google Inc. c. AEPD, Mario Costeja González [C-131/12] point 55 ; MITTELBERGER [n. 10], 11). Le Tribunal fédéral avait tenu un raisonnement similaire dans son arrêt concernant Google Street View en retenant la légitimation passive non seulement de Google Inc. mais également de Google Suisse Sàrl (arrêt du TF 1C_230/2011 du 31 mai 2012 consid. 4).

19 LUKAS BÜHLMANN/MICHAEL REINLE, «Extraterritoriale Wirkung der DSGVO», Digma 2017.1, 2 ; PASSADELIS/ROTH (n. 9), 5; KLAR (n. 13), art. 3 RGPD N 9 ; MITTELBERGER (n. 10), 22.

20 Ce qui inclut des travailleurs présents de manière temporaire, des étudiants en échange et des voyageurs dans l'UE, au moins au moment des premiers traitements de données (KLAR [n. 13], art. 3 RGPD N 63 et 64 ; VAN ALSENOY [n. 14], 85). La nationalité, le domicile ou le lieu du lieu des centres d'intérêts vitaux n'est pas importante ici.

21 SÉBASTIEN FANTI, Le nouveau règlement génera sur la protection des données et la Suisse, ExpertFocus 2017/11, 858 s.

22 Art. 3 (2) let. a RGPD.

23 Art. 3 (2) let. b RGPD.

### 2. En offrant des biens et services

Il ne suffit pas d'avoir des biens ou des services, ni même des clients dans l'UE, encore faut-il que l'assureur envisage d'offrir des biens ou des services à des personnes concernées dans l'UE[24]. Le fait qu'un site web soit accessible depuis l'UE n'est pas suffisant[25]. Ce qui est décisif, ce sont les circonstances concrètes et non la manière dont l'entité déclare envisager d'offrir des biens et des services dans l'UE[26]. La fréquence de l'offre de biens ou de services n'est pas déterminante non plus pour l'application de l'article 3 (2) RGPD[27]. Il faut donc vérifier dans chaque cas s'il est envisagé d'offrir des biens ou des services à des personnes concernées dans l'UE, en retenant des indices comme l'utilisation d'une langue ou d'une monnaie d'usage courant dans des États de l'UE, l'utilisation d'un nom de domaine autre que celui du pays dans lequel se trouve la société (« .fr » ou « .eu »), le recours à des publicités ou des offres spécifiques pour les pays de l'UE, la possibilité de commander et d'être livré directement dans l'UE, etc.[28].

L'assureur qui fournit en Suisse des services destinés à des clients dans l'UE, par exemple des assurances spécifiques pour les résidents européens, sera soumis au RGPD en vertu de l'article 3 (2) RGPD, mais en principe pas celui qui vise la clientèle suisse (dans le cadre de la LAMal[29] par exemple) mais accepte aussi des résidents de l'UE ou hors UE[30].

### 3. En suivant le comportement

Il y a un suivi du comportement lorsque des personnes physiques sont suivies sur Internet, ce qui comprend l'utilisation ultérieure éventuelle de techniques de traitement des données qui consistent en un profilage, afin notamment de prendre

24 Considérant 23 RGPD.

25 BÜHLMANN/REINLE (n. 19), 2 ; PASSADELIS/ROTH (n. 9), 6 ; considérant 23 RGPD.

26 KLAR (n. 13), art. 3 RGPD N 81 ; MITTELBERGER (n. 10), 23.

27 KLAR (n. 13), art. 3 RGPD N 70. L'article 27 (2) let. a RGPD qui prévoit cependant que le responsable du traitement ou le sous-traitant hors de l'UE n'a pas l'obligation de désigner un représentant au sein de l'UE si le traitement est occasionnel.

28 Considérant 23 RGPD, CJUE Weltimmo c. NAIH (C-230/14), confirmé par CJUE Hotel Alpenhof c. Heller (C-585/08); MITTELBERGER (n. 10), 23 ; BÜHLMANN/ REINLE (n. 19), 2.

29 Loi fédérale sur l'assurance-maladie du 18 mars 1994 (LAMal).

30 De la même manière un assureur privé suisse qui accepte parmi ses clients un client européen ne sera pas soumis au RGPD, mais il le serait s'il propose une offre d'assurance sur-mesure à destination de clients européens.

des décisions la concernant ou d'analyser ou de prédire ses préférences, ses comportements et ses dispositions d'esprit[31], soit toutes les formes de suivi et de profilage sur Internet, notamment à des fins de publicité comportementale. Les autres types d'opérations de suivi du comportement en dehors d'Internet, comme par exemple l'utilisation d'images satellites ne tombent pas sous le coup du RGPD[32]. En revanche, le suivi du comportement par le biais d'objets connectés pourrait tomber sous le coup du RGPD étant donné qu'ils sont reliés à Internet. Cela paraît peu probable pour l'activité traditionnelle des assureurs, mais n'est pas exclu dans le cas de recours à des applications mobiles collectant des données personnelles.

## III. Assureurs qui ne sont pas concernés

Un assureur suisse qui n'a pas d'établissement dans l'UE, et qui ne vise pas de résidents de l'UE en fournissant des biens ou des services, et qui ne fait pas de suivi du comportement en ligne de résidents de l'UE, n'est pas soumise au RGPD[33], même si elle:

- traite en Suisse des données de nationaux de l'UE résidents en Suisse[34] ;
- traite en Suisse des données d'employés frontaliers travaillant en Suisse et habitant dans l'UE[35] ;
- traite en Suisse des données de résidents européens en lien avec des biens et des services qu'elle n'a pas envisagé de proposer spécifiquement à des résidents européens[36] ;
- traite en Suisse en tant que sous-traitant des données pour un responsable de traitement établi dans l'UE[37] ; ou

31 Considérant 24 RGPD.

32 KLAR (n. 13), art. 3 RGPD N 92. Avis contraire : MITTELBERGER (n. 10), 25.

33 Art. 3 RGPD *a contrario*.

34 KLAR (n. 13), art. 3 RGPD N 64.

35 Qu'ils soient Suisses ou Européens.

36 DAVID VASELLA, «EDÖB zur DSVO und ihren Auswirkungen auf die Schweiz», daten:recht, 23 décembre 2017, 9.

37 Le contrat de sous-traitance va inclure des obligations reprises du RGPD, notamment celles figurant à son art. 28. Il s'agit d'engagements contractuels pour le sous-traitant, et non d'une application directe du RGPD. La protection de la personnalité des personnes concernées est néanmoins garantie, puisque le

- recourt à un sous-traitant établi dans l'UE[38].

Bien qu'elles n'y soient pas contraintes, un grand nombre d'entreprises suisses se mettent actuellement en conformité avec le RGPD, qu'elles appliquent des directives d'une société mère qui y est soumise ou spontanément à titre de bonnes pratiques[39].

S'il s'agit à n'en pas douter d'un standard dont il vaut la peine de s'inspirer, y compris dans l'optique de la révision en cours de la LPD, il est essentiel de ne pas prendre d'engagements inconsidérés. Il ne faut en particulier pas donner de garanties de conformité que l'entreprise n'est pas sûre de pouvoir assumer. En annonçant publiquement, par exemple sur un site web, respecter le RGPD, l'entreprise accepte alors contractuellement des obligations qu'elle n'a pas et dont la violation peut lui être reprochée tant par une autorité de contrôle que par un particulier[40]. Affirmer sa conformité au RGPD et en respecter toutes les formalités serait aussi pour une autorité de contrôle européenne un indice fort que l'entreprise se considère comme soumise au RGPD.

Mieux vaut donc pour les assureurs non soumis au RGPD de s'efforcer de respecter la LPD et les principes du RGPD (mais pas la nomination d'un représentant dans l'UE et les notifications aux autorités de contrôle européennes, etc.), et ne pas affirmer être en conformité avec le RGPD.

