GUIDE

de la loi fédérale revisée sur la protection des données

Recommandation sectorielle commune

iab. switzerland

SCHWEIZER MEDIEN
MÉDIAS SUISSES | STAMPA SVIZZERA | SWISS MEDIA

LEADING SWISS AGENCIES

SWA ASA
Schweizer Werbe-Auftraggeberverband
Utenti Svizzeri Pubblicità
Association Suisse des Annonceurs
Association of Swiss Advertisers

Février 2023

Auteur: VISCHER AG équipe de protection des données sous la direction de David Rosenthal ainsi que Rolf Auf der Maur (Directeur groupe Droit de l'Association IAB Switzerland)

Frais de protection CHF 95.--

LA NOUVELLE LOI SUR LA PROTECTION DES DONNÉES ET SON IMPORTANCE POUR LES MÉDIAS SUISSES ET AGENCES DE COMMUNICATION ET DE MÉDIAS DANS LE DOMAINE DU MARKETING EN LIGNE

I. INTRODUCTION

1 La loi fédérale sur la protection des données (LPD) a été révisée au cours des dernières années. Après de longues discussions au Parlement et dans le public, la nouvelle loi fédérale sur la protection des données (nLPD) ainsi que la nouvelle ordonnance sur la protection des données (OPDo) entreront définitivement en vigueur le 1er septembre 2023.

2 La révision de la LPD avait notamment pour objectif d'aligner le droit suisse sur les dispositions en vigueur dans l'Union européenne (l'UE), à savoir le Règlement général sur la protection des données (RGPD). Les entreprises suisses qui respectent déjà les dispositions du RGPD pourront donc mettre en œuvre la nLPD sans trop de difficultés. Toutefois, si une entreprise se penche pour la première fois sur ces dispositions, la mise en œuvre des nouvelles obligations de conformité ainsi que l'examen des contrats avec les prestataires de services, les clients et autres tiers nécessiteront des ressources financières, temporelles et humaines.

3 Outre la révision, d'autres développements ont eu lieu ces dernières années dans le domaine de la protection des données, qui posent de nombreuses questions juridiques et des problèmes pratiques difficiles pour les entreprises. On pense notamment à l'arrêt Schrems II de la Cour de justice de l'Union européenne[1], qui a bouleversé les principes jusqu'alors en vigueur en matière de communication de données vers des pays ne disposant pas d'une protection adéquate des données et qui a également impacté la Suisse.

4 La présente recommandation sectorielle de l'Association IAB Switzerland (IAB), de l'Association des Éditeurs de Médias Suisses (AMS), de Leading Swiss Agencies (LSA) et de l'Association Suisse des Annonceurs (ASA) a pour but de fournir à leurs membres, aux annonceurs et à d'autres personnes intéressées des réponses aux questions qui se posent fréquemment dans le cadre de la mise en œuvre de la loi nLPD. En outre, les réponses à ces questions sont présentées dans une deuxième partie à l'aide d'un graphique et de l'illustration de certains cas pratiques courants.

[1] Arrêt C-311/18 de la Cour de justice de l'Union européenne "Schrems II".

II. QUESTIONS FRÉQUENTES

1. Qu'est-ce qui change avec la nLPD et qu'est-ce qui reste pareil ?

5 La bonne nouvelle d'abord : Le concept de réglementation actuel n'a pas été modifié par la révision. Le traitement des données personnelles doit continuer à répondre à certains principes qui n'ont pas été modifiés par la révision. Comme c'était déjà le cas dans le cadre de la LPD actuelle, le traitement des données personnelles, y compris à des fins de marketing, ne nécessitera en principe pas de consentement ou d'autre motif justificatif après l'entrée en vigueur de la nLPD. En résumé, cela signifie que les traitements des données autorisés par la LPD actuelle resteront en principe autorisés sous la nLPD.

6 Bien entendu, la nLPD introduit également une série d'obligations nouvelles et élargies. Ces obligations n'ont pas d'effet ou qu'un effet indirect sur la légalité d'un traitement de données concret. Elles accompagnent plutôt le concept de réglementation générale en matière de protection des données. Entre autres, la nLPD élargit l'obligation d'**informer** les personnes concernées de la collecte de leurs données personnelles. Alors que jusqu'à présent, une information active n'était exigée que dans certaines circonstances, la nLPD prévoit désormais qu'une information doit être fournie lors de chaque collecte de données. La nLPD prescrit un certain contenu minimal, même s'il n'est pas trop étendu (voir question 6). Bien que les déclarations de protection des données deviennent ainsi plus exhaustives en Suisse, elles pourront rester relativement brèves à l'avenir par rapport à celles rédigées en vertu du RGPD.

7 Certaines des nouvelles obligations prévues par la nLPD visent à garantir que les entreprises assurent systématiquement la protection des données dans le cadre de leur conformité. Il s'agit principalement des obligations suivantes, qui ne sont toutefois pas examinées de manière détaillée dans la présente recommandation sectorielle :

- La nLPD reprend une série d'**obligations de documentation** du RGPD. Il s'agit notamment de l'obligation d'établir un **registre des activités de traitement** (art. 12 nLPD) et de l'obligation de réaliser **des analyses d'impact relatives à la protection des données** en cas de traitements de données sensibles (art. 22 nLPD).
- **Les violations de la sécurité des données** doivent **être annoncées** au Préposé fédéral à la protection des données et à la transparence (PFPDT ; art. 24 nLPD) lorsqu'elles sont susceptibles d'entraîner un risque élevé pour les personnes concernées.

2. Quand la nLPD entrera-t-elle en vigueur ?

8 La nLPD entrera en vigueur le 1er septembre 2023. Les entreprises en Suisse auront d'ici là le temps de vérifier et, si nécessaire, d'adapter leurs systèmes et processus, ainsi que leurs contrats et déclarations de protection des données.

9 Par ailleurs, les dispositions pénales (voir question 13) ne pourront être appliquées qu'après l'entrée en vigueur de la nLPD. Cela signifie que les autorités de poursuite pénale compétentes ne pourront pas encore ouvrir et mener des procédures pénales si, par exemple, les déclarations de protection des données ne répondent pas encore aux exigences de la nLPD.

3. Quand faut-il tenir compte de la nLPD dans le cadre du marketing en ligne ?

10 La nLPD s'applique toujours lorsque **des données personnelles**, c'est-à-dire toutes les données relatives à une personne physique identifiée ou identifiable, sont traitées. Cela ne change pas fondamentalement avec la nLPD, mais les données des personnes morales ne seront plus à l'avenir couvertes par la notion de données personnelles et ne seront donc plus protégées par la nLPD.

11 Dans le contexte du marketing en ligne, l'identité de la personne concernée à laquelle une publicité doit être adressée n'est souvent pas du tout connue. En règle générale, un utilisateur peut être reconnu et, en ce sens, "pioché" dans la masse lorsque, par exemple, un cookie a été placé dans son navigateur lors de sa dernière visite sur un site web. Le nom ou le visage qui se cache derrière l'utilisateur en question est toutefois inconnu. Dans un tel cas, selon la conception suisse, il n'y a pas de données personnelles (et la LPD ne s'applique donc pas) tant que l'entreprise, comme par exemple l'annonceur, n'a pas la possibilité de déterminer l'identité (c'est-à-dire le nom ou le "visage") de l'utilisateur. C'est pourquoi les adresses IP, par exemple, ne sont généralement pas considérées comme des données personnelles en Suisse. Cela ne changera pas avec l'entrée en vigueur de la nLPD.

12 Dans l'UE, c'est une autre conception qui prévaut. Ici, une information est déjà considérée comme une donnée personnelle selon le RGPD lorsque l'utilisateur est "singularisé", c'est-à-dire qu'il peut être reconnu parmi tous les utilisateurs ; il n'est justement pas nécessaire que le nom ou le visage de l'utilisateur soit également connu.[2] En effet, les adresses IP, par exemple, sont généralement considérées comme des données personnelles dans l'UE. Il est donc recommandé aux destinataires de la présente recommandation sectorielle de vérifier s'ils doivent également respecter le RGPD dans le cadre de leurs activités de marketing en ligne. Dans l'affirmative, il leur est recommandé de se conformer à la fois aux dispositions du RGPD à celles de la nLPD lors de la mise en œuvre de l'action concrète de marketing en ligne, car il n'est généralement pas possible de séparer les données relevant exclusivement de la nLPD de celles relevant du RGPD. Toutefois, lorsque cette séparation est possible (par exemple en filtrant le trafic Internet), de nombreuses entreprises en Suisse qui ne dépendent pas des données des utilisateurs de l'UE ou de l'EEE

[2] Cf. les décisions de diverses autorités européennes de protection des données concernant l'utilisation de Google Analytics, notamment la décision D155.027 de l'autorité de protection des données de la République d'Autriche du 22 décembre 2021, D.2. point 2. a), disponible à l'adresse suivante https://www.itm.nrw/wp-content/uploads/document-dsb.pdf et la décision de la Commission Nationale de l'Informatique et des Libertés (CNIL) française du 10 février 2022, point II, traduction non officielle disponible sur https://www.cnil.fr/sites/default/files/atoms/files/decision_ordering_to_comply_anonymised_-_google_analytics.pdf.

choisissent cette alternative (c'est-à-dire que les accès en provenance de l'UE ne font pas l'objet d'une analyse plus poussée ou que les cookies de suivi ne sont pas installés pour ces utilisateurs).

