



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

privatim

Konferenz der schweizerischen Datenschutzbeauftragten
Conférence des préposé(e)s suisses à la protection des données
Conferenza degli incaricati svizzeri per la protezione dei dati

**Préposé fédéral à la protection des données et à la transparence
PFPDT**

GUIDE

du 15 décembre 2022¹

**des autorités de protection des données
de la Confédération et des cantons**

**concernant le traitement numérique de données
personnelles dans le cadre d'élections et de votations
en Suisse**

Pour faciliter la compréhension, le document ne contient pas de renvoi vers des textes de loi spécifiques.

¹ Cette mise à jour remplace la version du 1 juin 2019



Table des matières

| | | |
|-----|--|----|
| 1 | Contexte | 4 |
| 2 | Autorités de surveillance et droit applicable..... | 4 |
| 3 | But et destinataires..... | 4 |
| 4 | Acteurs | 5 |
| 4.1 | Partis politiques et groupes d'intérêt | 5 |
| 4.2 | Responsables du traitement ou sous-traitants..... | 5 |
| 4.3 | Registres publics | 6 |
| 4.4 | Sociétés d'analyse de données..... | 7 |
| 4.5 | Vendeurs de données | 7 |
| 4.6 | Plateformes de données | 7 |
| 4.7 | Particuliers..... | 8 |
| 5 | Données personnelles, élections et votations..... | 8 |
| 5.1 | Données personnelles..... | 8 |
| 5.2 | Données sensibles et profils de personnalité..... | 8 |
| 6 | Principes de traitement..... | 9 |
| 6.1 | Bonne foi et transparence | 9 |
| 6.2 | Proportionnalité | 9 |
| 6.3 | Finalité | 10 |
| 6.4 | Exactitude des données | 10 |
| 6.5 | Sécurité des données..... | 10 |
| 7 | Atteinte à la personnalité et motifs justificatifs | 10 |
| 7.1 | Atteinte à la personnalité..... | 10 |
| 7.2 | Intérêt privé ou public prépondérant..... | 11 |
| 7.3 | Consentement | 11 |
| 7.4 | Consentement explicite | 12 |
| 8 | Processus de traitement des données dans le contexte politique | 12 |
| 8.1 | Collecte de données personnelles | 12 |
| 8.2 | Analyse..... | 14 |



| | | |
|-----|--|----|
| 8.3 | Attribution d'informations | 14 |
| 8.4 | Prise de contact avec les personnes concernées | 15 |
| 8.5 | Demande d'un consentement valable | 15 |
| 8.6 | Droits des personnes concernées | 15 |
| 9 | Conformité des sites web | 15 |
| 10 | Exemples pratiques | 16 |
| | Exemple 1 | 16 |
| | Exemple 2 | 17 |
| 11 | Résumé | 18 |



1 Contexte

La société numérique est une réalité globale. Des élections et des votations y sont notamment organisées à tous les échelons de la Confédération. Concernant le traitement de données, les nouveaux phénomènes qui apparaissent sans cesse peuvent avoir des effets sur le comportement électoral. Grâce à la communication en ligne, les acteurs du processus politique de formation d'opinion peuvent véhiculer des messages auprès des électeurs, rapidement et à moindre coût, ou ouvrir un dialogue, en particulier avec ceux qui évitent les médias traditionnels, pour des raisons financières notamment, et qui privilégient les plateformes numériques pour s'informer et échanger.

Le secteur du commerce en ligne collecte et traite de grandes quantités de données personnelles. Il les analyse ensuite pour établir le profil de ses clients existants et potentiels, leur envoyer des messages publicitaires ciblés et leur proposer ainsi des produits et services spécifiques. Les mêmes méthodes de traitement automatisé, à savoir le recours aux mégadonnées, aux outils d'analyse, au profilage et au micro-targeting, sont également utilisées pour adresser des messages ciblés aux électeurs et leur communiquer des informations avec lesquelles les partis et les groupes d'intérêt cherchent à influencer la formation de l'opinion politique en vue d'élections et de votations.

Selon la Constitution fédérale, la garantie des droits politiques protège la libre formation de l'opinion des citoyennes et des citoyens et l'expression fidèle et sûre de leur volonté. Les autorités chargées de la protection des données contribuent au déroulement constitutionnel du processus politique en rappelant aux parties prenantes qu'elles doivent respecter l'autodétermination informationnelle et la protection de la sphère privée garanties par le droit, ainsi que les principes qui en découlent pour le traitement des données personnelles. Toute personne traitant des données dans un contexte d'élections et de votations doit savoir que les informations sur les opinions politiques et philosophiques bénéficient d'un niveau de protection plus élevé que des données comparables du domaine professionnel ou commercial, et que les exigences de traitement posées aux responsables sont plus élevées.