# IV. Conséquences

## A. En général

Les assureurs soumis au RGPD doivent prendre toutes les mesures nécessaires pour assurer leur conformité au RGPD. Ils sont soumis aux mêmes obligations

responsable du traitement est soumis au RGPD et que le sous-traitant ne peut effectuer que les traitements que le responsable du traitement est en droit d'effectuer et lui demande d'effectuer.

38 DAVID VASELLA, «Zum Anwendungsbereich der DSGVO», Digma 2017.4, 2, 4 ; KLAR (n. 13), art. 3 RGPD N 38 ; Guide du sous-traitant de septembre 2017 de la CNIL ; PFPDT, Le RGPD et ses conséquences sur la Suisse, mai 2018, 7. Le sous-traitant établi dans l'UE sera en revanche directement soumis au RGPD.

39 En particulier en l'absence de codes de conduite ou recommandations spécifiques à leur domaine d'activité. C'est parfois aussi une sorte de mise en conformité anticipée à ce à quoi le droit suisse pourrait peut-être ressembler dans plusieurs années.

40 La société américaine Google avait par exemple été sanctionnée par la Federal Trade Commission lors du déploiement de Google Buzz aux USA en raison de garanties données quant au traitement de données en application du EU.-U.S. Safe Harbor, plutôt qu'en raison d'une violation d'exigences contenues directement dans le droit américain (FTC, in the matter of Google Inc., File No. 1023136, Docket No. C-4336).

que les responsables de traitement présents dans l'Union, mais doivent en plus nommer un représentant[41].

Nous aborderons en premier lieu les principes qui doivent être respectés lors de tout traitement, puis les obligations formelles que doivent remplir les assureurs soumis au RGPD, avant de terminer par les droits des personnes et les pouvoirs de l'autorité de contrôle.

## B. Principes

### 1. Grands principes

Comme en droit suisse, les responsables de traitement devront s'assurer que les données personnelles ne sont collectées et traitées que de manière licite et loyale (principe de bonne foi). Le traitement doit être transparent[42] et limité au but indiqué[43] comme l'exige le principe de finalité.

Les données doivent en outre être correctes et à jour (principe d'exactitude), et traitées de manière adéquate, pertinente et limitée à ce qui est nécessaire (principe de proportionnalité ou de minimisation des données)[44].

### 2. Justification du traitement

Contrairement à la LPD[45], le RGPD exige que tout traitement repose sur l'un des fondements énumérés à l'article 6 RGPD[46] : consentement de la personne concernée[47], nécessité contractuelle[48], conformité à l'égard d'une obligation légale d'un État membre ou de l'UE[49], ou intérêts légitimes du responsable de traitement[50]. Le fondement choisi doit être communiqué pour chaque traitement[51].

41 Voir IV.C.1. ci-dessous.
42 Art. 5 (1) let. a RGPD.
43 Art. 5 (1) let. b RGPD.
44 Art. 5 (1) let. c RGPD.
45 Si dans le RGPD le consentement est un des fondements possibles du traitement, le consentement en droit suisse est une des justifications que peut invoquer le responsable du traitement lorsqu'il porte une atteinte à la personnalité de la personne concernée, notamment parce que les principes sont violés (Art. 13 LPD ; PHILIPPE MEIER, Protection des données, Berne 2011, 317).
46 En relation avec le considérant 40 RGPD.
47 Art. 6 (1) let. a RGPD.
48 Art. 6 (1) let. b RGPD.
49 Art. 6 (1) let. c RGPD.
50 Art. 6 (1) let. f RGPD.

Constitue un consentement toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle une personne concernée accepte, par une déclaration écrite ou un acte positif clair, que des données personnelles la concernant fassent l'objet d'un traitement[52]. Le consentement, pour être valable, doit consister en une déclaration ou un acte positif univoque, ce qui semble exclure un consentement tacite ou purement passif[53], par exemple en cas de cases cochées par défaut ou d'inactivité[54].

Le consentement ne sera pas réputé être donné librement si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au traitement de données personnelles qui ne sont pas nécessaires à l'exécution dudit contrat ou si la personne concernée ne dispose pas d'une véritable liberté de choix ou n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice, en particulier lorsqu'il existe un déséquilibre manifeste entre la personne concernée et le responsable du traitement[55]. L'assureur a le fardeau de la preuve du consentement de la personne concernée au traitement de données personnelles la concernant[56].

Le Groupe de Travail « Art. 29 » considère que si le consentement est demandé, le responsable de traitement doit renoncer à invoquer une autre justification du traitement[57]. Une telle exigence ne nous semble pas découler du RGPD.

L'assureur pourra évidemment justifier le traitement de certaines données par une obligation légale ou l'exécution du contrat d'assurance. Dans certains cas les intérêts de l'assureur pourraient également être considérés comme légitimes. Le considérant 47 RGPD précise qu'un tel intérêt légitime pourrait par exemple, exister lorsqu'il existe une relation pertinente et appropriée entre la personne concernée et le responsable du traitement dans les situations telles que celles où la personne concernée est un client du responsable du traitement ou est à son service. En tout état de cause, l'existence d'un intérêt légitime devrait faire

51 Art. 13 (1) let. c RGPD.

52 Art. 4 (11) RGPD. L'article 7 RGPD précise les conditions particulières s'appliquant au consentement de la personne concernée. Voir également Les « Guidelines on Consent under Regulation 2016/679 (wp259rev. 01) » du Groupe de Travail « Art. 29 » du 16 avril 2018.

53 ALAIN BENSOUSSAN/JEAN-FRANÇOIS HENROTTE/MARC GALLARDO/SÉBASTIEN FANTI, General Data Protection Regulation: Texts, Commentaries and Practical Guidelines, Mechelen 2018, 92.

54 Considérant 32 RGPD.

55 Art. 7 (4) RGPD et considérant 42 *in fine* et 43 RGPD.

56 Art. 7 (1) RGPD ; BENSOUSSAN et al. (n. 53), 92.

57 Les « Guidelines on Consent under Regulation 2016/679 (wp259rev.01) » du Groupe de Travail « Art. 29 » du 16 avril 2018, 23.

l'objet d'une évaluation attentive, notamment afin de déterminer si une personne concernée peut raisonnablement s'attendre, au moment et dans le cadre de la collecte des données personnelles, à ce que celles-ci fassent l'objet d'un traitement à une fin donnée[58].

### 3. Protection des données dès la conception (Privacy by Design) et protection des données par défaut (Privacy by Default)

Le RGPD a également introduit, du moins de manière formelle, les principes de protection des données dès la conception et de protection des données par défaut.

Les responsables de traitement doivent mettre en œuvre des mesures techniques et organisationnelles dès les premières étapes de la conception des opérations de traitement, de manière à préserver dès le départ la vie privée et les principes en matière de protection des données (*Privacy by Design*)[59]. Ces mesures pourraient consister, entre autres, à réduire à un minimum le traitement des données personnelles (principe de minimisation des données[60]), à pseudonymiser[61] les données personnelles dès que possible, à garantir la transparence en ce qui concerne les fonctions et le traitement des données personnelles, à permettre à la personne concernée de contrôler le traitement des données et à permettre au responsable du traitement de mettre en place des dispositifs de sécurité ou de les améliorer[62].

Conformément au principe de protection des données par défaut, les assureurs sont tenus d'adopter des mesures techniques et organisationnelles consistant à limiter par défaut le traitement de données personnelles à ce qui est strictement nécessaire, en ce qui concerne la quantité de données traitées, leur accessibilité et

58 Voir également Groupe de Travail « Art. 29 », avis (WP 217) adopté le 9 avril 2014 sous l'empire de l'ancienne directive mais toujours valable.

59 Art. 25 (1) RGPD.

60 Art. 5 (1) let. c RGPD.

61 L'article 4 (5) RGPD définit la pseudonymisation comme étant « le traitement de données personnelles de telle façon qu'elles ne puissent plus être attribuées à une personne concernée sans avoir recours à des informations supplémentaires, pour autant que celles-ci soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir cette non-attribution à une personne identifiée ou identifiable ».