4. Qui est responsable du respect des dispositions de la nLPD ?

13 La responsabilité du respect de la nLPD incombe au responsable du traitement, c'est-à-dire à l'entreprise qui détermine les **finalités** du traitement des données et les **moyens de traitement utilisés** à cette fin. Même si le rôle du responsable du traitement existait déjà en principe sous la LPD en vigueur (sous la dénomination de "maître du fichier"), la notion est nouvellement introduite par la nLPD. Elle a été reprise du RGPD et les définitions de la nLPD et du RGPD coïncident également dans une large mesure; de sorte que si une entreprise a le rôle de responsable du traitement en vertu du RGPD, elle l'a également en vertu de la nLPD.

14 Si, par exemple, un annonceur utilise les données de ses clients qui se sont inscrits sur son site web afin de pouvoir leur diffuser de la publicité, il le fait clairement en tant que responsable du traitement : La publicité sert sa propre promotion des ventes (finalité) et il détermine en outre notamment quelles données clients doivent être utilisées, si la publicité doit être diffusée par l'intermédiaire d'un prestataire de services, en ligne ou hors ligne, etc. (moyens de traitement).

15 Il faut également partir du principe que, par exemple, un éditeur qui met son site web à disposition de l'annonceur (ou, à sa demande, d'une agence de publicité ou d'un réseau publicitaire) afin que celui-ci y affiche sa publicité (par exemple par l'intégration d'un cookie tiers) est également considéré comme un responsable du traitement. En effet, l'éditeur, en intégrant le cookie tiers (ou une technologie de suivi similaire), permet la collecte des données de l'utilisateur et décide donc de manière déterminante de la finalité et des moyens du traitement. Il s'ensuit que, dans le contexte du marketing en ligne, l'annonceur dont les produits et services sont finalement promus n'est pas le seul responsable du traitement des données qui s'y rapportent. Au contraire, d'autres acteurs de la chaîne de valeur du marketing en ligne qui collectent les données des utilisateurs et les traitent, parfois en partie pour leur propre compte et parfois conjointement avec l'annonceur (voir question 5), peuvent également être considérés comme des responsables du traitement et donc être tenus de respecter les dispositions relatives à la protection des données. D'ailleurs, selon la jurisprudence de l'UE, le fait qu'une entité donnée ait effectivement accès aux données personnelles ne joue aucun rôle pour déterminer si elle est considérée comme responsable du traitement.

16 En pratique, il est souvent difficile de déterminer si un acteur est considéré comme responsable du traitement (voir également question 5). C'est pourquoi le chapitre III présente, en guise de support, quelques situations courantes de marketing en ligne dans lesquelles sont évalués les rôles possibles des acteurs impliqués en matière de protection des données.

5. Quels contrats doivent être conclus avec les prestataires de services et autres tiers qui ont accès aux données personnelles ?

17 La réponse à cette question dépend en grande partie du rôle du prestataire de services ou d'un autre tiers dans le traitement des données personnelles.

18 Si le prestataire de services reçoit les données afin de les traiter exclusivement **pour le compte et aux fins du responsable du traitement**, il est alors qualifié de **sous-traitant**. Le sous-traitant ne décide pas lui-même de ce qu'il advient des données, mais son service consiste à être l'exécutant du responsable du traitement lors du traitement des données personnelles. Les fournisseurs d'outils publicitaires, comme par exemple Google dans le contexte des services Google Analytics, agissent régulièrement en tant que responsables du traitement (ou du moins se considèrent eux-mêmes comme tels) lors de l'évaluation des données d'utilisation. Il importe peu que le sous-traitant prenne des décisions secondaires sur la manière dont les données sont traitées (par exemple, les mesures techniques et organisationnelles prises pour protéger les données) ou qu'il définisse lui-même son offre de services et la propose exclusivement de manière standardisée.[3] Les outils publicitaires, par exemple, choisissent eux-mêmes leurs systèmes et déterminent le type d'analyses qu'ils proposent ainsi que les algorithmes qu'ils utilisent pour effectuer l'analyse nécessaire des données. Ces aspects ne leur sont pas imposés par leurs mandants, mais cela ne change rien à leur qualification de sous-traitants. Même si, dans de tels cas, le responsable du traitement ne détermine pas toutes les circonstances du traitement des données, son contrôle réside dans le fait qu'il est libre de faire appel à un sous-traitant ou de résilier le contrat avec un sous-traitant existant et de passer à un autre prestataire de services.

19 Le mandant, en tant que responsable du traitement, doit conclure avec le prestataire de services, en tant que sous-traitant, un contrat de sous-traitance. Alors que le RGPD prescrit clairement le contenu d'un tel contrat, la nLPD ne s'exprime pas à ce sujet. En pratique, les contenus exigés en Suisse sont toutefois les mêmes que dans l'UE, raison pour laquelle un contrat de sous-traitance doit notamment couvrir les aspects suivants[4] :

- **Finalités du traitement** : Il est possible de faire référence à un contrat principal (s'il en existe un), ou les finalités du traitement doivent être clairement énumérés dans le contrat de sous-traitance lui-même ;
- **Droit d'instruction du responsable du traitement** : Le sous-traitant ne peut traiter les données que sur instruction documentée du responsable du traitement. Le droit d'instruction doit également porter sur la question de savoir si les données peuvent être communiquées à l'étranger et, dans l'affirmative, à quelles conditions. Le sous-traitant doit en outre informer immédiatement le responsable du traitement s'il estime qu'une instruction est contraire à la législation sur la protection des données ou à une autre

3 DAVID ROSENTHAL, Controller oder Processor : Die datenschutzrechtliche Gretchenfrage, in : Jusletter 17 juin 2019, n. 41 ss.

4 Pour plus d'informations sur le contenu minimal d'un contrat de sous-traitance, voir ROSENTHAL, Controller oder Processor : Die datenschutzrechtliche Gretchenfrage, in : Jusletter 17 juin 2019, annexe : Was in einen ADV gehört.

disposition légale ; il peut suspendre l'exécution du traitement des données jusqu'à ce que le responsable du traitement confirme ou modifie l'instruction ;

- **Recours à des sous-traitants** : La nLPD prévoit désormais qu'un sous-traitant ne peut faire appel à des sous-traitants que si le responsable du traitement l'y autorise de manière générale ou dans un cas particulier. En pratique, le responsable du traitement a le droit de s'opposer dans un délai raisonnable au recours à un nouveau sous-traitant ou au remplacement d'un sous-traitant existant ; si aucun accord ne peut être trouvé entre le sous-traitant et le responsable du traitement, le responsable du traitement a un droit de résiliation extraordinaire. Le responsable du traitement est en outre tenu de soumettre ses sous-traitants à des obligations contractuelles au moins aussi strictes que celles prévues dans le contrat de sous-traitance entre le responsable du traitement et le sous-traitant ;
- **Mesures de sécurité des données** : Le sous-traitant doit être tenu de protéger les données personnelles par des mesures techniques et organisationnelles appropriées. Une liste des mesures prises est jointe en annexe ;
- **Obligation de collaborer** : Le sous-traitant doit être tenu d'assister le responsable du traitement dans le traitement des données et la réponse aux demandes des personnes concernées, dans la réalisation d'analyses d'impact relative à la protection des données ainsi qu'en cas de violation de la sécurité des données (par exemple, si des données sont perdues ou retirées à la suite d'une attaque par un logiciel malveillant).
- **Audits et droits de contrôle** : Le responsable du traitement doit avoir la possibilité de contrôler le traitement des données par le sous-traitant. Cela se traduit généralement par l'obligation du sous-traitant de mettre à la disposition du responsable du traitement toutes les informations et tous les documents nécessaires pour que le responsable du traitement puisse vérifier le respect de la protection et de la sécurité des données. Il peut s'agir, par exemple, de rapports d'audit établis par des organismes de contrôle de contrôle externes. Dans de rares cas, le responsable du traitement a également le droit de procéder à des audits sur place ; mais ce ne sera généralement pas le cas pour les grands fournisseurs, tels que Google, Microsoft et autres fournisseurs similaires ;
- **Fin du contrat** : Après l'expiration du contrat, le sous-traitant doit être tenu, à la demande du responsable du traitement, de restituer les données ou de les effacer définitivement et de confirmer l'effacement au responsable du traitement.

20 Comme indiqué à la question 12, un prestataire de services ou un autre tiers ayant accès aux données des utilisateurs peut également être considéré comme un responsable du traitement s'il participe au moins aux décisions concernant les finalités et les moyens du traitement des données et si ces décisions vont au-delà de la définition de l'offre de services et de la mise en place des

mesures de sécurité des données nécessaires.[5] Ainsi, l'éditeur peut être considéré comme un prestataire de services de l'annonceur lorsqu'il met son site web à la disposition de l'annonceur pour la diffusion de publicités, mais il détermine, par l'intégration d'un cookie tiers ou d'une technologie de suivi similaire, la collecte des données de l'utilisateur dans une mesure si importante qu'il devient également le responsable du traitement et non pas seulement sous-traitant.