2 Autorités de surveillance et droit applicable

Dès lors que les méthodes de traitement établissent des liens avec des personnes identifiées ou identifiables et qu'elles émanent de particuliers ou d'organes fédéraux, elles sont soumises à la loi fédérale du 25 septembre 2020 sur la protection des données (LPD) et à la surveillance exercée par le Préposé fédéral à la protection des données et à la transparence (PFPDT). Lorsque des données personnelles sont traitées par les organes de droit public des cantons dans le cadre d'élections et de votations, ces traitements sont soumis à la législation cantonale sur la protection des données et à la surveillance locale de la protection des données. C'est pourquoi le guide est une publication commune du PFPDT et de la Conférence des préposés suisses à la protection des données (privatim).

La loi fédérale du 25 septembre 2020 sur la protection des données entièrement révisée et ses ordonnances d'exécution entreront en vigueur le 1^{er} septembre 2023, juste avant les élections fédérales. Notre publication [La nouvelle loi fédérale sur la protection des données : le point de vue du PFPDT](#) donne davantage d'informations sur le sujet. Le droit de la protection des données est aussi en cours de révision dans divers cantons (voir [ch. 8.1](#)).

3 But et destinataires

Le guide est destiné à tous les partis politiques et à tous ceux qui participent à la formation d'opinion politique.



Les autorités chargées de la protection des données le rédigent dans l'exercice de leur mission légale de conseil aux personnes privées et aux organes publics et de sensibilisation du public aux risques systémiques liés au traitement des données personnelles. Il vise à offrir des éléments d'interprétation du droit cantonal et fédéral applicable, qui permettent aux destinataires de déterminer les méthodes de traitement qui sont autorisées sous l'angle du droit la protection des données du point de vue des autorités chargées de la protection des données dans le contexte de la formation de la volonté politique dans l'espace numérique. Il aide également à définir les conditions à remplir.

Son but est aussi d'inciter les acteurs qui participent à la formation d'opinion à appliquer des méthodes de traitement numériques reconnaissables et compréhensibles pour tous. Il faut toutefois bien distinguer la problématique de ce droit légal à la transparence et le débat public sur les informations fallacieuses et la véracité de leur contenu, qui ne saurait faire l'objet ni de la législation sur la protection des données ni du guide. Le vote électronique n'est pas non plus abordé dans ce contexte.

4 Acteurs

4.1 Partis politiques et groupes d'intérêt

Dans le processus politique, les données sont traitées principalement par les partis politiques et les groupes d'intérêt qui poursuivent des objectifs politiques, religieux, sociaux, scientifiques et autres, sous des formes juridiques de droit privé telles que l'association ou la fondation, avec pour but légitime d'influencer la formation d'opinion.

Les partis et les groupes d'intérêt sont libres, dans le contexte du processus politique, de faire appel à des tiers pour le traitement de données en leur confiant tout ou partie du processus ou en se procurant des données auprès de tiers.

Ils sont alors qualifiés de « responsable du traitement » ou, selon le droit en vigueur, de « maître privé du fichier » et assument à ce titre la responsabilité générale de la collecte, de la conservation, de la gestion et de l'utilisation des données traitées (voir [tableau A](#)).

4.2 Responsables du traitement ou sous-traitants

Selon la législation sur la protection des données, les données peuvent être traitées soit au titre de responsable du traitement (encore appelé dans la loi en vigueur « maître du fichier »), soit au titre de sous-traitant. Le responsable du traitement est une personne privée ou un organe d'une autorité qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données personnelles (voir [tableau A](#)). Le sous-traitant est une personne privée ou un organe de l'autorité publique qui traite des données personnelles pour le compte du responsable du traitement (voir [tableau C](#)). Le responsable du traitement reste responsable du respect des dispositions de protection des données, même lorsqu'il confie le traitement des données personnelles à un tiers (sous-traitant). Il est également possible que la responsabilité soit partagée entre plusieurs personnes ou organe d'une autorité traitant des données.

Exemple : l'électeur A visite le site Internet d'un parti et consulte son programme sans y adhérer. Le parti souhaite utiliser les médias sociaux pour cibler les électeurs qui ont visité son site sans y adhérer, c'est-à-dire les électeurs comme A.



À cette fin, il insère sur son site un pixel espion lu par les médias sociaux. Lorsqu'un électeur visite ce site, son navigateur établit alors automatiquement une connexion avec les serveurs des médias sociaux et leur envoie toute une série d'informations. De cette manière, les médias sociaux peuvent généralement surveiller chaque visite sur le site. C'est de cette manière, notamment, que des électeurs sont ajoutés à un groupe cible publicitaire spécifique dans les médias sociaux. Ainsi, après avoir visité le site du parti et consulté les médias sociaux, A voit de la publicité pour le parti sur les médias sociaux.

Le parti et les médias sociaux ont une responsabilité commune.

Si le sous-traitant se trouve dans un pays sans garanties suffisantes du point de vue de la protection des données, des mesures particulières doivent être prises. C'est notamment le cas lorsque des données personnelles sont enregistrées sur un serveur américain. Pour plus d'information sur ce sujet, voir le site du PFPDT ([Transmission à l'étranger \(admin.ch\)](#)).