62 Considérant 78 RGPD. L'avis 5/2018 du 31 mai 2018 du Contrôleur européen à la protection des données (CEPD) fournit quelques exemples de méthodologies destinées à développer la protection des données dès la conception. Voir également ANN CAVOUKIAN, Privacy by Design: Take the Challenge, 2009 ; ISMAËL TALL, « Le renforcement de la loi fédérale sur la protection des données : le cas de la protection de la vie privée dès la conception (privacy by design) », Cahier de l'IDHEAP, no 289.

leur période de conservation[63]. Il faudrait donc une action positive de l'assureur pour modifier ces paramètres.

#### 4. Durée de conservation

Conformément au principe de proportionnalité, le RGPD exige que les données personnelles ne soient conservées que pendant une durée n'excédant pas celle nécessaire au regard des finalités du traitement correspondant[64]. En d'autres termes, les assureurs doivent supprimer les données permettant l'identification des personnes concernées dès l'instant où elles ne sont plus nécessaires au traitement, sauf exception pour les finalités d'archivage dans l'intérêt public et de recherches scientifiques, statistiques ou historiques, pour autant que les droits des personnes concernées soient protégés par des mesures techniques et organisationnelles[65].

Le responsable du traitement est responsable du respect de ce principe, mais la nouveauté est qu'il doit maintenant être en mesure de documenter cette durée[66] et de la communiquer (ou au moins les critères pour la déterminer)[67] à la personne concernée.

À cette obligation de conserver les données aussi peu longtemps que possible peuvent s'opposer des obligations légales de conserver ces données pendant un certain temps. Ces obligations légales priment évidemment.

### C. Formalités

#### 1. Registre des activités de traitement

En plus des principes liés au traitement de données, l'assureur soumis au RGPD doit respecter un certain nombre de formalités. Elles remplacent les autorisations qu'il était nécessaire d'obtenir préalablement au traitement dans certains pays.

63 Art. 25 (2) RGPD.
64 Art. 5 (1) let. e RGPD.
65 Art. 89 (1) et considérant 50 RGPD.
66 Art. 5 (2) RGPD en relation avec l'article 24 RGPD. Elle doit en ouvre être mentionnée dans le registre des fichiers (art. 30 RGPD).
67 Art. 13 (2) let. a RGPD.

L'assureur doit en particulier tenir un registre[68]. Cela doit lui permettre de démontrer sa conformité, mais également d'avoir une vue d'ensemble des données qu'il traite. Le registre doit contenir en particulier les finalités du traitement[69], une description des catégories de personnes concernées et des catégories de données personnelles[70], le cas échéant, les transferts de données personnelles vers un pays tiers ou à une organisation internationale[71]. Dans la mesure du possible doivent figurer également dans ce registre les délais prévus pour l'effacement des différentes catégories de données[72], ainsi qu'une description générale des mesures de sécurité techniques et organisationnelles[73].

Le registre doit revêtir la forme écrite y compris la forme électronique[74] et être tenu à la disposition de l'autorité de contrôle sur demande[75]. Des modèles de registre d'activité de traitement ont été élaborés par diverses autorités nationales de protection des données (dont la Commission nationale française de l'informatique et des libertés (CNIL), l'Information Commissioner's Office anglaise (ICO), la Commission belge de la protection de la vie privée (CPVP))[76].

L'obligation de tenir un registre ne s'applique pas aux assureurs qui comptent moins de 250 employés, et si le traitement qu'ils effectuent n'est pas susceptible de comporter un risque pour les droits et des libertés des personnes concernées, s'il est occasionnel, ou encore s'il ne porte pas sur des données sensibles[77] ou sur des données personnelles relatives à des condamnations pénales[78]. Cela paraît donc assez peu probable.

68 Qu'il intervienne en qualité de sous-traitant ou de responsable de traitement (considérant 82 RGPD).
69 Art. 30 (1) let. b RGPD.
70 Art. 30 (1) let. c RGPD.
71 Art. 30 (1) let. e RGPD.
72 Art. 30 (1) let. f RGPD.
73 Art. 30 (1) let. g RGPD.
74 Art. 30(3) RGPD.
75 Art. 30 (4) RGPD.
76 <www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement>; <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/documentation/how-do-we-document-our-processing-activities/> , <www.privacycommission.be/fr/canevas-de-registre-des-activites-de-traitement>, consulté le 05.07.2018.
77 Au sens de l'article 9 (1), notamment liées à la santé.
78 BENSOUSSAN et al. (n. 53), 183; La prise de position de Groupe du Travail « Art. 29 » précise les exceptions de l'article 30 (5) RGPD (<http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=624045>, consulté le 05.07.2018).

### 2. Désignation d'un délégué à la protection des données (DPD)

L'assureur qui réalise un suivi régulier et systématique des personnes à grande échelle[79] ou qui traite des données sensibles (notamment liées à la santé) devra désigner un délégué à la protection des données (DPD ou *Data Protection Officer, DPO)*[80].

Parmi les missions du DPD, il doit en particulier:

- informer et conseiller le responsable de traitement ou le sous-traitant ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent en vertu du RGPD[81] ;
- analyser et vérifier la conformité des activités de traitement y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits qui s'y rapportent[82] ;
- être un point de contact pour les personnes concernées au sujet de toutes les questions relatives au traitement de leurs données personnelles et à l'exercice de leurs droits[83] et ainsi que pour l'autorité de contrôle[84] et coopérer avec cette dernière[85] ;
- collecter des informations pour identifier les activités de traitement ; et
- conseiller le responsable du traitement lorsqu'une analyse d'impact est réalisée[86].

79 Les lignes directrices concernant les délégués à la protection des données (WP 243) du Groupe de Travail « Art. 29 » adoptées le 13 décembre 2016 et révisées dernièrement le 5 avril 2017 (cité: Lignes directrices DPD) précisent les notions d'« activités de base », « suivi régulier et systématique » et de « «grande échelle ». Des exemples de traitement à grande échelle cités comprennent le traitement de données clients par une banque ou par un assureur.

80 La nomination d'un DPD n'est ainsi pas obligatoire dans toutes les entreprises. Cependant, il découle des lignes directrices DPD (n. 79), 7, que lorsqu'un DPD est désigné volontairement, les mêmes obligations que celles prévues pour les DPD devant être désignés obligatoirement seront applicables.

81 Art. 39 (1) let. a RGPD.

82 Art. 39 (1) let. b RGPD.

83 Art. 38 (4) RGPD.

84 Art. 39 (1) let. e RGPD.

85 Art. 39 (1) let. d RGPD; BENSOUSSAN et al. (n. 53), 214.

86 Art. 35 (2) RGPD et Art. 39 (1) let. c RGPD.

Il découle de cette liste que le DPD joue un rôle important dans l'organisation dans laquelle il est amené à œuvrer étant donné que son rôle inclut le fait de conseiller les employés et de leur dispenser des formations adéquates, ce qui suppose une relation directe avec eux[87]. En plus de ces obligations légales, il doit aussi remplir un rôle de chef d'orchestre pour coordonner toutes les démarches liées à la protection des données, qu'elles soient spontanées ou requises par la loi.

S'agissant des qualités que le DPD doit revêtir, celui-ci doit notamment disposer de connaissances spécialisées de la législation et des pratiques en matière de protection des données[88] et effectuer sa mission en toute indépendance[89], sans recevoir d'instruction en ce qui concerne l'exercice de sa mission, ni être relevé de ses fonctions ou pénalisé par l'assureur[90].

Il n'est pas interdit au DPD d'exercer d'autres fonctions[91]. Cependant, les assureurs doivent vérifier que ses autres fonctions ne donnent pas lieu à un conflit d'intérêts[92].