21 Si le mandant et le prestataire de services ou d'autres tiers agissent tous deux en tant que responsables du traitement, il convient de faire une distinction:

- Si les deux décident **ensemble** des finalités et des moyens de la collecte et du traitement des données, ils sont alors considérés comme responsables conjoints du traitement (également appelé en anglais *joint controllership*). Dans l'exemple déjà expliqué (l'éditeur intègre un cookie tiers de l'annonceur sur son site web afin que ce dernier puisse collecter des données d'utilisateur et diffuser sa publicité auprès des utilisateurs), les deux acteurs sont régulièrement qualifiés de responsables conjoints du traitement en ce qui concerne l'installation du cookie et la collecte de données qui y est liée, du moins lorsque l'éditeur participe par exemple à la détermination des utilisateurs dont les données sont collectées ou qu'il participe d'une autre manière à la gestion des paramètres de la collecte de données.[6] Le RGPD prévoit que les responsables conjoints du traitement doivent impérativement conclure un ***joint controllership agreement***. Certes, la nLPD ne contient pas d'obligation explicite de conclure un tel contrat, mais il est courant en Suisse d'en conclure un. Ce contrat doit notamment préciser lequel des responsables du traitement concernés apparaîtra dans les rapports externes et, par exemple, répondra aux demandes des personnes concernées ou s'acquittera des obligations d'information.
- Si l'annonceur communique les données au prestataire de services ou à un autre tiers pour que ce dernier les traite (également) à ses propres fins, ce dernier est alors également le **seul responsable du respect de la protection des données** dans ce contexte. C'est le cas, par exemple, lorsque l'annonceur, après avoir collecté les données de l'utilisateur par l'installation d'un cookie tiers sur le site web de l'éditeur (pour lequel les deux peuvent être considérés comme des responsables conjoints du traitement, voir ci-dessus), les compare avec ses propres données et, sur cette base, diffuse de la publicité directe à l'utilisateur. Cette utilisation sert exclusivement les finalités de l'annonceur et il en détermine également les moyens, ce qui fait de lui le seul responsable du traitement. Pour un tel **transfert de responsable du traitement à responsable du traitement,** ni le RGPD ni la nLPD ne prévoient la conclusion obligatoire d'un contrat (tant que les deux acteurs se trouvent

---

5 Pour plus d'informations sur le contenu minimal d'un contrat de sous-traitance, voir ROSENTHAL, Controller oder Processor : Die datenschutzrechtliche Gretchenfrage, in : Jusletter 17 juin 2019 n. 11 ss.

6 Cf. divers arrêts de la Cour de justice de l'Union européenne : C-210/16 de la Cour de justice de l'Union européenne ("Facebook Fanpage"), C-25/17 ("Jehovas Zeugen") et C-40/17 ("Like Button").

dans un pays présentant un niveau de protection des données adéquat; voir question 12). Toutefois, même dans une constellation où le mandant et le prestataire de services ou d'autres tiers sont chacun des responsables indépendants du traitement, il est souvent conseillé de conclure un contrat précisant les finalités pour lesquelles le prestataire de services destinataire peut traiter les données et qu'il doit les garder secrètes.[7]

22 Il est également possible, et même assez fréquent dans la pratique, que le prestataire de services ou un autre tiers n'ait pas de rôle unique par rapport à un seul service. Le rôle du prestataire de services ou autre tiers doit donc être déterminé séparément pour chaque traitement de données. Dans un tel cas, il peut être approprié, par exemple, qu'un contrat de sous-traitance contienne une "clause spéciale" dans laquelle un éventuel transfert de responsable du traitement vers un autre responsable du traitement est également réglementé. Dans la pratique, nous voyons également de plus en plus de prestataires de services qui, pour des raisons pratiques et de responsabilité, essaient consciemment d'éviter les constellations de responsables conjoints du traitement et défendent la position selon laquelle ils sont des responsables indépendants de l'éditeur.

23 En vue de l'entrée en vigueur de la nLPD, il est recommandé aux destinataires de la présente recommandation sectorielle de vérifier les contrats conclus avec des tiers et, le cas échéant, de les adapter ou, si nécessaire, de les conclure.

6. La nLPD étend les obligations d'information - qu'est-ce que cela signifie et sur quels points du traitement des données la personne concernée doit-elle être informée si elle doit recevoir de la publicité en ligne ?

24 La LPD en vigueur ne prévoit une obligation d'information active de la part du responsable du traitement que dans certains cas, bien qu'il soit déjà courant aujourd'hui d'informer les personnes concernées de la collecte et du traitement de leurs données personnelles au moyen d'une déclaration de protection des données. Avec l'entrée en vigueur de la nLPD, il sera désormais obligatoire d'informer activement sur chaque collecte de données ; la violation intentionnelle de cette obligation sera désormais punissable.

25 La personne concernée doit être informée au moins des éléments suivants au moment de la collecte des données :

- l'identité et les coordonnées du responsable du traitement (c'est-à-dire l'entreprise en tant que responsable du traitement) ;
- les finalités du traitement ;
- les éventuels destinataires des données, sans qu'il soit nécessaire de mentionner leur nom ;

7 ROSENTHAL, Controller oder Processor : Die datenschutzrechtliche Gretchenfrage, in : Jusletter 17 juin 2019, n. 59 ss.

- dans quels pays il est prévu de communiquer les données et, s'il s'agit de pays ne présentant pas un niveau de protection des données adéquat, sur la base de quelles garanties (par exemple les SCC de l'UE) ou exceptions légales (par exemple le consentement de la personne concernée dans un cas individuel) cela se fera (ici, la nLPD va exceptionnellement plus loin que le RGPD).

26 Il est toutefois courant de couvrir d'autres points dans la déclaration de protection des données, par exemple d'indiquer que les personnes concernées peuvent demander des informations sur le traitement de leurs données ou l'effacement et la rectification de leurs données, et à quelle adresse elles peuvent envoyer ces demandes.

27 La déclaration de protection des données doit toujours être mise à la disposition des personnes concernées au moment de la collecte de leurs données personnelles. Dans le graphique présenté au chapitre III ci-dessous, c'est par exemple l'éditeur qui fournit la déclaration de protection des données aux personnes concernées lorsqu'elles visitent son site web et les données personnelles de l'utilisateur sont donc collectées auprès de tiers au moyen de cookies tiers (ou d'autres technologies de suivi). Que les données soient ensuite techniquement transmises à l'annonceur (ou à d'autres acteurs) ou que les annonceurs les collectent eux-mêmes techniquement auprès de l'utilisateur sur le site web, cela ne change rien, car l'éditeur est dans tous les cas co-responsable et doit donc mentionner ce processus dans la déclaration de protection des données. Comme la nLPD prévoit que les catégories de destinataires des données doivent être mentionnés, l'éditeur doit s'assurer qu'il indique dans sa déclaration de protection des données qu'il transmet les données aux annonceurs intégrés (ou à d'autres acteurs) ou qu'il collecte ces données personnelles sur son site web. De son côté, l'annonceur doit informer dans sa déclaration de protection des données qu'il traite les données collectées par le biais d'un tiers à des fins de marketing. Cette obligation est souvent remplie lorsque l'éditeur mentionne nommément les annonceurs dans sa déclaration de protection des données et fournit également un lien vers leur déclaration de protection des données. Les annonceurs l'exigent souvent aussi de l'éditeur. Cela explique également pourquoi les annonceurs (et autres tiers fournisseurs de technologies de suivi) sont généralement mentionnés nommément et pas seulement regroupés en tant que catégorie de destinataires, ce qui serait autrement suffisant en soi.

28 Etant donné que la loi révisée sur la protection des données prévoit des obligations d'information plus étendues et que la violation intentionnelle sera en outre punissable, il est recommandé aux destinataires de la présente recommandation sectorielle de vérifier leurs déclarations de protection des données et, si nécessaire, de les adapter.

7. Qu'est-ce que le profilage ?

29 La nLPD introduit désormais la notion de profilage. Ce concept a également été reprise du RGPD. Il y a profilage lorsque les données d'une personne sont utilisées pour évaluer certains aspects

personnels et que cette évaluation est effectuée de manière automatisée, c'est-à-dire par un ordinateur et non par un être humain. Le profilage décrit donc un processus de traitement visant à identifier des modèles qui permettent de tirer des conclusions, par exemple, sur le comportement possible, les capacités, les intérêts ou la santé d'une personne ou d'un groupe de personnes.