4.3 Registres publics

Les communes tiennent un registre des électeurs élaboré sur la base du contrôle des habitants. La législation relative au séjour et à l'établissement impose aux nouveaux arrivants et aux personnes quittant une commune de s'annoncer en présentant une preuve d'identité. Ainsi, leur inscription ou leur désinscription auprès du contrôle des habitants permet de déterminer le début et la fin du droit de vote et de l'établir correctement dans le registre électoral. Les registres des électeurs font foi pour les élections et les votations au niveau de la Confédération, des cantons et des communes. Selon le droit fédéral, les registres peuvent être consultés par tout électeur. Les cantons définissent sous quelle forme la consultation est possible (consultation sur place, remise de listes sur papier, remise sous forme numérique). Ils décident également si le contrôle des habitants peut être consulté et, le cas échéant, sous quelle forme.

Certains cantons regroupent les contrôles communaux des habitants dans un registre de tous les habitants du canton. D'autres données sont alors souvent ajoutées à ces registres centralisés (par ex., adresse électronique et numéro de portable repris de la déclaration d'impôt).

Les collectivités publiques responsables des registres publics doivent s'assurer, en leur qualité de responsable du traitement, que les données qui y sont traitées sont en sécurité et qu'elles ne sont transmises à des tiers que si la loi l'autorise. Elles doivent fournir des garanties indiquant que les finalités de traitement sont respectées et qu'il ne peut pas y avoir de fuite de données ([voir tableau B](#)).

Les mesures techniques et organisationnelles prises pour la protection de ces données centralisées varient selon les collectivités locales. Les adresses et les coordonnées sont certes des données personnelles qui relèvent du droit de la protection des données, mais elles ne constituent généralement pas des données sensibles.

Le droit cantonal peut autoriser les services communaux du contrôle des habitants à transmettre, sur demande, les adresses des habitants qui répondent à certains critères (par ex., liste des jeunes habitants) à des particuliers, à des partis ou à d'autres tiers. En général, le demandeur n'a le droit d'utiliser ces listes qu'à des fins bien définies, souvent dans un but idéal, et il lui est interdit de les transmettre à des tiers. Avant de transmettre les données au demandeur, le service compétent de la commune vérifie que la communication est conforme à la législation. Les habitants d'une commune qui souhaitent protéger leurs données personnelles détenues par le contrôle des habitants ont la possibilité de faire bloquer leurs données afin qu'elles ne soient pas communiquées à des tiers sous forme de liste ou de toute autre manière. Il faut pour cela que la commune informe les personnes concernées des conditions et de l'étendue de la communication ainsi que des possibilités de blocage. Actuellement, peu de communes proposent le blocage spécifique de données à des fins de publicité politique. Dans la pratique,



des mesures sont prises pour essayer d'éviter que les mesures de protection mises en place dans le contrôle des habitants et dans le registre des électeurs (par ex., droit de blocage dans le contrôle des habitants) puissent être contournées en consultant l'autre registre.

4.4 Sociétés d'analyse de données

Des sociétés d'analyse de données peuvent être mandatées pour gérer et analyser les données pertinentes des partis et des groupes d'intérêt. Il peut notamment s'agir d'agences de communication ou d'autres sociétés spécialisées dans certaines méthodes d'analyse (par ex., analyse de sites Internet, agence d'indexation).

Mais elles peuvent aussi faire le commerce de données, c'est-à-dire qu'elles peuvent acquérir des données auprès de différentes sources afin de les analyser et de les revendre à des groupes intéressés.

Les vendeurs privés de données qui traitent des données personnelles dans le contexte du processus politique en assument la responsabilité générale au titre de responsable du traitement (voir remarque dans le [tableau A](#)) ou de sous-traitant (voir [tableau C](#)).

4.5 Vendeurs de données

Les vendeurs professionnels de fichiers d'adresses ou les sociétés qui proposent des services similaires rassemblent des informations de toutes sortes, les traitent et les commercialisent de manière systématique et aussi structurée que possible en fonction de caractéristiques personnelles. Les données proposées proviennent d'une multitude de demandes, d'inscriptions, de commandes et de déclarations faites lors de l'achat de marchandises et de services, de l'acceptation de conditions générales de vente ou de la participation à des concours. Des informations publiées par les autorités (statistiques sur les résultats d'une élection, taux de chômage, annonces officielles, registre du commerce et registre des débiteurs) servent aussi de sources de données. D'autres données encore sont collectées lors d'enquêtes menées auprès des consommateurs ou en analysant des sources publiques. Les vendeurs de données combinent toutes ces données et mettent par exemple en relation des adresses privées avec d'autres informations telles que les habitudes d'achat, des aspects sociodémographiques ou encore la situation de vie et le logement.