Précisons que le DPD ne sera pas tenu personnellement responsable du manquement de son organisation au RGPD. La responsabilité incombe à l'assureur, notamment si celui-ci entrave ou échoue à soutenir le DPD dans la réalisation des objectifs premiers de celui-ci[93].

87 ROSEMARY JAY, in : Sweet & Maxwell (édit.), Guide to the General Data Protection Regulation, 2017, n°10-020.

88 Art. 37 (5) RGPD et considérant 97 RGPD. Les lignes directrices du G29 indiquent que plus les activités de traitement de données personnelles sont sensibles ou complexes, plus il est attendu du DPD un haut niveau d'expertise (lignes directrices DPD [n. 79], 13). JAY relève qu'en fonction de la taille des entreprises concernées, il risque d'être difficile pour elles de recruter un expert en la matière (JAY [n. 87], n°10-011).

89 Le considérant 97 in fine RGPD précise que le DPD, qu'il soit ou non employé du responsable du traitement, devrait être en mesure d'exercer ses fonctions et ses missions en toute indépendance.

90 Art. 38 (3) RGPD.

91 Art. 38 (6) RGPD.

92 Lignes directrices DPD (n. 79), 28.

93 Lignes directrices DPD (n. 79), 20 et 28 ; Art. 24 (1) RGPD. Le responsable de traitement ou le sous-traitant doivent fournir au DPD des ressources appropriées afin qu'il puisse remplir ses obligations conformément au RGPD. L'article 38 (3) *in fine* RGPD prévoit qu'il doit faire directement rapport au niveau le plus élevé de la direction du responsable du traitement ou du sous-traitant.

L'assureur devra veiller à ce que son DPD soit joignable et mettre à disposition ses coordonnées en les communiquant à l'autorité de contrôle[94]. Le DPD est soumis au secret professionnel ou à une obligation de confidentialité en ce qui concerne l'exercice de ses missions, conformément au droit de l'Union ou au droit des États membres[95].

L'assureur qui ne nomme pas un DPD alors qu'il en remplissait les conditions peut se voir imposer une amende par l'autorité de contrôle compétente[96], et ce, indépendamment de la mise en place d'un autre programme de conformité au RGPD ayant porté ses fruits[97].

### 3. Désignation d'un représentant

Lorsque le RGPD s'applique de manière extraterritoriale, l'assureur[98] doit désigner un représentant[99] dans un des États membres dans lesquels se trouvent les personnes physiques et dont les données personnelles font l'objet d'un traitement lié à l'offre de biens ou de services, ou dont le comportement fait l'objet d'un suivi[100].

Cette obligation ne s'applique pas aux autorités et organismes publics, ni aux responsables de traitement privés qui ne traitent qu'occasionnellement des données personnelles et pour autant qu'il ne s'agisse pas de données sensibles ou représentant un risque important[101].

La désignation du représentant doit se faire par un mandat écrit de l'assureur pour agir en son nom en ce qui concerne les obligations qui lui incombe en vertu du RGPD[102]. L'assureur n'est en revanche pas obligé d'annoncer son représentant aux autorités de contrôle[103].

94 Art. 37 (7) RGPD.
95 Art. 38 (5) RGPD. Sur la question de la problématique de nommer un avocat conseil interne à l'organisation en tant que DPD, voir JAY (n. 87), n°10-017.
96 Art. 83 (4) let. a RGPD.
97 JAY (n. 87), n°10-018.
98 Qu'il soit responsable de traitement ou sous-traitant.
99 Le représentant est défini à l'article 4 (17) RGPD.
100 Art. 27 (1) et (3) RGPD.
101 Art. 27 (2) RGPD ; considérant 80 RGPD.
102 Considérant 80 RGPD.
103 Contrairement à ce qui prévaut pour le délégué à la protection des données.

Les tâches du représentant, sont notamment de tenir un registre des activités de traitement de l'assureur, effectuées sous la responsabilité de ce dernier[104] et de coopérer avec l'autorité de contrôle en lui communiquant sur demande toute information dont elle a besoin pour l'accomplissement de ses missions[105]. Enfin, le représentant pourrait faire l'objet de mesures coercitives en cas de non-respect du RGPD par le responsable du traitement ou le sous-traitant[106].

### 4. Transparence (devoir d'information aux personnes concernées)

Lorsqu'il traite les données personnelles de ses assurés, l'assureur est tenu de leur fournir les informations listées aux articles 13 et 14 RGPD d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples[107]. Ces informations concernent notamment l'identité et les coordonnées du responsable du traitement et de son représentant, l'identité du DPD, les intérêts légitimes poursuivis, les éventuels destinataires ou catégories de destinataires de données personnelles, les éventuels transferts de données à l'étranger, la durée de conservation et les droits de la personne concernée.

Le principe de la transparence exige que toute information et communication relatives au traitement de ces données soient aisément accessibles, faciles à comprendre et formulées en des termes clairs et simples[108]. Il n'est toutefois pas nécessaire de fournir ces informations lorsque l'assuré dispose déjà de ces informations[109], lorsque la loi prévoit expressément l'enregistrement ou la communication de ces données ou lorsque la communication à l'assuré se révèle impossible ou exigerait des efforts disproportionnés[110]. Le nombre de personne

104 Art. 30 (1) RGPD.

105 Art. 58 (1) RGPD ; considérant 82 RGPD ; art. 30 (4) RGPD.

106 Considérant 80 *in fine* RGPD. La question de la responsabilité subsidiaire du représentant est débattue en doctrine, étant donné la formulation ambiguë de l'article 27 (5) RGPD et le fait que ni les articles 57 et 58 RGPD traitant du pouvoir des autorités de contrôle, ni l'article 83 RGPD traitant des amendes administratives ne mentionnent la question de sa responsabilité. JAY relève que cette insécurité juridique est problématique, étant donné que selon l'interprétation retenue, d'autres entités que les sous-traitants ou responsables de traitements pourraient être tenu à des obligations primaires (JAY [n. 87], n°4-039).

107 Art. 12 (1) RGPD. Les informations listées aux articles 13 et 14 RGPD doivent être fournies à la personne concernée au moment où ces données sont collectées (art. 13 [1] RGPD), ou si ces données sont collectées auprès d'une autre source, dans un délai raisonnable en fonction des circonstances propres à chaque cas (considérant 61 RGPD). Voir également les Lignes directrices sur la transparence (WP 260) du Groupe de Travail « Art. 29 », adoptée le 29 novembre 2017 et révisé dernièrement le 11 avril 2018.

108 Considérant 39 RGPD.

109 Art.13 (4) et 14 (5) let. a RGPD.

110 Art. 14 (5) let. b et c RGPD.

concernées, l'ancienneté des données ainsi que les garanties appropriées éventuelles adoptées devrait être pris en considération afin d'évaluer la proportionnalité de ces mesures[111].

### 5. Analyse d'impact relative à la protection des données (AIPD)

Avant toute activité de traitement « susceptible d'engendrer un risqué élevé pour les droits et libertés des personnes physiques[112] », l'assureur doit effectuer une analyse d'impact relative à la protection des données (AIPD)[113]. Le traitement « à grande échelle » de données sensibles, ou les activités de profilage, sont cités, de manière non exhaustive, à titre d'exemples de traitement à risque élevé[114].

L'AIPD doit être effectuée « avant le traitement »[115], conformément aux principes de protection des données dès la conception et de protection des données par défaut[116]. L'AIPD doit au moins contenir une description des activités de traitement et de leur finalité ainsi qu'une évaluation de la nécessité et de la proportionnalité du traitement, des risques en découlant et des mesures adoptées pour atténuer ces risques, notamment les garanties et les mesures de sécurité destinées à protéger les données personnelles et à se conformer au RGPD[117].

Si un DPD a été nommé, son avis sur l'élaboration de l'AIPD doit être sollicité[118]. Toutefois, la responsabilité de veiller à ce qu'une AIPD soit effectuée incombe toujours au responsable de traitement[119].