30 Un exemple de profilage consisterait pour l'éditeur à suivre le comportement de l'utilisateur sur son site web afin de pouvoir déduire les intérêts de l'utilisateur sur la base de modèles comportementaux. L'évaluation des modèles comportementaux pourrait indiquer que l'utilisateur s'intéresse au golf et au bon vin, ce qui pourrait alors être utilisé pour diffuser des publicités personnalisées. Si l'éditeur se contente de trier les utilisateurs inscrits sur son site web par âge ou par sexe afin d'analyser la répartition démographique, il ne s'agit pas de profilage, car il n'y a pas d'évaluation des caractéristiques personnelles. Inversement, le profilage ne doit pas nécessairement aboutir à un "profil". La sélection automatique de certaines personnes sur la base d'une évaluation de leurs intérêts présumés constitue déjà un profilage.

31 Si, en revanche, le profilage conduit à une combinaison de données telle qu'elle produit une image des caractéristiques essentielles d'une personne concernée, et si ce "profil" est enregistré en tant que tel et comporte à ce titre un risque élevé pour les droits de la personnalité, on parle alors d'un profilage à risque élevé. Il s'agit d'un profilage qui aboutit à un profil de la personnalité (et qui doit donc être considéré comme délicat[8]).

32 La distinction entre le profilage normal et le profilage à risque élevé n'a toutefois peu de conséquences pratiques et juridiques. La seule exception dans le domaine qui nous intéresse ici est qu'en cas de profilage à risque élevé, le consentement doit être explicite s'il doit être obtenu (voir question 8) et une analyse d'impact relative à la protection des données doit être effectuée.

33 Cela dit, le traitement peut évidemment être qualifié de "disproportionné" parce que – avec ou sans profilage – il va particulièrement loin et nécessite donc un consentement ou un autre motif justificatif.

8. Faut-il obtenir le consentement de la personne concernée pour lui diffuser de la publicité en ligne ?

34 Il n'en reste pas moins vrai qu'en Suisse, aucun consentement (ou autre motif justificatif tel qu'un intérêt prépondérant) n'est requis pour que de la publicité, y compris de la publicité en ligne, puisse être diffusée à une personne concernée. Un consentement n'est en principe pas non plus nécessaire pour effectuer un profilage (avec ou sans risque élevé) ou pour transmettre des données d'utilisateurs à des tiers afin que ceux-ci puissent les utiliser, par exemple, à leurs propres fins de marketing. Ceci à condition que

[8] La question de savoir si cette conclusion est nécessaire est toutefois controversée.

- les utilisateurs ont été suffisamment informés dans la déclaration de protection des données, lors de la collecte des données personnelles, que leurs données seront utilisées à des fins de marketing (y compris le profilage, si applicable) et qu'elles seront transmises à des tiers afin que ceux-ci puissent les traiter à leurs propres fins de marketing ;
- le traitement des données ne doit pas être considéré comme disproportionné ; un exemple pourrait être celui d'un éditeur qui crée des profils complets de ses utilisateurs inscrits qui vont au-delà de l'attribution à des intérêts individuels) ;
- aucune donnée personnelle sensible, par exemple des données relatives à la santé, n'est transmise à des tiers.

35 La nLPD et le RGPD s'opposent ici, car le RGPD exige un motif juridique pour tout traitement de données, donc également pour le traitement à des fins de marketing propre ou de tiers. En l'absence de motif juridique, le traitement des données est illégal selon le RGPD. Alors qu'un simple marketing en ligne est normalement considéré comme un intérêt légitime d'un responsable du traitement, les autorités allemandes de protection des données, par exemple, exigent le consentement des personnes concernées pour toute forme de profilage ou de création de profil à des fins de marketing - même pour leurs propres clients. En Suisse, le seuil est plus élevé dans la mesure où certaines activités ne sont pas soumises en soi à une obligation de consentement (comme par exemple l'envoi de publicité électronique de masse).

9. Le consentement de l'utilisateur doit-il être obtenu pour l'installation de cookies ?

36 En Suisse, il ne sera pas non plus nécessaire à l'avenir d'obtenir le consentement de l'utilisateur pour l'installation de cookies et de technologies de suivi similaires (indépendamment des finalités pour lesquelles ils sont installés et indépendamment du fait qu'il s'agisse de cookies internes ou de cookies tiers). L'article pertinent de la loi sur les télécommunications (art. 45c LTC) n'a pas été modifié dans le cadre de la révision de la LPD, et aucune adaptation au droit plus strict de l'UE n'est actuellement en cours.

37 L'utilisateur doit toutefois être informé au préalable de l'installation de cookies qui, du point de vue de l'éditeur, constituent des données personnelles et lui permettent donc d'identifier les utilisateurs ; cela peut se faire au moyen de la déclaration de protection des données, d'une déclaration relatives aux cookies ou d'une bannière de cookies) et une possibilité d'opposition doit être mise à sa disposition (il peut s'agir d'une gestion du consentement en matière de cookies, mais dans la forme la plus simple, il suffit d'indiquer à l'utilisateur qu'il peut également bloquer les cookies dans son navigateur web). Ce principe est différent de celui de l'UE, où la directive 2002/58/CE (directive "vie privée et communications électroniques") exige que l'utilisateur donne son consentement à tous les cookies et à l'utilisation de diverses autres techniques de suivi (même

celles qui sont considérées comme "sans cookie") qui ne sont pas techniquement nécessaires au fonctionnement du site web.[9]

38 Attention : Certains estiment qu'en raison de la nouvelle obligation de protection des données par défaut (art. 7 al. 3 nLPD), il sera à l'avenir également nécessaire d'obtenir le consentement pour l'installation de cookies en Suisse. Selon le point de vue défendu ici, cela n'est pas correct. Premièrement, cette réglementation (contrairement à la réglementation de l'UE en matière de cookies) ne s'applique que si nous sommes en présence de données personnelles. Deuxièmement, cette nouvelle règle stipule uniquement que lorsque des paramètres de cookies (ou d'autres paramètres de protection des données) sont proposés à l'utilisateur, ceux-ci doivent être préréglés sur la position la plus favorable à la protection des données avant que les cookies concernés ne soient automatiquement installés ; le réglage par défaut non confirmé au préalable par l'utilisateur doit donc être limité au minimum. La possibilité d'un tel réglage n'est toutefois pas obligatoire. S'il n'y a pas de paramètres que l'utilisateur peut modifier, il n'y a pas non plus de paramètres par défaut. Si l'utilisateur arrive sur une page de sélection, le réglage le plus avantageux du point de vue de l'éditeur peut déjà être présélectionné sur cette page, à condition qu'il ne soit appliqué que si l'utilisateur le confirme.

10. La personne concernée peut-elle s'opposer à la réception de publicité en ligne ?

39 Oui, elle peut le faire, à tout moment et sans avoir à justifier son opposition. Il est recommandé d'attirer l'attention de l'utilisateur, dans la déclaration de protection des données, sur la manière et le lieu où il peut faire valoir cette opposition et sur le fait qu'une entreprise peut également mettre en œuvre de telles oppositions (liste de blocage).

11. Est-il toujours possible en Suisse de s'appuyer sur le Transparency and Consent Framework de l'IAB ?

40 L'IAB, l'AMS, la LSA et l'ASA estiment que cela reste possible, même si le Transparency and Consent Framework a été soumis à des pressions dans l'UE. La procédure en cours dans l'UE n'a pas d'effet juridique en Suisse. Cela ne changera pas avec l'entrée en vigueur de la nLPD.

41 Il convient toutefois de noter que le cadre pour l'obtention des consentements légitimes est axé sur le RGPD. Comme expliqué notamment à la question 8, les exigences de la nLPD et du RGPD divergent à cet égard, notamment parce qu'en Suisse, le consentement n'est généralement pas nécessaire pour le traitement des données personnelles à des fins de marketing.

42 L'expérience pratique montre toutefois que le Transparency and Consent Framework a également une certaine validité dans les faits en Suisse, c'est-à-dire que les acteurs du marché s'appuient sur son utilisation, y compris pour les éditeurs suisses, et qu'ils l'exigent. A cela s'ajoute le fait que de

9 Pour en juger, la liste de vérification suivante peut vous aider : https://www.rosenthal.ch/downloads/VISCHER-TrackingChecklist.pdf.

plus en plus d'éditeurs décident volontairement d'obtenir le consentement des personnes concernées, même lorsque cela ne serait pas nécessaire d'un point de vue juridique.

12. Les données personnelles peuvent-elles encore être communiquées à l'étranger ? Que se passe-t-il si le pays destinataire ne dispose pas d'une protection des données adéquate ?