Les vendeurs privés de données qui traitent des données personnelles dans le contexte du processus politique en assument la responsabilité générale au titre de responsable du traitement (voir remarque dans le [tableau A](#)) ou de sous-traitant (voir [tableau C](#)).

4.6 Plateformes de données

Les plateformes de données gérées par des opérateurs de moteurs de recherche comme Google et les réseaux sociaux qui favorisent la communication et les rencontres virtuelles comme Facebook ou Twitter collectent des attributs personnels (par ex., nom, sexe, âge) que les utilisateurs indiquent au moment de la création de leur compte. Viennent s'y ajouter les nombreuses traces de données collectées automatiquement lorsque des internautes, enregistrés ou non, surfent sur ces plateformes : données techniques telles que l'adresse IP ou le numéro d'appareil, pages marquées au moyen du bouton « J'aime », publications partagées, etc. D'autres informations encore sont collectées à partir de pages web ou d'applications externes liées à ces plateformes par des partenariats publicitaires.

D'autres plateformes, spécialisées dans la collecte de signatures pour les votations, recueillent de grandes quantités de données de contact avec des adresses électroniques, des adresses de domicile



et des indications sur les préférences politiques. Ces plateformes peuvent être gérées directement par les partis ou les groupes d'intérêt, ou il peut s'agir de plateformes de tiers qui proposent leurs services et leurs données aux cercles intéressés.

Les plateformes de données privées qui traitent des données personnelles dans le contexte du processus politique et en assumant la responsabilité générale au titre de responsable du traitement (voir remarque dans le [tableau A](#) et le [tableau D](#)). Si elles traitent de telles données en tant que sous-traitants ou qu'elles les transmettent à des tiers, les remarques du [tableau C](#) s'appliquent.

4.7 Particuliers

Les informations traitées à des fins de formation de l'opinion politique avant des élections ou des votations sont destinées aux électeurs. Alors que la publicité politique est interdite à la radio et à la télévision et que la presse écrite imprime et distribue ce type de publicité sans interaction préalable avec les lecteurs, les plateformes de données offrent la possibilité de transmettre des messages politiques à des groupes de personnes ciblés. Ces personnes peuvent alors elles-mêmes commenter et partager les messages reçus. Dans le monde, les plus grandes plateformes sont utilisées par des milliards d'utilisateurs. Les exploitants des réseaux, mais aussi leurs clients, ont ainsi accès à de grandes quantités de données (adresses, textes, enregistrements sonores, vidéos, images) concernant les utilisateurs, leurs familles, leurs amis et leurs connaissances, données dont ils peuvent tirer des indications sur leurs préférences politiques et philosophiques. Ces informations sont stockées sur les comptes d'utilisateur dans les centres de données des opérateurs de plateformes, et en partie sur les smartphones et autres ordinateurs des utilisateurs. Leur communication ciblée ou leur diffusion publique permet à ces opérateurs et à des tiers d'influencer l'expression de l'opinion politique et le comportement électoral d'autres personnes. Au même titre que les responsables du traitement professionnels, chaque particulier auquel des données sont adressées est responsable de leur traitement dans le contexte politique (voir [tableau E](#)). Pour pouvoir assumer cette responsabilité, le particulier doit déjà avoir conscience qu'elle lui incombe.

5 Données personnelles, élections et votations

5.1 Données personnelles

On entend par données personnelles toutes les informations concernant une personne physique identifiée ou identifiable. Les données purement factuelles, qui ne permettent pas d'établir un lien avec une personne identifiée ou identifiable, ne sont pas soumises à la protection des données. On peut en déduire que la véracité des contenus politiques factuels et la problématique de l'influence exercée sur les électeurs au moyen d'informations fallacieuses ne relèvent pas de la protection des données. Si des contenus indubitablement faux portent atteinte à la personnalité et à l'honneur d'une personne, les dispositions pertinentes du droit civil (art. 28 CC) et du code pénal (art. 173 ss et 261^{bis} CP) s'appliquent.

5.2 Données sensibles et profils de personnalité

Les données dont on peut tirer des indications sur les opinions politiques ou philosophiques sont des données sensibles. La loi pose des exigences particulières pour leur traitement. Au fil des étapes de traitement, d'analyse et de recoupement, des données qui n'étaient pas sensibles au départ peuvent devenir des données sensibles ou permettre d'établir des profils de personnalité, qui sont alors particulièrement protégés par la loi, conformément à la jurisprudence du Tribunal administratif fédéral dans l'affaire Moneyhouse.



Bien qu'il n'existe pas encore de jurisprudence étendue à ce sujet, le traitement numérique des données en lien avec le processus politique est très probablement soumis au niveau de protection applicable pour les données sensibles, ne serait-ce qu'en raison de la finalité du traitement qui vise à influencer les opinions philosophiques de nombreuses personnes. C'est notamment le cas lorsque des méthodes d'analyse automatisées sont utilisées qui, en recoupant un grand nombre de données délicates et non délicates, permettent d'établir des profils de la personnalité qui, selon la jurisprudence du Tribunal administratif fédéral dans l'affaire Moneyhouse², indiquent également une protection accrue des personnes concernées.