111 Considérant 62 RGPD).

112 Art. 35 (1) RGPD et considérant 84 RGPD.

113 Parfois également appelé Etude d'impact vie privée (EIVP).

114 L'article 35 (3) RGPD et le considérant 91 prévoient les cas dans lesquels une AIPD peut être requise. Étant donné qu'il s'agit d'une liste non exhaustive, d'autres opérations de traitement peuvent néanmoins présenter un risque élevé et donc être obligatoirement soumis à une AIPD. Voir également les « Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is ‹likely to result in a high risk› for the purposes of Regulation 2016/679 » du Groupe de Travail « Art. 29 » (WP 248rev.01) (cité : Lignes directrices AIPD).

115 Art. 35 (1) et (10) RGPD et considérant 90 et 93 RGPD.

116 Art. 25 RGPD et considérant 78 RGPD ; BENSOUSSAN et al. (n. 53), 202.

117 Art. 35 (7) RGPD.

118 Art. 39 (1) let. c RGPD. À noter que si le traitement est entièrement ou partiellement effectué par un sous-traitant, ce dernier doit aider le responsable du traitement à effectuer l'AIPD et fournir toutes les informations nécessaires, en application de l'article 28 (3) let. f RGPD ; Lignes directrices AIPD (n. 114), 17.

119 Art. 35 (2) RGPD et Lignes directrices AIPD (n. 114), 17.

L'assureur doit consulter l'autorité de contrôle préalablement au traitement lorsqu'une AIPD indique que le traitement présenterait un risque élevé si des mesures pour atténuer le risque ne sont pas prises[120].

Quand bien même une AIPD ne s'avèrerait pas nécessaire, les assureurs doivent évaluer de manière continue les risques créés par leurs activités de traitement dans le but d'identifier quand un type de traitement deviendrait « susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques » et donc rendre une AIPD nécessaire[121].

## D. Transferts à l'étranger

### 1. Pays dits sûrs

Les transferts de données personnelles à destination d'un pays de l'UE ne sont pas soumis à des restrictions particulières, contrairement à ce qui prévaut pour les transferts vers des pays tiers[122].

Il en va de même pour les transferts de données personnelles vers un pays tiers ayant fait l'objet d'une décision d'adéquation de la Commission européenne[123]. La liste des pays tiers faisant l'objet d'une décision d'adéquation, et dont la Suisse fait partie, est publiée au Journal officiel de l'Union européenne et sur le site web de la Commission européenne[124].

Les transferts de données personnelles vers les entreprises américaines ayant adhéré aux standards prévus par le *EU-U.S. Privacy Shield* sont assimilés aux transferts vers un pays adéquat[125].

120 Art. 36 (1) RGPD et considérant 94 RGPD.

121 Lignes directrices AIPD (n. 114), 7.

122 Art. 44 à 50 RGPD. Ces restrictions s'appliquent tant aux responsables de traitement qu'aux sous-traitants (JAY [n. 87], n° 8-022).

123 Considérant 103 RGPD.

124 Art. 45 (8) RGPD ; La liste existante de pays ayant précédemment été approuvés par la Commission comme offrant un niveau de protection adéquat restera applicable, à savoir: Andorre, l'Argentine, le Canada, la Suisse, les îles Féroé, Guernesey, Israël, l'île de Man, Jersey, la République orientale de l'Uruguay, et la Nouvelle-Zélande (<https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en>, consulté le 05.07.2018 ; journal officiel UE). En l'absence de décision contraire, les décisions d'adéquation de la Commission prises sous le couvert de la Directive 95/46/CE restent valables jusqu'à leur modification, leur remplacement ou leur abrogation par une décision de la Commission européenne (art. 45 [9] RGPD).

125 La Commission européenne a formellement adopté une décision d'adéquation visant à reconnaître au mécanisme du EU-U.S. Privacy Shield un niveau de protection équivalent aux exigences européennes.

### 2. Transferts moyennant des garanties particulières

En l'absence de décision d'adéquation, les données personnelles peuvent néanmoins être transférées si des garanties appropriées sont offertes par le responsable de traitement ou le sous-traitant (importateur) pour pallier l'insuffisance du niveau de protection des données personnelles dans le pays de destination[126].

Ces garanties peuvent revêtir plusieurs formes, notamment[127] :

- des règles d'entreprise contraignantes[128] ;
- des clauses-types de protection des données adoptées par la Commission européenne[129] ;
- des clauses-types de protection des données adoptées par une autorité de contrôle[130] ;
- des clauses contractuelles autorisées par une autorité de contrôle[131] ;
- un code de conduite[132] ; ou
- un mécanisme de certification approuvé[133].

Ces garanties devraient assurer le respect des exigences en matière de protection des données et des droits des personnes concernées d'une manière appropriée au traitement au sein de l'Union, y compris l'existence de droits opposables de la personne concernée et de voies de droit effectives, ce qui comprend le droit d'engager un recours administratif ou juridictionnel effectif et d'introduire une action en réparation, dans l'Union ou dans un pays tiers[134].

126 Art. 46 (1) RGPD.

127 L'article 46 (2) RGPD établit une liste des garanties appropriées.

128 Art. 46 (2) let. b RGPD. Ces règles d'entreprise contraignantes doivent répondre à plusieurs conditions définies par l'article 47 (1) RGPD et être approuvées par l'autorité de contrôle compétente selon le mécanisme de contrôle de la cohérence prévue à l'article 63 RGPD. À cet égard, l'article 64 (1) let. f RGPD prévoit que le Comité européen de la protection des données rend un avis lorsqu'une autorité de contrôle envisage de prendre une décision visant à approuver des règles d'entreprise contraignantes.

129 Art. 46 (2) let. c RGPD en conformité avec la procédure d'examen établie à l'article 93 (2) RGPD. Les clauses-types approuvées sous l'égide de l'ancienne directive demeurent valable jusqu'à leur modification, leur remplacement ou leur abrogation par la Commission, conformément à l'article 46 (5) RGPD.

130 Art. 46 (2) let. d RGPD en conformité avec la procédure d'examen établie à l'article 93 (2) RGPD.

131 Art. 46 (3) let. a et (4) RGPD.

132 Art. 46 (2) let. e RGPD.

133 Art. 46 (2) let. d RGPD.

134 Considérant 108 RGPD et art. 46 (1) *in fine* RGPD.

### 3. Dérogation pour situations particulières

En l'absence d'une décision d'adéquation[135] ou de garanties appropriées[136], un transfert de données personnelles vers un pays tiers ou à une organisation internationale peut aussi avoir lieu si l'une des conditions de l'article 49 (1) RGPD est remplie. Parmi celles-ci, on peut relever le consentement explicite de la personne concernée[137], la nécessité contractuelle[138], les motifs importants d'intérêt public[139] , les actions en justice[140], les intérêts vitaux[141] et les données de registres publics[142].

Lorsqu'un transfert ne peut être fondé sur un des motifs particuliers de l'article 49 (1) RGPD, une dérogation limitée est prévue concernant les transferts non répétitifs impliquant un nombre limité de personnes concernées, lorsque ce transfert est nécessaire aux fins des intérêts légitimes impérieux poursuivis par les responsables du traitement et lorsque ces intérêts prévalent sur les intérêts ou les libertés et droits fondamentaux de la personne concernée et lorsque le responsable du traitement a évalué toutes les circonstances entourant le transfert de données[143]. Le responsable du traitement doit informer l'autorité de contrôle et les personnes concernées dès lors qu'il s'appuie sur cette dérogation.

135 Au sens de l'article 45 RGPD.

136 Au sens de l'article 46 RGPD.

137 Art. 49 (1) let. a RGPD, ce motif n'étant pas applicable aux activités des autorités publiques dans l'exercice de leurs prérogatives de puissance publique conformément à l'article 49 (3) RGPD.