43 La nLPD ne modifie pas les principes relatifs à la communication de données personnelles à l'étranger. Les données personnelles peuvent toujours être communiquées aux pays qui disposent d'une législation garantissant une protection adéquate des données. À l'avenir, le Conseil fédéral décidera de manière contraignante quels sont ces pays. Dans l'intervalle, la liste des pays du PFPDT fournit des informations à ce sujet.[10]

44 Si des données personnelles doivent être communiquées à des pays dont le Conseil fédéral décide qu'ils ne disposent pas d'une protection des données adéquate, cela ne sera possible, même dans le cadre de la nLPD, que si des mesures supplémentaires sont prises ou si certaines exceptions s'appliquent. En outre, il sera possible de conclure régulièrement les clauses contractuelles types de la Commission Européenne (**SCC de l'UE**), dont une nouvelle version est disponible depuis juin 2021 et qui ont été déclarées applicables à la Suisse par le PFPDT, avec des destinataires de données situés dans des pays qui ne disposent pas d'un niveau de protection des données adéquat. A l'avenir, l'utilisation des SCC de l'UE ne devra plus être annoncée au PFPDT. Toutefois, pour qu'ils puissent être utilisés pour des transferts de données depuis la Suisse, ils doivent contenir des dispositions supplémentaires et des modifications imposées par le PFPDT (appelées *Swiss Amendments*).[11]

45 Si des données personnelles doivent être communiquées au sein du même groupe d'entreprises, par exemple si un référentiel de données est exploité à l'échelle du groupe et que chaque entreprise du groupe, dont certaines sont situées dans des pays ne présentant pas un niveau de protection des données adéquat, y dépose les données de ses utilisateurs (enregistrés) d'une part et utilise les données personnelles qu'elles contiennent à leurs fins de marketing respectives d'autre part, le groupe peut également le faire sur la base de ce que l'on appelle les règles d'entreprise contraignantes (en anglais *Binding Corporate Rules* ou BCR). Cette alternative est souvent négligée par rapport aux SCC de l'UE. L'inconvénient des règles d'entreprise contraignantes est qu'elles nécessitent l'approbation préalable du PFPDT. Les règles d'entreprise contraignantes sont donc rarement utilisées dans la pratique.

46 Le fait que la légitimité de la communication de données dans des pays ne disposant pas d'un niveau de protection des données adéquat, en particulier les États-Unis, fasse l'objet d'un débat public très controversé n'a donc rien à voir avec l'entrée en vigueur de la nLPD. L'élément

10 https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland.html.

11 https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland.html. https://www.rosenthal.ch/downloads/VISCHER-faq-scc.pdf

déclencheur a plutôt été l'arrêt Schrems II, dans lequel la Cour de justice de l'Union européenne a jugé qu'une communication de données ne peut être licite que si le destinataire des données peut être contraint par ses autorités nationales de fournir des données personnelles (*Lawful Access*), sans que lui-même ou la personne concernée puisse intenter une action en justice, et si de telles demandes de communication répondent à certaines autres garanties. En ce qui concerne les États-Unis, la Cour de justice de l'Union européenne a jugé que deux lois américaines relatives à la surveillance de masse (Foreign Intelligence Surveillance Act (FISA) Section 702 et Executive Order 12333) en particulier ne répondaient pas à ces garanties.

47 Depuis lors, il ne suffit plus de conclure les SCC de l'UE avec le destinataire à l'étranger. Les parties contractantes doivent plutôt s'assurer, et c'est désormais une règle explicite dans les nouvelles SCC de l'UE, qu'elles peuvent respecter les SCC de l'UE indépendamment du droit national du destinataire des données et qu'elles doivent documenter cette évaluation. Cette évaluation et cette documentation doivent être effectuées dans le cadre d'une évaluation de l'impact du transfert (en anglais *Transfer Impact Assessment* ou **TIA**). Cependant, la précision avec laquelle un TIA doit être réalisé et le risque résiduel d'accès aux autorités considéré comme acceptable sont controversés. Une méthode fréquemment utilisée et largement reconnue en Suisse[12] est la méthode de calcul ROSENTHAL.[13]

48 En 2023, la situation pourrait se détendre grâce à une récente évolution juridique, en tout cas en ce qui concerne les États-Unis ; en octobre 2022, le président américain a signé un décret qui limite quelque peu les activités des services de renseignement américains (supposées ou réelles). Les autorités européennes examinent à présent si cela résout les problèmes identifiés dans l'arrêt Schrems II sous le droit américain et si, par conséquent, un TIA ne sera plus nécessaire à l'avenir pour les États-Unis. Si tel est le cas, cela devrait également déterminer la situation juridique en Suisse et nous reviendrions à la situation antérieure à l'arrêt Schrems II, qui, bien qu'il ne s'applique pas formellement à la Suisse, est également suivi dans notre pays.[14]

49 En pratique, le problème du transfert de données vers les États-Unis (par exemple, dans le contexte l'utilisation de services tels que Google Analytics) se pose en particulier lorsque l'on travaille avec le consentement de l'utilisateur, car l'instrument du consentement est utilisé non seulement pour justifier le suivi de l'utilisateur, mais aussi pour respecter les dispositions relatives au transfert de données personnelles vers des pays tiers ne présentant pas un niveau de protection de données adéquat, comme les États-Unis. En effet, si un utilisateur, conscient de la

---

12 Voir par exemple la prise de position de la Chancellerie fédérale du 27 septembre 2022 sur le cadre juridique de l'utilisation de services de cloud public dans l'administration fédérale, en particulier pp. 21 ss., disponible sur https://www.bk.admin.ch/bk/de/home/digitale-transformation-ikt-lenkung/bundesarchitektur/cloud.html.

13 Disponible à l'adresse https://www.rosenthal.ch/downloads/Rosenthal_EU-SCC-TIA.xlsx ; des explications détaillées sur le risque d'accès illégal et le modèle de calcul sont disponibles ici : ROSENTHAL, FAQ on the Risk of Foreign Lawful Access and the Statistical "Rosenthal" Method for assessing IT, disponible à l'adresse https://www.rosenthal.ch/downloads/Rosenthal-LA-method-FAQ.pdf.

14 Voir à ce sujet https://www.vischer.com/know-how/blog/eu-u-s-data-privacy-framework-wann-und-wie-es-fuer-die-schweiz-gelten-wird-39748/ https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7631.

possibilité d'un accès problématique par les autorités américaines, accepte néanmoins que ses données soient communiquées aux États-Unis dans un cas particulier, le problème Schrems II disparaît également selon l'avis défendu ici.[15] Dans l'UE, les responsables de la protection des données se montrent également critiques à l'égard de cette approche, mais en Suisse, aucune opposition ne s'est fait entendre jusqu'à présent.

50 Il est recommandé aux destinataires de la présente recommandation sectorielle de vérifier le plus rapidement possible leurs contrats existants avec des prestataires de services et d'autres tiers dans des pays tiers ne présentant pas un niveau de protection des données adéquat. A cet égard, il convient notamment de vérifier si les contrats sont déjà conformes, si nécessaire, aux nouveaux SCC de l'UE, y compris aux *Swiss Amendments* et, si ce n'est pas le cas, de les adapter.[16] Il faut également en tenir compte lors de l'examen des contrats avec de nouveaux prestataires de services. Il convient également d'effectuer les TIAs nécessaires et de documenter les résultats. En même temps, il convient de vérifier dans quelle mesure les consentements recueillis auprès des utilisateurs couvrent également l'aspect de la communication de données personnelles vers des pays tiers ne présentant pas un niveau de protection des données adéquat, y compris le risque d'accès par les autorités étrangères. Pour qu'il y ait consentement, l'utilisateur doit être informé de ce risque.

13. Qu'est-ce qui sera punissable à l'avenir ? Qui peut être sanctionné et quel est le montant des amendes encourues ?

51 La nLPD élargira la liste des infractions et augmentera les sanctions possibles. Ainsi, sera à l'avenir puni, entre autres, celui qui intentionnellement

- ne respecte pas les obligations d'information (voir question 6), soit en omettant totalement de fournir des informations, soit en fournissant des informations erronées ;
- ne suit pas les exigences en matière de communication de données à l'étranger (voir question 12) ;
- confie le traitement des données à un sous-traitant sans que certaines (pas toutes) des exigences présentées à la question 5 soient remplies.

52 La violation intentionnelle de ces dispositions peut, sur plainte, être punie d'une amende allant jusqu'à CHF 250’000. Les personnes physiques responsables sont sanctionnées en premier lieu. Il peut s'agir d'une part des personnes qui prennent les décisions concrètes (par exemple, le fait de passer volontairement sous silence certains aspects dans une déclaration de protection des données), et d'autre part des dirigeants qui auraient dû empêcher ou remédier à de telles violations par des directives, instructions ou autres mesures appropriées. Contrairement au RGPD, l'entreprise elle-même n'est sanctionnée qu'en deuxième lieu, notamment lorsque l'identification

[15] Au sujet de Google Analytics : https://www.vischer.com/en/knowledge/blog/how-to-legally-use-google-analytics-in-europe-39512/.

[16] L'aperçu suivant peut être utilisé comme base pour l'examen https://www.vischer.com/fileadmin/uploads/vischer/Photos/New-Blog/VISCHER-EU-SCC-Update-Call-2022_FR.pdf.

de la personne physique responsable nécessiterait des efforts disproportionnés et qu'une amende de CHF 50’000 CHF au maximum est envisageable. Cela devrait plutôt être l'exception.