6 Principes de traitement

Tout acteur qui traite des données personnelles dans le contexte d'élections ou de votations doit respecter les principes généraux de la législation sur la protection des données. Les organes publics sont en outre tenus de respecter le principe de la légalité, qui impose que tout traitement de données personnelles repose sur une base légale suffisante.

6.1 Bonne foi et transparence

Les acteurs doivent traiter les données conformément au principe de la bonne foi. Ils n'ont donc pas le droit de collecter et de traiter des données d'une manière inattendue pour les personnes concernées et avec laquelle elles ne seraient vraisemblablement pas d'accord.

Le principe de transparence exige que les personnes concernées puissent reconnaître la collecte et le traitement de leurs données. Elles doivent aussi connaître la finalité de chaque traitement, l'identité de la personne qui l'effectue et les catégories de destinataires potentiels des données, lorsque celles-ci sont transmises à des tiers. Elles doivent aussi pouvoir reconnaître la collecte de données personnelles auprès de tiers, tels que des vendeurs de données. C'est seulement à ces conditions que les électeurs peuvent avoir conscience des méthodes de traitement des données et des technologies numériques utilisées pour les approcher et influencer leurs opinions politiques. De même les partis et les groupes d'intérêt ne peuvent prétendre que les méthodes de traitement des données qu'ils utilisent sont acceptées que si celles-ci sont reconnaissables et compréhensibles.

Les organes étatiques qui mettent à disposition des données dans le contexte d'élections ou de votations satisfont aux exigences de transparence en matière de protection des données en respectant les bases légales et les éventuelles prescriptions relatives à leur devoir d'information lorsqu'ils accomplissent leurs tâches.

6.2 Proportionnalité

Le principe de proportionnalité doit aussi être appliqué en ce qui concerne la quantité de données personnelles traitées ou la durée du traitement. La proportionnalité est donnée lorsque l'acteur qui traite les données ne traite que les données appropriées et objectivement nécessaires pour atteindre un objectif (légitime) donné. Les moyens utilisés doivent être raisonnables par rapport à l'objectif poursuivi et les droits des personnes concernées doivent être respectés. La finalité du traitement et les moyens utilisés doivent enfin être acceptables pour les personnes concernées.

² Arrêt TAF A-4232/2015 du 18 avril 2017



6.3 Finalité

Le principe de finalité impose de ne traiter les données personnelles que pour les finalités pour lesquelles elles ont été collectées, qui ressortent des circonstances et qui sont prévues par la loi. Sauf motif justificatif particulier, les données ne peuvent par la suite pas être traitées d'une autre manière, qui ne serait pas compatible avec les finalités initialement indiquées. Le principe de finalité s'applique également en cas d'intégration de services ou d'applications de tiers (par ex., services d'infolettres ou logiciels pour la planification et la gestion de visites de porte-à-porte) ; les tiers ne peuvent pas simplement utiliser les données pour leurs propres finalités.

6.4 Exactitude des données

Tout acteur qui détient un fichier doit s'assurer que les données qui y figurent sont exactes, dès lors qu'elles concernent des personnes. Celui qui traite les données doit prendre toute mesure appropriée permettant d'effacer ou de rectifier les données personnelles inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées.

6.5 Sécurité des données

Enfin, selon le principe de la sécurité des données, la protection des données personnelles contre un traitement non autorisé doit être assurée par des mesures organisationnelles et techniques appropriées. Cette protection n'incombe pas uniquement au responsable du traitement, mais aussi à tous ceux qui traitent des données personnelles, même si elles ne se présentent pas sous forme de fichier. L'obligation concerne donc tous les acteurs qui traitent des données personnelles dans le contexte des élections et des votations. Ils doivent évaluer les risques organisationnels et techniques spécifiques à la protection des données et mettre en place les mesures de protection appropriées. Pour pouvoir s'acquitter de cette tâche, ils doivent disposer d'une documentation interne qui précise comment remplir ces obligations en fonction des catégories de données traitées.

7 Atteinte à la personnalité et motifs justificatifs

7.1 Atteinte à la personnalité

Le responsable du traitement privé qui traite des données personnelles ne doit pas porter une atteinte illicite à la personnalité des personnes concernées. Constitue par exemple une atteinte à la personnalité le fait de traiter des données personnelles en violation des principes de traitement (voir [ch. 6](#)), de traiter des données personnelles contre la manifestation expresse de la volonté de la personne concernée ou de communiquer à des tiers des données sensibles ou des profils de personnalité.

Exemple : un parti politique envoie une infolettre aux personnes qui y sont abonnées. Ce traitement de données ne porte pas atteinte à la personnalité des personnes concernées. Toutefois, si une personne se désabonne, le fait de continuer à lui envoyer l'infolettre porte atteinte à sa personnalité, étant donné que ses données sont alors traitées contre la manifestation expresse de sa volonté.