138 Art. 49 (1) let. b RGPD, ce motif n'étant pas applicable aux activités des autorités publiques dans l'exercice de leurs prérogatives de puissance publique conformément à l'article 49 (3) RGPD.

139 Art. 49 (1) let. d RGPD, étant précisé que l'intérêt public doit être reconnu par le droit de l'Union ou le droit de l' État membre auquel le responsable de traitement est soumis, conformément à l'article 49 (4) RGPD. Parmi les exemples d'intérêts publics, le considérant 112 RGPD retient le cas d'échange international de données entre autorités de la concurrence, administrations fiscales ou douanières, entre autorités de surveillance financière, entre services chargés des questions de sécurité sociale ou relatives à la santé publique, par exemple aux fins de la recherche des contacts des personnes atteintes de maladies contagieuses ou en vue de réduire et/ou d'éliminer le dopage dans le sport.

140 Art. 49 (1) let. e RGPD.

141 Art. 49 (1) let. f RGPD.

142 Art. 49 (1) let. g RGPD. Le considérant 111 RGPD précise que dans le cas des registres publics, ce transfert ne devrait pas porter sur la totalité des données personnelles ni sur des catégories entières de données contenues dans le registre et, lorsque celui-ci est destiné à être consulté par des personnes ayant un intérêt légitime, le transfert ne devrait être effectué qu'à la demande de ces personnes ou lorsqu'elles doivent en être les destinataires, compte dûment tenu des intérêts et des droits fondamentaux de la personne concernée.

143 Art. 49 (1), 2e paragraphe RGPD et considérant 113 RGPD.

## E. Délégation de traitement

Il est communément admis qu'un responsable de traitement ne peut pas effectuer personnellement toutes les opérations de traitement et qu'il va recourir à un ou plusieurs sous-traitants[144]. Le sous-traitant devra alors, si l'assureur est soumis au RGPD, respecter un certain nombre d'exigences qui devront figurer dans un contrat écrit. Le sous-traitant doit s'engager à[145] :

- ne traiter les données personnelles que conformément aux dispositions du RGPD et aux instructions écrites du responsable de traitement, le contrat de sous-traitance représentant ces instructions écrites[146] ;
- prendre toutes les mesures techniques et organisationnelles nécessaires à assurer la confidentialité et la sécurité des données personnelles, y compris s'assurer que les personnes autorisées à traiter des données personnelles s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité[147] ;
- ne traiter les données personnelles que pour le compte du responsable de traitement et ne pas les utiliser dans son propre intérêt[148] ;
- ne transférer des données personnelles hors de l'UE qu'avec l'accord écrit du responsable de traitement et en prenant les mesures commandées par le RGPD[149] ;
- ne faire appel à des sous-sous-traitants qu'avec l'accord préalable écrit du responsable de traitement. Même dans ce cas, le sous-traitant demeure seul responsable des actes des sous-sous-traitants[150] ;
- restituer ou supprimer toutes les données personnelles lorsqu'elles ne sont plus nécessaires et dans tous les cas à la fin du contrat de sous-traitance[151] ;

144 L'article 4 (8) RGPD définit le sous-traitant comme étant : « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données personnelles pour le compte du responsable du traitement ».

145 Art. 28 RGPD. Voir également ÉMILIE M. PRAZ, « Responsabilités et outils de conformité selon la RGPD : obligations du responsable de traitement et du sous-traitant », PJA 2018, 609 ss.

146 Art. 28 (3) let. a RGPD.

147 Art. 28 (3) let. b RGPD.

148 Art. 28 (1) RGPD.

149 Art. 46 RGPD.

150 Art. 28 (2) et (4) RGPD.

- informer immédiatement le responsable de traitement de tout incident de sécurité ou violation de données personnelles et lui transmettre toutes les informations utiles en vue d'une éventuelle notification à l'autorité[152] ;
- informer immédiatement le responsable de traitement de toute demande d'une personne concernée ou d'une autorité[153] ; et
- assister le responsable de traitement pour annoncer une violation de données personnelles, répondre aux demandes d'autorités ou de personnes concernées, réaliser des analyses d'impact relative à la protection des données, et démontrer de manière générale le respect des prescriptions du RGPD[154].

Le responsable du traitement et le sous-traitant peuvent choisir de recourir à un contrat *ad hoc* ou à des clauses contractuelles types, qui sont adoptées soit directement par la Commission soit par une autorité de contrôle conformément au mécanisme de contrôle de la cohérence, puis par la Commission[155]. À ce jour, un tel contrat n'a pas encore été adopté.

L'adhésion du sous-traitant à un code de conduite approuvé[156] ou à un mécanisme de certification approuvé[157] peut être utilisée pour démontrer l'existence de garanties suffisantes par le sous-traitant. L'obligation de recourir à un contrat *ad hoc* parallèlement à une telle adhésion demeure nécessaire.

## F. Failles de sécurité (obligation d'annonce)

En cas d'incident correspondant à une violation de données personnelles susceptible d'engendrer un risque pour les droits et liberté des personnes concernées[158], un régime spécifique de notification institué par les articles 33 et 34 RGPD doit

151 Art. 28 (3) let. g RGPD. Le considérant 81 RGPD précise que les données personnelles ne doivent pas être supprimées si le droit de l'Union ou le droit d'un État membre auquel le sous-traitant est soumis exige la conservation des données personnelles.

152 Art. 28 (3) let. f et 33 RGPD.

153 Art. 28 (3) let. e RGPD.

154 Art. 28 (3) let. f RGPD.

155 Conformément à l'article 28 (7) RGPD et au considérant 81 RGPD.

156 Art. 28 (5) et 40 RGPD.

157 Art. 28 (5) et 42 RGPD.

158 Un tel incident est défini par l'article 4 (12) RGPD comme une violation de la sécurité entraînant de manière accidentelle ou illicite la destruction, la perte, l'altération, la divulgation non autorisée de données personnelles transmises, conservées ou traitées d'une autre manière ou l'accès non autorisé à de telles données. Voir également JAN KLEINER/LUKAS STOCKER, « Data Breach Notifications », Digma 2015.3, 90 ss ; SYLVAIN MÉTILLE, «Annoncer les failles de sécurité n'est plus une option», Expert Focus 11/2017, 863-867.

être respecté par l'assureur afin d'éviter de causer préjudice aux personnes concernées[159].

Toute violation de donnée faisant courir des risques aux droits et libertés individuelles des personnes concernées doit faire l'objet d'une notification à l'autorité de contrôle[160].

L'obligation de notification est assortie d'un délai à partir de la prise de connaissance de la violation par le responsable de traitement. La notification doit se faire sans retard injustifié et, si possible, 72 heures au plus tard après en avoir pris connaissance[161]. Lorsqu'elle est effectuée passé ce délai de 72 heures, la notification doit en outre comporter une motivation[162].

Le sous-traitant doit également notifier au responsable de toute violation de données sans retard injustifié après en avoir pris connaissance[163].

Lorsque la violation de données est susceptible d'engendrer un risque élevé pour les droits et libertés de la personne concernée, le responsable du traitement doit également la lui communiquer dans les meilleurs délais afin qu'elle puisse prendre les précautions qui s'imposent[164].

159 Le considérant 85 RGPD précise qu' une « violation de données personnelles risque, si l'on n'intervient pas à temps et de manière appropriée, de causer aux personnes physiques concernées des dommages physiques, matériels ou un préjudice moral tels qu'une perte de contrôle sur leurs données personnelles ou la limitation de leurs droits, une discrimination, un vol ou une usurpation d'identité, une perte financière, un renversement non autorisé de la procédure de pseudonymisation, une atteinte à la réputation, une perte de confidentialité de données personnelles protégées par le secret professionnel ou tout autre dommage économique ou social important ».