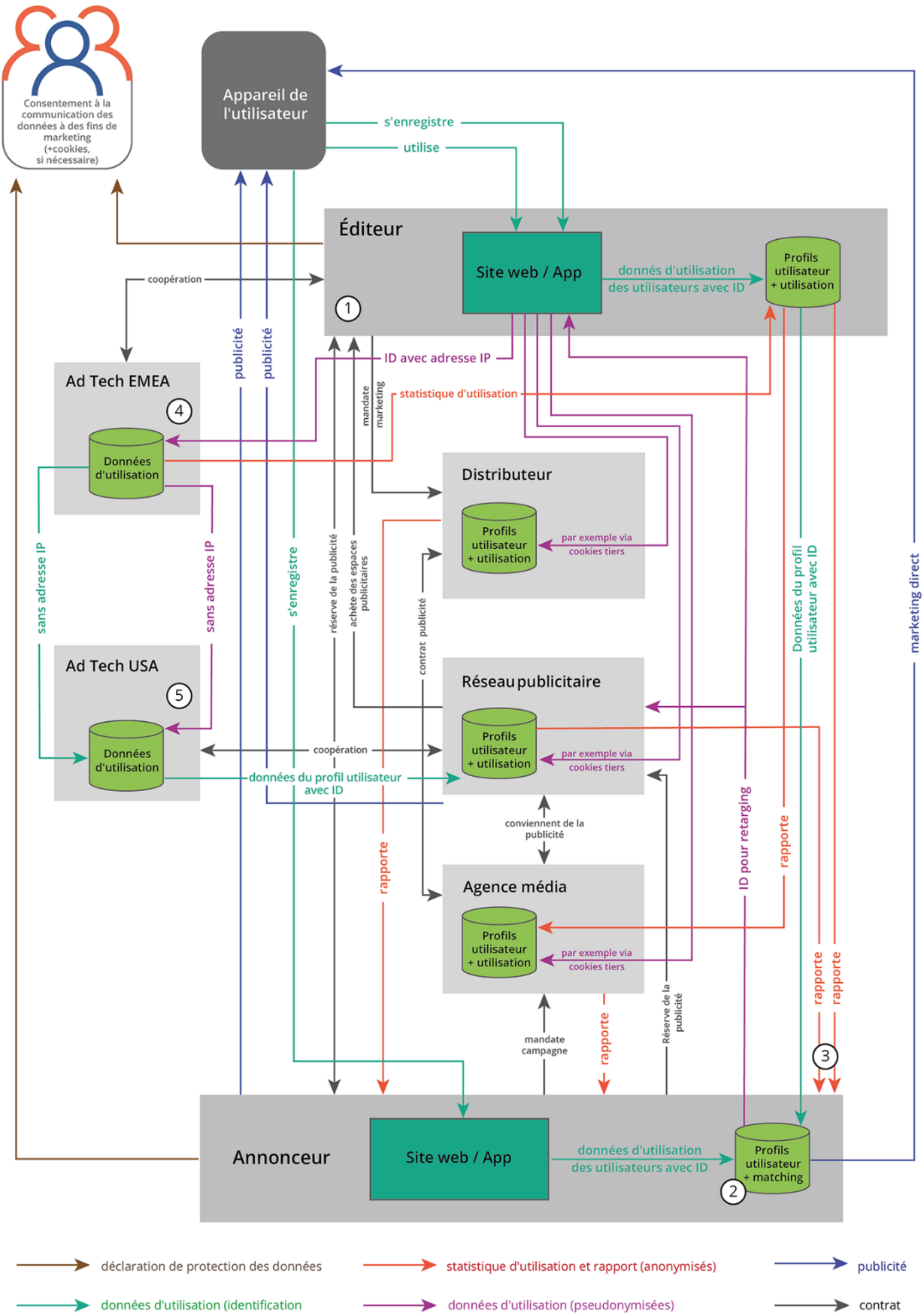
53 Il est également important de savoir que la poursuite pénale n'incombe pas au PFPDT, mais aux autorités cantonales de poursuite pénale. Il s'agit en outre principalement de délits poursuivis sur plainte, pour lesquels il existe un délai de trois mois pour la partie lésée dans ses droits.

III. CAS PRATIQUES

1. Illustration

54 Les explications ci-dessus sont illustrées dans le graphique suivant. Il représente les relations entre les acteurs communs du marketing en ligne et montre de manière schématique quelles données sont transmises et communiquées entre eux et à quelles fins.

Le graphique n'a pas la prétention de couvrir chaque cas particulier auquel les destinataires de cette recommandation sectorielle sont confrontés dans le contexte du marketing en ligne. Il devrait toutefois montrer dans quel rôle en matière de protection des données les différents acteurs peuvent se trouver et aider en outre à identifier et à classer correctement les questions pertinentes en matière de protection des données (du point de vue de la revLPD) dans le contexte du marketing en ligne.



Représentation simplifiée. Par souci de clarté, certaines relations possibles ont été omises.

2. Cas pratique (1)

a) *État de fait*

55 L'annonceur réserve un espace publicitaire sur le site web de l'éditeur. Alternativement, le distributeur, le réseau publicitaire ou l'agence média peuvent le faire pour le compte de l'annonceur. Pour cela, un cookie tiers ou une technologie de suivi similaire (par exemple *Cookieless Device* ou empreinte digitale) est implémenté sur le site web de l'éditeur.

56 L'utilisateur visite le site web de l'éditeur. Il est informé dans la déclaration de protection des données de l'éditeur que

- des cookies tiers sont implémentés sur le site web de l'éditeur et que celui-ci peut s'y opposer, par exemple en modifiant ses paramètres dans le système de gestion du consentement de l'éditeur ;
- ses données d'utilisation sont collectées ; en font notamment partie l'adresse IP, les identifiants des appareils ainsi que le comportement d'utilisation ;
- ces données d'utilisation peuvent être communiquées à des tiers via les cookies tiers afin que ceux-ci puissent les traiter à leurs propres fins de marketing.

57 Par le biais du cookie tiers, l'annonceur collecte les données d'utilisation de l'utilisateur et lui diffuse de la publicité sur les emplacements publicitaires réservés.

b) Analyse

58 Du point de vue de la protection des données, cette situation est évaluée de la manière suivante :

- Les données telles que l'adresse IP ainsi que les identifiants des appareils ne constituent généralement pas en soi des données personnelles au sens de la nLPD. Les parties partiront néanmoins du principe que les données d'utilisation doivent être qualifiées de données personnelles dans la mesure où l'annonceur pourrait disposer d'informations supplémentaires lui permettant d'identifier l'utilisateur. Dans la mesure où le RGPD s'applique, les données doivent être qualifiées de données personnelles – par précaution seulement – dès lors qu'elles permettent une "singularisation", c'est-à-dire une reconnaissance de l'utilisateur.
- Dans le contexte de la collecte des données au moyen du cookie tiers, l'éditeur et l'annonceur doivent souvent être qualifiés de **responsables conjoints du traitement**. Ils concluent un contrat entre responsables conjoints du traitement pour se protéger mutuellement (même si, en vertu de la LPD, ce contrat n'est pas obligatoire).
- Pour savoir si l'éditeur peut communiquer les données d'utilisation à l'annonceur (ou au distributeur, au réseau publicitaire ou à l'agence média) à des fins de marketing, il faut que l'utilisateur en soit informé dans la **déclaration de protection des données** de l'éditeur. Si

l'annonceur collecte lui-même les données par le biais de ses propres cookies tiers, il devrait également être mentionné nommément.

- D'un point de vue purement juridique, un consentement actif à la communication des données n'est nécessaire en Suisse que dans quelques cas individuels (par exemple lorsque des données personnelles sensibles sont communiquées, lorsque l'annonceur est autorisé à établir des profils plus détaillés des utilisateurs ou que de tels profils lui sont transmis, ou lorsqu'une communication internationale de données vers les États-Unis ou un autre pays tiers ne présentant pas un niveau de protection de données adéquat doit être garantie par un consentement). Il peut néanmoins être indiqué d'obtenir un tel consentement en raison des attentes des utilisateurs ou de dispositions contractuelles.
- Si un consentement n'est pas nécessaire, il est malgré tout possible en droit suisse de s'opposer à un traitement (**possibilité d'opt-out**). Cela vaut également pour la communication de données ou la collecte de données par l'annonceur. Celle-ci ne pourra guère être justifiée par un intérêt prépondérant ; l'éditeur devrait donc être en mesure de l'empêcher si une telle opposition a lieu et si l'utilisateur ne doit pas être privé de l'utilisation du site web.
- Dans le cadre du traitement des données des utilisateurs à ses propres fins de marketing, l'annonceur est toutefois le seul responsable du traitement. Il informe l'utilisateur sur le traitement des données à des fins de marketing dans sa propre déclaration de protection des données.

c) *Remarque*

59 En pratique, d'autres acteurs sont régulièrement intercalés entre l'éditeur et l'annonceur. Par exemple, un réseau publicitaire est mandaté par l'annonceur de placer sa publicité sur des plateformes appropriées. Le réseau publicitaire a placé un cookie tiers sur le site web de l'éditeur. Grâce à ce cookie et aux données d'utilisation que le réseau publicitaire collecte via le cookie tiers, il diffuse la publicité de l'annonceur sur le site web de l'éditeur.