Exemple : un avocat indépendant se porte candidat à une fonction publique et envoie de la publicité électorale à sa clientèle. Son activité d'avocat et la publicité en vue de son élection n'ont pas de finalité commune. Il n'y a pas non plus de lien logique entre les deux finalités. Ce changement de finalité de traitement ne répond en outre pas aux attentes légitimes de la clientèle. L'avocat n'a donc pas le droit d'utiliser les données de contact de sa clientèle à des fins politiques sans avoir au préalable obtenu son consentement.

Une atteinte à la personnalité n'est pas illicite lorsqu'elle est justifiée par le consentement de la personne concernée, par un intérêt privé ou public prépondérant, ou par la loi. La suite du texte ne traitera pas de la base légale servant de motif justificatif (voir les exemples au [ch. 4.3](#)).

7.2 Intérêt privé ou public prépondérant

Une atteinte à la personnalité peut être justifiée par des intérêts privés ou publics prépondérants. Dans chaque cas, il faut peser les intérêts en évaluant l'importance réelle ou supposée de l'atteinte à la personnalité, et en déterminant si les intérêts privés ou publics sous-jacents au traitement des données sont importants au point de justifier de manière objective et acceptable pour la personne concernée, que la protection de sa personnalité doive passer au second plan.

Le traitement de données dans le contexte politique peut justifier un intérêt privé, voire public légitime, et les droits politiques sont garantis par la Constitution. La question de savoir si cet intérêt est plus important que la protection de la personnalité et doit être qualifié de prépondérant dépend en particulier des données traitées et de la manière dont elles sont traitées.

Exemple : un parti politique achète à un vendeur de fichiers d'adresses un lot de données collectées initialement à des fins marketing. Il utilise ensuite ces adresses pour l'envoi de recommandations de vote. Même s'il est probable que le principe de finalité a été violé dans ce cas, l'atteinte à la personnalité qui en découle est minime et est souvent justifiée par l'intérêt prépondérant du parti.

7.3 Consentement

S'il n'y a pas d'intérêt prépondérant ou que celui qui traite les données ne veut pas prendre le risque qu'un tel intérêt ne soit pas reconnu par la justice en cas de litige, le traitement des données des personnes concernées par l'atteinte à la personnalité doit être justifié par le consentement de ces dernières. Le consentement doit être libre et éclairé.

Un consentement est libre, lorsque les personnes concernées peuvent choisir d'activer ou de désactiver individuellement des aspects et des fonctionnalités dans des applications numériques (par ex., en cochant des cases) et qu'elles peuvent donc réellement décider si elles souhaitent mettre leurs données à disposition et dans quelle mesure. Elles doivent en outre avoir la possibilité, à tout moment, de révoquer leur consentement et de demander l'effacement de leurs données. Pour répondre à ces exigences, les acteurs doivent investir dans des technologies favorables aux exigences de la protection des données.

Un consentement est éclairé lorsque, avant de s'enregistrer, les personnes concernées ont été informées de façon équitable et complète sur le traitement de leurs données et sur le fonctionnement des méthodes d'analyse utilisées à cet effet, analyse automatisée et intelligence artificielle comprises. Elles doivent également être informées de leurs droits, comme celui de se rétracter à tout moment. Une



information équitable est claire, facile à trouver et formulée dans un langage simple et compréhensible. Une information est complète lorsqu'elle se présente en ligne sous forme de texte exposant les buts et le fonctionnement des méthodes de traitement et des technologies numériques à des niveaux adaptés à différents utilisateurs, et donnant en particulier des indications sur la durée de traitement des données et sur la possibilité que les données soient transmises à des tiers. Les informations sont données successivement en commençant par une information succincte bien visible sur la page d'enregistrement, qui résume les points essentiels du traitement des données. Chacun de ces points contient un lien vers les passages concernés des règlements de traitement pertinents et vers les dispositions de la protection des données. Dans le contexte politique, une information équitable ne doit en particulier pas tromper les personnes concernées en leur fournissant des informations fausses ou erronées sur son expéditeur ou sur sa provenance ; et si une personne concernée est contactée directement, elle doit savoir si elle interagit avec une personne réelle ou un programme informatique. La personne doit aussi savoir si une information lui est adressée personnellement ou si elle est adressée à tout le monde. Le cas échéant, les conditions d'utilisation doivent permettre de comprendre à l'aide de quelles technologies ou procédures et selon quels critères les attributions personnalisées sont effectuées. Pour que l'information soit complète, elle doit également préciser si les données sont recoupées avec des données issues des médias sociaux avant d'être analysées (appariement ou *social matching*).