160 Art. 33 (1) RGPD. Le contenu de la notification à l'autorité de contrôle est détaillé à l'article 33 (3) RGPD.

161 Art. 33 (1) RGPD.

162 Art. 33 (4) RGPD.

163 Art. 33 (2) RGPD.

164 Art. 34 (1) RGPD et le considérant 86 RGPD. Le considérant 86 RGPD précise qu'il convient que « de telles communications aux personnes concernées soient effectuées aussi rapidement qu'il est raisonnablement possible et en coopération étroite avec l'autorité de contrôle, dans le respect des directives données par celle-ci ou par d'autres autorités compétentes, telles que les autorités répressives. Par exemple, la nécessité d'atténuer un risque immédiat de dommage pourrait justifier d'adresser rapidement une communication aux personnes concernées, alors que la nécessité de mettre en œuvre des mesures appropriées empêchant la poursuite de la violation des données personnelles ou la survenance de violations similaires peut justifier un délai plus long pour la communication ». L'article 34 (2) RGPD détermine également le contenu de la notification à la personne concernée, qui est d'ailleurs très proche de celui de la notification de l'article 33 auquel il est largement renvoyé.

Le responsable de traitement est dispensé de son devoir de notification aux personnes concernées dans les trois cas suivants[165] :

- s'il a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et que ces dernières ont été appliquées aux données affectées par ladite violation, en particulier celles qui rendent les données incompréhensibles à toute personne non autorisée, telles que le chiffrement[166] ;
- s'il a pris des mesures ultérieures qui garantissent que le risque élevé au regard des droits et des libertés des personnes concernées n'est plus susceptible de se matérialiser[167] ; ou
- lorsque la notification risque d'entraîner des efforts disproportionnés. Dans ce cas, il convient plutôt de procéder à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace[168].

Enfin, le responsable de traitement doit conserver une trace documentée de chaque violation indiquant son contexte, ses effets et les mesures prises pour y remédier. Cette documentation permettra à l'autorité de contrôle de vérifier le respect de l'article 33 RGPD[169].

## G. Droits de la personne concernée

### 1. En général

Le RGPD renforce l'obligation d'information à l'égard des personnes concernées[170] et leurs droits[171]. Ces droits concernent également le droit d'accès aux

165 Art. 34 (3) RGPD.
166 Art. 34 (3) let. a RGPD.
167 Art. 34 (3) let. b RGPD.
168 Art. 34 (3) let. c RGPD.
169 Art. 33 (5) RGPD.
170 Art. 12 RGPD et considérant 58, qui précisent que le principe de transparence exige que toute information adressée au public ou à la personne concernée soit concise, aisément accessible formulée en des termes clairs et simples; Lignes directrices sur la transparence (WP 260 du Groupe de Travail « Art. 29 », adoptée le 29 novembre 2017 et révisé dernièrement le 11 avril 2018).
171 Art. 7 RGPD et chapitre IV.B.2.

données traitées[172], le droit de rectification[173], le droit à l'oubli[174], le droit à la limitation du traitement[175], le droit à la portabilité des données[176] et le droit d'opposition[177].

### 2. Droit d'accès aux données traitées

Sur demande de l'assuré, l'assureur doit lui indiquer si ses données personnelles sont traitées ou non, et lorsqu'elles le sont, lui remettre une copie desdites données[178], ainsi que lui communiquer les finalités du traitement, les catégories de données personnelles concernées, les destinataires ou catégories de destinataires, la durée de conservation, les informations disponibles sur les sources, l'existence d'une prise de décision automatisée, ainsi que des informations sur la logique sous-jacente prévue par ce traitement[179]. Ceci permet à la personne concernée de prendre connaissance du traitement et de pouvoir en vérifier la licéité[180]. Ces informations doivent être fournies par l'assureur dans les meilleurs délais et en tout état de cause dans un délai d'un moins à compter de la réception de la demande. En fonction sa complexité et du nombre de demandes, ce délai peut être prolongé de deux mois[181].

Le droit d'accès ne doit pas porter atteinte aux droits ou libertés d'autrui, y compris le secret des affaires ou à la propriété intellectuelle. Cependant, ces considérations ne devraient pas aboutir à refuser toute communication d'informations à la personne concernée[182], mais on prendra les mesures nécessaires par exemple en caviardant les noms de tiers.

172 Art. 15 (1) et art. 13 (2) et (3) RGPD.
173 Art. 16 RGPD.
174 Art. 17 RGPD.
175 Art. 18 RGPD.
176 Art. 20 RGPD.
177 Art. 21 et 22 RGPD.
178 Art. 15 (3) RGPD.
179 Art. 15 (1) let. a à h RGPD.
180 Art. 15 (1) RGPD ; considérant 63 RGPD.
181 Art.13 (3) RGPD. L'assureur doit motiver sa réponse lorsqu'il a l'intention de ne pas donner suite à de telles demandes. Il doit en outre l'informer de la possibilité d'introduire une réclamation auprès d'une autorité de contrôle (art. 13 (4) RGPD).
182 Art. 15 (4) et considérant 63 RGPD.

### 3. Droit de rectification

Les personnes dont les données sont traitées sont en droit d'exiger de l'assureur que celui-ci rectifie les inexactitudes des données personnelles les concernant. Dans certains cas, si les données personnelles sont incomplètes, il peut être requis de l'assureur de compléter ces données, ou d'enregistrer une déclaration supplémentaire de l'assuré[183].

### 4. Droit à l'oubli

Les assurés ont le droit d'obtenir l'effacement de leurs données, notamment lorsque leurs données ne sont plus nécessaires au regard de la finalité pour laquelle elles ont été collectées ou traitées, ou que l'assuré retire son consentement au traitement et qu'il n'existe aucun autre fondement au traitement et pour les autres motifs listés à l'article 17 (3) RGPD.

### 5. Droit à la limitation du traitement

L'assuré peut également exiger la limitation du traitement de ses données personnelles[184]. Les méthodes visant cette limitation pourraient consister, entre autres, à déplacer temporairement les données sélectionnées vers un autre système de traitement, à les rendre inaccessibles aux utilisateurs, ou à les retirer temporairement d'un site internet[185].

### 6. Droit à la portabilité

Lorsque la personne concernée a fourni les données personnelles sur la base de son consentement ou lorsque le traitement est nécessaire pour l'exécution d'un contrat, elle peut faire valoir son droit à la portabilité des données et recevoir les données fournies à l'assureur dans un format structuré, couramment utilisé et

183 Art. 16 RGPD.

184 Art. 18 (1) let. a à d RGPD.

185 Dans les fichiers automatisés, la limitation du traitement devrait en principe être assurée par des moyens techniques de façon à ce que les données personnelles ne fassent pas l'objet d'opérations de traitements ultérieures et ne puissent pas être modifiées. Le fait que le traitement des données personnelles est limité devrait être indiqué de manière claire dans le fichier (considérant 67 RGPD).

lisible par machine[186]. Une exception au droit à la portabilité existe lorsque la divulgation des données est susceptible de porter atteinte aux droits et libertés de tiers[187].

Comme pour l'exercice du droit d'accès, il est vivement recommandé aux assureurs d'anticiper ces demandes et d'avoir en place une procédure permettant d'y donner facilement suite.

Le droit à la portabilité des données ne devrait pas s'appliquer lorsque le traitement est fondé sur un motif légal autre que le consentement ou l'exécution d'un contrat[188]. Étant donné sa nature, ce droit ne devrait pas être exercé à l'encontre de responsables du traitement qui traitent des données personnelles dans l'exercice de leurs missions publiques, comme les assureurs sociaux[189]. Il ne devrait dès lors pas s'appliquer lorsque le traitement des données personnelles est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ou à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement[190].

Le droit à la portabilité des données s'entend sans préjudice du droit à l'effacement[191].