60 Dans ce cas, il existe une responsabilité commune entre l'éditeur et le réseau publicitaire en ce qui concerne la collecte des données. L'annonceur sera également considéré comme un responsable conjoint du traitement avec ces derniers, même s'il n'a pas accès aux données d'utilisation collectées par le réseau publicitaire. Ceci en raison du fait que la collecte des données sert ses objectifs de marketing et qu'il a au moins participé à la décision sur les moyens du traitement des données dans la mesure où il a transféré le placement de la publicité au réseau publicitaire. Cela a pour conséquence que l'on devrait également en être informé et même, dans les cas mentionnés, demander un consentement par analogie avec la situation de l'annonceur.

61 Si le réseau publicitaire utilise en outre les données d'utilisation à d'autres fins, il est considéré comme le seul responsable du traitement. Il informe de ces traitements de données dans sa

propre déclaration de protection des données. Attention : Il existe un nombre croissant de prestataires de services qui s'opposent à la qualification de responsables conjoints du traitement (et qui ne proposent donc pas de contrat entre responsables conjoints du traitement). Cela ne change cependant rien au fait que l'éditeur reste également responsable de ce qu'il fait sur son site web.

3. Cas pratique (2)

a) État de fait

62 Cette situation est basée sur le cas pratique 1.

63 L'utilisateur s'inscrit alors en plus sur le site de l'annonceur. En pratique, on lui demandera souvent s'il consent à recevoir de la publicité (personnalisée ou non) par e-mail ou par le biais d'autres canaux push.

64 La déclaration de protection des données de l'annonceur est mise à la disposition de l'utilisateur pour qu'il en prenne connaissance. Il est informé que

- ses données d'utilisation ainsi que ses données d'enregistrement sont collectées ; il s'agit entre autres de l'adresse IP, des identifiants des appareils, de son comportement d'utilisation mais aussi de son adresse e-mail ;
- l'annonceur traite ses données à des fins de marketing et qu'il reçoit également de la publicité (personnalisée ou non) par e-mail ou par d'autres canaux push désignés (régulièrement : uniquement s'il y consent) ;
- qu'il est possible de s'opposer à tout moment à la communication de données personnelles à l'annonceur ainsi qu'à l'envoi de publicité (ou de révoquer son consentement) ;
- l'annonceur évalue à cet effet les données d'utilisation de l'utilisateur (profilage) ;
- l'annonceur met en relation les données d'utilisation et d'enregistrement de l'utilisateur avec les données qu'il reçoit de tiers ;

65 L'utilisateur utilise maintenant le site web de l'annonceur. Cette utilisation est analysée (par exemple l'accès aux pages, la durée de la visite, les transactions, etc.) et l'annonceur établit un profil d'utilisateur.

66 L'annonceur attribue à l'utilisateur un identifiant unique. Il l'utilise dans le cadre de l'emploi de ses cookies tiers.

67 Si l'utilisateur visite maintenant le site web de l'éditeur, il est reconnu comme utilisateur de l'annonceur grâce à son identifiant.

68 L'éditeur collecte pour lui-même les données d'utilisation de l'utilisateur et crée en outre un profil de l'utilisateur (il l'informe en conséquence dans sa propre déclaration de protection des

données). Parallèlement, il transmet à l'annonceur les données d'utilisation et le profil avec l'identifiant (il informe l'utilisateur également de cette communication de données dans sa déclaration de protection des données).

69 L'annonceur met en relation les données d'utilisation et d'enregistrement dont il dispose via l'identifiant avec le profil et les données d'utilisation qu'il a reçus de l'éditeur. Sur la base de ces données, il évalue les intérêts de l'utilisateur (profilage) et lui diffuse (sur le site de l'annonceur) directement de la publicité personnalisée.

b) Analyse

70 Du point de vue de la protection des données, cette situation est évaluée de la manière suivante :

- L'annonceur traite **des données personnelles** puisqu'il connaît l'identité de l'utilisateur.
- Les parties partiront du principe que l'éditeur traite lui aussi des données personnelles, car il ne peut être exclu qu'il puisse découvrir l'identité de l'utilisateur à partir des données dont il dispose. C'est notamment le cas lorsque l'utilisateur s'enregistre également sur le site de l'éditeur. Dans la mesure où le RGPD s'applique, les données devraient – par précaution seulement – être considérées comme des données personnelles dès lors qu'elles permettent une "singularisation", c'est-à-dire une reconnaissance de l'utilisateur.
- L'éditeur et l'annonceur sont considérés comme des **responsables du traitement indépendants**. Ils concluent un contrat pour la communication des données.
- La question de savoir si l'éditeur et l'annonceur peuvent se transmettre mutuellement les données dépend de la question de savoir si l'utilisateur en est informé dans leurs **déclarations de protection des données** respectives. D'un point de vue purement juridique, un consentement n'est nécessaire en Suisse que dans quelques cas individuels (par exemple lorsque des données personnelles sensibles sont communiquées, lorsque l'annonceur est autorisé à établir des profils plus détaillés des utilisateurs ou que de tels profils lui sont transmis, ou lorsqu'une communication internationale de données vers les États-Unis ou un autre pays tiers ne présentant pas un niveau de protection de données adéquat doit être garantie par un consentement). Il peut néanmoins être indiqué d'obtenir un tel consentement en raison des attentes des utilisateurs ou d'un point de vue purement juridique. Attention : Si un site web ou une application utilise des paramètres de protection des données (par exemple au moyen d'un système de gestion du consentement), ceux-ci doivent être préréglés sur l'option la plus respectueuse de la protection des données. Il n'y a toutefois aucune obligation de proposer de telles possibilités de paramétrage.
- Si le consentement n'est pas nécessaire, il est malgré tout possible en droit suisse de s'opposer à un traitement (**possibilité d'opt-out**). Cela vaut également pour la communication de données ou la collecte de données par l'annonceur. Celle-ci ne pourra

guère être justifiée par un intérêt prépondérant, l'éditeur devrait donc être en mesure de l'empêcher si une telle opposition a lieu et si l'utilisateur ne doit pas être privé de l'utilisation du site web.

- L'**envoi d'e-mails publicitaires** ou d'autres messages push doit être évalué séparément[17], car il est régi différemment sur le plan juridique.[18] S'il n'y avait pas de relation contractuelle, un consentement serait nécessaire. Mais comme, dans ce cas pratique, les utilisateurs se sont inscrits auprès de l'annonceur et ont ainsi conclu un accord d'utilisation, l'annonceur n'a pas besoin de consentement, en tout cas pour la publicité de masse pour ses propres produits et services comparables – à condition qu'il ait informé dans sa déclaration de protection des données de l'envoi des messages et de la possibilité de s'y opposer à tout moment (possibilité d'opt-out ici aussi).

4. Cas pratique (3)

a) État de fait

71 Les faits sont basés sur le cas pratique 1.

72 L'éditeur effectue une série d'analyses, comme entre autres le nombre d'utilisateurs à qui la publicité de l'annonceur est diffusée pendant une période donnée.

73 Il met ces statistiques à la disposition de l'annonceur. Elles ne contiennent que des informations agrégées, pas de données sur les utilisateurs individuels. Il n'y a donc pas de données personnelles.

b) Analyse

74 Dans la mesure où l'éditeur collecte ces données au niveau de l'utilisateur, il traite des données personnelles. Il sait à quel utilisateur la publicité a été diffusée.

75 Mais s'il agrège les rapports à l'annonceur de manière à ce que celui-ci ne puisse pas déduire l'identité des différents utilisateurs, il communique à l'annonceur des données anonymisées. Ces données ne sont plus considérées comme des données personnelles, ni en vertu de la nLPD, ni du RGPD.

76 Le droit de la protection des données ne s'applique pas à cette communication et à cette utilisation par l'annonceur. L'éditeur et l'annonceur ne doivent pas conclure de contrat pour la transmission des données (du point de vue de la protection des données). En ce qui concerne l'établissement des statistiques, l'éditeur peut invoquer, du point de vue de la protection des données, le motif justificatif du traitement de données personnelles à des fins non personnelles.

---

17 La liste de contrôle suivante est utile à cet égard : https://www.rosenthal.ch/downloads/VISCHER-Marcom-Checklist.pdf.

18 Art. 3 al. 1 lit. o LCD.

Celui-ci est également disponible sous la nLPD, mais les données doivent être rendues anonymes dès que le but du traitement le permet.

5. Cas pratique (4)

a) *État de fait*

77 L'éditeur utilise les services d'une société Ad Tech basée dans l'EEE.

78 L'utilisateur visite le site web de l'éditeur. Il est informé dans la déclaration de protection de données de l'éditeur que

- des cookies sont implémentés sur le site web et qu'il peut s'y opposer, par exemple en modifiant ses paramètres dans le système de gestion du consentement de l'éditeur ;
- l'éditeur enregistre et analyse son comportement d'utilisateur sur le site web ;
- l'éditeur peut faire appel à des sous-traitants.

79 L'éditeur génère (par exemple à l'aide du cookie interne) un identifiant pour l'utilisateur. En outre, il enregistre le comportement d'utilisation de l'utilisateur.

80 L'identifiant, l'adresse IP et les autres données d'utilisation sont transmises à l'entreprise Ad Tech. Celle-ci analyse les données et fournit des statistiques d'utilisation à l'éditeur.