7.4 Consentement explicite

Le traitement de données sensibles ou de profils de personnalité requiert toujours un consentement (libre et éclairé) explicite. Pour que le consentement soit explicite, il faut un acte de consentement actif de la part des personnes concernées. Il y a donc consentement explicite lorsque les personnes concernées se sont enregistrées sur le site web d'un acteur et ont explicitement accepté (par ex. en cochant la case correspondante) le traitement de leurs données. En revanche, les déclarations par lesquelles ces personnes acceptent seulement des conditions générales d'utilisation ne constituent pas un consentement explicite. Il en va de même pour les déclarations par lesquelles elles s'abonnent ou commentent des contenus de ces acteurs, par exemple sur les médias sociaux. Une personne peut en outre consentir uniquement au traitement de ses propres données. Il n'est pas possible de donner un consentement pour le traitement des données de tiers.

8 Processus de traitement des données dans le contexte politique

Le droit suisse autorise le traitement des données par des responsables privés pour autant qu'il n'y ait pas d'atteinte à la personnalité des personnes concernées. Le cas contraire nécessite un motif justificatif (voir [ch. 7](#)). La légalité doit être assurée tout au long du processus de traitement des données. Pour illustrer ce que cela signifie dans le contexte politique, ce processus peut être divisé en fonction de divers éléments : la collecte, l'analyse, l'attribution des informations et la prise de contact avec les personnes concernées.

8.1 Collecte de données personnelles

Si les données personnelles sont collectées directement auprès de la personne concernée, le processus de collecte peut être conçu de manière à respecter ses droits de la personnalité (voir aussi [ch. 7](#)). Dans ce contexte, la transparence et la finalité ainsi que le devoir d'information lors de la collecte de



données sensibles et de l'établissement de profils de personnalité sont essentiels. Il faut donc que les personnes concernées soient notamment informées des données qui sont traitées, des finalités et des modalités de ce traitement. Avec l'entrée en vigueur de la nouvelle loi sur la protection des données en septembre 2023, il devient aussi obligatoire d'informer les personnes concernées lorsque des données non sensibles sont collectées à leur sujet (voir la publication [La nouvelle loi fédérale sur la protection des données : le point de vue du PFPDT](#)).

Si les autres principes de traitement sont par ailleurs respectés et qu'il n'est pas prévu de communiquer des données sensibles ou des profils de personnalité à des tiers, la personnalité des personnes concernées n'est pas atteinte et il n'est pas nécessaire de donner un motif justificatif pour le traitement des données.

Exemple : un parti rassemble des informations en collectant des signatures, en abordant personnellement la population sur des stands, lors de visites à domicile ou par téléphone et ajoute ces informations à celles qu'il détient déjà grâce à l'envoi d'infolettres. Il obtient également des données à partir de sources publiques telles que des annuaires téléphoniques et des registres publics. Mais la majorité des données provient directement des personnes concernées. Dans ce cas, le parti est tenu d'informer les personnes concernées qu'il collecte leurs données pour s'adresser directement à elles et qu'il se procurera, le cas échéant, des données complémentaires librement accessibles.

Si le traitement des données risque de constituer une atteinte à la personnalité, il est recommandé de demander le consentement des personnes concernées, ce qui n'est pas difficile à faire dans ce contexte.

Il est bien plus compliqué de préserver les droits de la personnalité dès lors que la collecte concerne les données personnelles de tiers. Le respect du principe de transparence est, par exemple, pratiquement impossible ou demanderait une charge de travail importante dans le cas où le traitement porterait sur les données d'un grand nombre de personnes. Dans un tel cas ou dans le cas où il serait prévu de transmettre des données sensibles ou des profils de personnalité à des tiers, il faudrait absolument un motif justificatif suffisant.

Exemple : un groupe d'intérêt politique collecte des données personnelles en fouillant des pages et des portails Internet. Il confie cette tâche à des tiers ou leur achète directement les informations. Les informations souhaitées sont collectées en utilisant des services d'indexation qui explorent systématiquement le contenu de pages web et recherchent des adresses électroniques. Dans ces conditions, il est impossible de respecter le principe de transparence et encore moins d'informer activement les personnes concernées. Cette méthode risque aussi de violer le principe de finalité. En conséquence, un intérêt prépondérant doit exister pour ce type de traitement. Si l'acquisition de données repose sur une violation flagrante du droit, l'invocation d'intérêts prépondérants atteint toutefois ses limites, comme c'est le cas lorsque des services d'indexation sont utilisés au mépris des conditions d'utilisation des réseaux sociaux.

La gestion de données collectées au moyen d'un logiciel de campagne peut se situer à la limite de ce qui est justifié par un intérêt prépondérant. Ces logiciels fonctionnent un peu comme un système de gestion de contenu (CMS) flexible. Ils relient les réseaux sociaux courants à un système unique qui permet des interactions avec certains groupes de personnes. Une fois en possession d'une adresse électronique, le groupe d'intérêt peut utiliser une fonction spéciale pour chercher sur les réseaux sociaux à qui elle appartient (social matching) afin d'ajouter les informations ainsi trouvées à ses fichiers (voir [ch. 7](#)). Selon les circonstances, ce



traitement de données porte fortement atteinte aux droits de la personnalité des personnes concernées, de sorte qu'il n'est souvent plus possible de le justifier par un intérêt prépondérant. Le consentement des personnes concernées est alors obligatoire.