### 7. Droit d'opposition

Les assurés disposent du droit de s'opposer au traitement de leur données par l'assureur basé sur l'exécution d'une mission d'intérêt public ou des intérêts légitimes[192] ou à des fins de prospection[193], ou de recherches scientifiques, historiques ou statistiques[194].

186 Art. 20 (1) RGPD.
187 Art. 20 (4) RGPD.
188 Art. 20 (1) let. a et b et considérant 68 RGPD.
189 Art. 20 (3) RGPD.
190 Considérant 68 RGPD.
191 Art. 20 (3) RGPD et art. 17 RGPD.
192 Art. 21 (1) RGPD.
193 Art. 21 (2) RGPD.
194 Art. 21 (6) RGPD.

De plus, l'assuré a le droit de ne pas être l'objet d'une décision résultant exclusivement d'un traitement automatisé produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire[195]. Est expressément inclus le profilage, à savoir toute forme de traitement automatisé de données personnelles visant à évaluer certains aspects personnels liés à une personne physique, notamment par l'analyse et la prédiction d'éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles ou les intérêts, la fiabilité ou le comportement, ou la localisation et les déplacements[196].

Toutefois, la prise de décision fondée sur un tel traitement, y compris le profilage, devrait être permise notamment lorsqu'elle est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement, ou si la personne concernée a donné son consentement explicite[197].

En tout état de cause, un traitement de ce type devrait être assorti de garanties appropriées, qui devraient comprendre une information spécifique à l'assuré ainsi que le droit d'obtenir une intervention humaine, d'exprimer son point de vue, d'obtenir une explication quant à la décision prise à l'issue de ce type d'évaluation et de contester la décision[198].

## V. Pouvoirs de l'autorité et sanctions

L'article 68 RGPD prévoit la constitution d'un Comité européen de la protection des données (CEPD), doté de la personnalité juridique et représenté par son président, en lieu et place du Groupe de Travail « Art. 29 ». Son rôle est de contribuer à l'application cohérente du RGPD dans l'ensemble de l'Union.

Afin d'assurer la cohérence du contrôle et de l'application du RGPD, l'article 58 RGPD prévoit trois types de pouvoirs dont les États membres doivent, par voie législative, doter leur autorité nationale de contrôle.

195 Art. 22 RGPD. Voir également MARIA-URANIA DORAS, «Automatisierte Einzelentscheidungen», Digma 2017.2, 98 ss.
196 Art. 4 (4) RGPD.
197 Art. 22 (2) RGPD.
198 Considérant 71 RGPD.

Il s'agit tout d'abord d'un pouvoir d'enquête, notamment celui d'ordonner la communication d'informations dont l'autorité de contrôle a besoin pour exercer ses missions, de mener des enquêtes sous forme d'audits, d'examiner les certifications octroyées au responsable du traitement ou sous-traitant[199], de notifier au responsable ou au sous-traitant une violation alléguée des prescriptions du RGDP, d'accéder à toutes les données et les informations nécessaires ainsi que d'accéder à tous les locaux, installation et moyen de traitement du responsable ou du sous-traitant dans le respect du droit de l'UE et du droit procédural national[200].

S'y ajoute le pouvoir de prendre des mesures correctrices, ce qui inclut notamment le pouvoir d'avertir le responsable ou sous-traitant du fait que leurs traitements envisagés sont susceptibles de violer les dispositions du RGPD, de les rappeler à l'ordre en cas de violation avérée, de leur ordonner de satisfaire aux demandes d'exercice des droits des personnes concernées, de leur ordonner la mise en conformité de leur traitement de manière spécifique et dans un délai déterminé, de leur ordonner la communication d'une violation de données à une personne concernée, de limiter temporairement ou définitivement le traitement, incluant une interdiction de traiter, d'ordonner la rectification, la limitation ou l'effacement de données et la notification de ces mesures aux destinataires auxquels les données ont été divulguée, de retirer ou ordonner à l'organisme de certification de retirer une certification délivrée ou lui faire interdiction de délivrer des certifications si les conditions de la certification ne sont pas ou plus réunies[201], d'infliger des amendes administratives et d'ordonner la suspension des flux de données adressés à un destinataire situé dans un pays tiers ou à une organisation internationale[202].

Enfin, les autorités de contrôle disposent de pouvoirs d'autorisation et de conseil, incluant notamment celui de conseiller le responsable du traitement dans le cadre de la consultation préalable à une AIDP, émettre (de sa propre initiative ou sur demande) des avis à l'attention des pouvoirs législatifs ou exécutifs de l'État membre ou d'autres institutions et organismes ainsi que du public, sur toute question relative à la protection des données à caractère personnel, émettre un avis sur un projet de code de conduite et les approuver; agréer des organismes de

199 Conformément à l'article 42 (7) RGPD.
200 Art. 58 (1) let. a à f RGPD.
201 Au sens de l'article 42 RGPD.
202 Art. 58 (2) let. a à j RGPD.

certification, octroyer des certifications ou approuver des critères de certification, adopter des clauses-types de protection des données[203], approuver des règles d'entreprise contraignantes[204].

Parmi les mesures correctrices les plus importantes, figurent les amendes administratives que les autorités nationales de contrôle pourront fixer. Ces amendes seront imposées en complément ou à la place des mesures correctrices que peut prendre l'autorité[205].

Les amendes en cas de violations, prévues à l'article 83 (4) RGPD, peuvent s'élever jusqu'à EUR 10'000'000 (ou dans le cas d'une entreprise jusqu'à 2% du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu). Pour les violations les plus graves[206], ou en cas de non-respect d'une injonction émise par l'autorité de contrôle[207], l'amende pourra s'élever jusqu'à EUR 20'000'000, respectivement jusqu'à 4%.

Il n'y a pas d'amende minimale ni même d'amende automatique en cas de violation. Au contraire, pour décider s'il y a lieu d'imposer une amende et pour décider de son montant, il est tenu compte dans chaque cas de la nature, la gravité et la durée de la violation, du nombre de personnes concernées, du dommage qu'elles ont subi, du fait que la violation a été commise délibérément ou par négligence, des mesures prises pour atténuer le dommage, du fait qu'il s'agit d'une première violation ou d'une récidive, et de la coopération avec l'autorité en vue de remédier à la violation[208].

S'agissant de la collaboration des responsables de traitement situés en Suisse, on peut se demander si elle est compatible avec l'article 271 CP réprimant les actes exécutés sans droit pour un État étranger. Il n'y a actuellement pas non plus de procédure claire permettant à une autorité étrangère d'encaisser l'amende imposée à une entreprise suisse sans présence dans l'UE et la légalité même de cette amende sous l'angle de l'ordre public suisse n'est pas certaine puisque de telles amendes n'existent pas en droit suisse

203 Au sens des articles 46 (2) let. c RGPD.
204 Conformément à l'article 47 RGPD.
205 Conformément à l'article 83 (2) RGPD.
206 Soit celles figurant à l'article 83 (5) RGPD.
207 En vertu de l'article 58 (2) RGPD.
208 Art. 83 (2) let. a à k RGPD.

## VI. Conclusion

Le RGPD prévoit des conditions strictes, et relativement claires, auxquelles une entreprise qui n'est pas présente au sein de l'Union Européenne peut être soumise à ce règlement. La nationalité des personnes dont les données sont traitées n'est pas un critère de rattachement.

Les assureurs suisses qui visent les résidents européens avec des produits d'assurance et qui traitent dans ce cadre des données personnelles seront soumis au RGPD. Ils ont tout intérêt à se mettre rapidement en conformité.

Pour tous les autres qui ne sont concernés par le RGPD, ils n'ont pas de démarches particulières à entreprendre. Ils auraient toutefois tort de l'ignorer. À n'en pas douter le RGPD va s'imposer comme un standard international. Que ses principes soient ou non repris lors de la révision de la LPD suisse, les assureurs qui pourront s'aligner sur ce règlement auront un avantage compétitif, et les assurés n'y seront certainement pas insensibles non plus.