81 Il s'agit du cas d'application de Google Analytics.

b) *Analyse*

82 Du point de vue suisse, **aucune donnée personnelle** n'est en principe transmise à l'entreprise Ad Tech, dans la mesure où l'on peut supposer que l'entreprise Ad Tech n'est raisonnablement pas en mesure d'identifier l'utilisateur – ne serait-ce que parce qu'elle a pris des mesures appropriées pour s'assurer que les éventuelles données relatives à l'identité de l'utilisateur dont dispose l'entreprise Ad Tech dans un autre contexte ne sont pas réunies.

83 En pratique, les parties se comporteront néanmoins régulièrement comme s'il s'agissait de données personnelles (en particulier si l'applicabilité du RGPD ne peut pas être exclue). Ainsi, l'entrepreneur Ad Tech doit être traité comme un **sous-traitant** de l'éditeur. Les parties doivent conclure un contrat de sous-traitance dans lequel il est notamment stipulé que l'entreprise Ad Tech ne peut traiter les données qu'aux fins de l'éditeur (analyse du comportement des utilisateurs et établissement de statistiques d'utilisation) et qu'il est notamment interdit de les relier à d'éventuelles bases de données "propres" à l'entreprise Ad Tech.[18]

84 Si, en revanche, l'entreprise Ad Tech est autorisée par contrat à utiliser les données également à d'autres fins propres, l'éditeur et l'entreprise Ad Tech concluent en outre un contrat pour la

[18] Google Analytics: https://www.vischer.com/en/knowledge/blog/how-to-legally-use-google-analytics-in-europe-39512/.

communication des données. L'éditeur doit en outre s'assurer qu'il informe les utilisateurs de cette communication de données à des fins étrangères de tiers et qu'ils peuvent s'y opposer (à moins qu'un consentement ne soit même demandé).

6. Cas pratique (5)

a) *État de fait*

85 Les faits sont basés sur le cas pratique 4.

86 Pour l'évaluation des données, l'entreprise Ad Tech dans l'EEE fait appel à sa société mère ou à un hyperscaler ayant son siège aux États-Unis. Cela signifie que les données personnelles de l'éditeur, que celui-ci confie à l'entreprise Ad Tech dans l'EEE, sont en fin de compte envoyées aux Etats-Unis.

87 L'entreprise Ad Tech dans l'EEE transmet l'identifiant et même, le cas échéant, l'adresse IP et d'autres données d'utilisation à l'entreprise Ad Tech aux États-Unis. Cette dernière analyse les données et transmet des statistiques d'utilisation à l'éditeur.

b) *Analyse*

88 L'entreprise Ad Tech aux États-Unis agit en tant que sous-traitant de l'entreprise Ad Tech dans l'EEE. Les deux parties concluent un contrat de sous-traitance. Ce contrat de sous-traitance contient des dispositions identiques, voire plus strictes, que celles contenues dans le contrat de sous-traitance entre l'éditeur et l'entreprise Ad Tech dans l'EEE.

89 L'entreprise Ad Tech de l'EEE communique des données à un pays ne présentant pas un niveau de protection des données adéquate. C'est pourquoi les deux parties concluent les SCC de l'UE. Elles y implémentent les *Swiss Amendments* pour toutes les communications de données en provenance de Suisse.

90 En outre, ils effectuent un TIA afin de pouvoir évaluer le risque d'un *Lawful Access*.

IV. CE QUI DEVRAIT ÊTRE FAIT

91 L'IAB, l'AMS, la LSA et l'ASA recommandent à leurs membres d'examiner leurs activités dans le contexte du marketing en ligne, indépendamment du rôle et des tâches qu'ils assument dans le cadre du marketing en ligne. Pour ce faire, il est recommandé de procéder aux étapes suivantes :

- Examiner le rôle que jouent, en matière de protection des données, les services impliqués dans ses propres activités de marketing en ligne (responsable du traitement, sous-traitant, responsable conjoint du traitement) ;
- Vérifier l'exhaustivité et de l'exactitude de ses propres déclarations de protection des données, notamment en ce qui concerne ...

- la liste des tiers (et leurs déclarations de protection des données) dont les outils de collecte de données sont intégrés dans leur propre site web ou application ;
- les finalités pour lesquelles les données personnelles des utilisateurs doivent également être utilisées par ces tiers ;
- comment déclarer une opposition (ou retirer un consentement).

- Examiner les activités de marketing en ligne afin de déterminer si
  - la nLPD ou le RGPD s'appliquent exclusivement ;
  - des données personnelles sensibles sont communiquées, des profils d'utilisateurs sont créés ou communiqués, ou si des données personnelles sont communiquées à des pays tiers ne présentant pas un niveau de protection des données adéquat (comme les États-Unis) ;
  - si une opposition au traitement de données personnelles à des fins de marketing (ou la révocation d'un consentement) est facilement possible pour les utilisateurs et si elle est correctement mise en œuvre (par exemple pas d'utilisation de cookies, pas de communication de données personnelles après leur communication, le cas échéant également l'effacement de données) ;
  - les données personnelles sont utilisées à des fins qui n'ont pas été communiquées de manière transparente ;
  - les données personnelles soient pseudonymisées le plus tôt possible (pas d'utilisation de vrais noms, là où un pseudonyme ou un code suffit) , voire rendues anonymes ;
  - les données ne sont conservées que pendant la durée raisonnablement nécessaire à la réalisation de l'objectif (c'est-à-dire qu'elles peuvent effectivement contribuer à l'acquisition de connaissances, par exemple) ;
  - lorsque des paramètres de protection des données sont proposés à un utilisateur sur un site web ou dans une application, les paramètres par défaut doivent être aussi favorables que possible à la protection des données. Ceux qui ne le souhaitent pas devraient y renoncer ou demander le consentement préalable nécessaire ;
  - il existe un niveau de sécurité des données approprié, de sorte que non seulement la confidentialité, l'intégrité et la disponibilité des données personnelles sont protégées, mais qu'il est également garanti que le traitement des données personnelles reste traçable.
- Examiner les contrats avec les prestataires de services et autres tiers, notamment en ce qui concerne les prescriptions de la nLPD pour les contrats de sous-traitance (en cas de sous-traitance) et, dans le cas de SCC de l'UE, l'utilisation des *Swiss Amendments* (en cas de

communication dans des pays tiers ne présentant pas un niveau de protection des données adéquat).

- Examiner la possibilité de répondre à d'éventuelles demandes de renseignements conformément aux prescriptions de la nLPD.
- Examiner si les données personnelles peuvent également être effacées ou bloquées de manière fiable à la demande d'une personne concernée.
- Si un traitement de données un peu plus délicat devait débuter après l'entrée en vigueur de la nLPD ou se poursuivre après des modifications importantes, établir une analyse d'impact relative à la protection des données ; celle-ci devrait être conservée en conséquence.
- Vérifier si les exigences pour l'établissement d'un registre de traitement ou d'une journalisation selon l'OPDo sont réalisés, ce qui est notamment le cas lorsque
    - des données personnelles sensibles font l'objet d'un traitement automatisé à grande échelle ou
    - un profilage à risque élevé est effectué.

92 Les étapes à mettre en œuvre concrètement et l'ordre dans lequel elles doivent l'être dépendent en grande partie de l'organisation, des tâches, des services contractuels et de l'activité de marketing concrète.

Zurich, janvier 2023

L'Association IAB (Interactive Advertising Bureau) Switzerland est la représentante de la branche du marketing et de la publicité numérique en Suisse. En tant que membre de l'IAB Europe, elle est également active au niveau international et représente l'industrie dans tous les domaines. L'IAB s'est fixé pour objectif de pratiquer un marketing actif pour le marché de la publicité numérique, de transmettre le savoir-faire, de simplifier la planification de la publicité numérique et de créer des bases et des normes juridiques.

L'Association Médias Suisses (AMS) est l'organisation sectorielle des entreprises de médias privées suisses. L'Association regroupe plus de 100 entreprises de médias qui éditent ensemble environ 300 publications et exploitent de nombreuses plateformes d'information numériques ainsi que plus de 20 chaînes de radio et de télévision.

LEADING SWISS AGENCIES réunit les principales agences de communication de Suisse au sein d'une association. Cela fait de nous un label de qualité pour les mandants. En tant que communauté d'intérêts des principales agences de Suisse, nous définissons des normes de qualité, fournissons une orientation sur des marchés en mutation et nous nous engageons pour des relations de partenariat avec les mandants. Nous encourageons également les échanges entre nos membres. Tout cela dans le but de proposer en Suisse des solutions de communication qui répondent aux exigences les plus élevées – et qui s'imposent également au niveau international. Plus d'informations sur leadingswissagencies.ch.

L'ASA défend les intérêts de ses membres aussi bien vis-à-vis des organes étatiques que du secteur publicitaire et des médias. L'association recherche en principe un consensus raisonnable avec lequel tous les acteurs économiques peuvent vivre et se développer. L'accent est mis sur les thèmes de la liberté de publicité, la transparence et l'équité, la recherche et les statistiques publicitaires, le savoir-faire.