8.2 Analyse

Dans un contexte politique, la création de profils a pour but non seulement de distinguer chaque groupe en fonction de ses intérêts communs, mais aussi d'avoir des groupes au sein desquels les personnes ont des positions et des idées politiques similaires.

Afin de prévoir le comportement des personnes, on utilise des intelligences artificielles et on les répartit en fonction de critères démographique, idéologique, socio-économique et psychique. Les profils ainsi constitués peuvent être utilisés pour adresser des messages politiques spécifiques aux personnes concernées.

Dès la compilation des données, le responsable du traitement doit faire attention à ce que les nombreuses données, délicates ou non, ne soient pas combinées d'une façon à établir des profils de personnalité au sens de la loi sur la protection des données, profils sujets à une protection légale qualifiée et accrue. Le Tribunal administratif fédéral s'est largement exprimé sur la question dans l'arrêt Moneyhouse ([ch. 5](#)). La protection qualifiée s'applique également, par la volonté du législateur, au traitement de données sensibles telles que les opinions politiques et philosophiques ([ch. 5.2](#)).

Il n'existe a priori pas de base légale permettant à un organe public d'effectuer des analyses politiques en lien avec des personnes.

8.3 Attribution d'informations

Les partis et les groupes d'intérêt ont pour but d'influencer l'opinion des personnes en vue d'élections ou de votations. À cet effet, ils utilisent des listes de distribution ou les réseaux sociaux pour envoyer des informations ciblées à des groupes dont ils ont établi le profil, en supposant que leurs membres réagissent particulièrement à un certain type de message. Dans ce procédé de micro-targeting, ce ne sont pas seulement les messages ou les contenus qui sont individualisés, mais aussi la manière dont ils sont abordés. Pour que le procédé fonctionne, il faut que les données collectées sur les personnes ciblées soient assez précises pour déterminer le message politique à leur délivrer en passant par leur canal de communication préféré. Le micro-targeting peut surtout être efficace lors de votations, sachant d'expérience que les électeurs n'ont souvent pas d'opinion arrêtée d'avance sur l'objet de votation et qu'ils sont donc plus faciles à influencer.

Toutefois, les messages politiques personnalisés n'ont pas toujours pour seul but d'influencer le vote en soi. Ils visent parfois à favoriser ou à entraver l'exercice des droits politiques selon que les données indiquent que les destinataires partagent ou non l'avis de l'expéditeur. Leur but peut aussi uniquement être d'inciter les destinataires à voter dans le sens de l'expéditeur : les messages sont alors envoyés uniquement à ses partisans et ses opposants politiques sont volontairement laissés de côté.



8.4 Prise de contact avec les personnes concernées

Souvent les personnes concernées apprennent le traitement de leurs données au moment où elles reçoivent un message politique pour la première fois (voir [ch. 8.1 à 8.3](#)), en particulier quand le traitement repose sur un intérêt prépondérant. C'est pourquoi il faut les informer lors de l'envoi du message politique, en leur indiquant qui est responsable de l'envoi, où elles peuvent trouver des informations complémentaires sur le traitement de leurs données et comment elles peuvent faire valoir leurs droits de personnes concernées. Il faut leur expliquer aussi clairement que possible le traitement de leurs données (voir [ch. 8.1 à 8.3](#)) pour qu'elles comprennent sans équivoque le contexte politique du message. Il faut en outre leur proposer une possibilité simple et rapide de s'opposer.

8.5 Demande d'un consentement valable

Pour connaître les conditions d'un consentement valable, voir les explications aux [ch. 7.3 et 7.4](#).

8.6 Droits des personnes concernées

Les responsables du traitement sont tenus de garantir simplement les droits des personnes concernées en matière de protection des données. Toute personne concernée a ainsi le droit de demander au responsable du traitement un accès aux données qu'il traite la concernant et elle peut exiger la correction de données personnelles inexactes ou l'effacement de ses données.

Toutes les personnes doivent donc pouvoir exercer de manière appropriée leur droit d'accès, de correction et d'effacement. Pour ce faire, elles doivent tout d'abord être informées de leurs droits et de la manière dont elles peuvent les exercer. La page web du responsable du traitement et la prise de contact avec les personnes concernées s'y prêtent particulièrement. Si les données sont traitées sous une responsabilité commune ou qu'elles sont confiées à des tiers au titre de sous-traitant, il doit être facile pour les personnes concernées de savoir auprès de quel acteur elles peuvent faire valoir leurs droits.

L'exercice des droits doit être simple et, en règle générale, gratuit pour les personnes concernées.

9 Conformité des sites web

Quiconque gère un site web et traite des données personnelles est tenu de respecter les principes de traitement du droit de la protection des données ; les organes publics doivent en outre respecter le principe de la légalité. La liste de questions ci-après permet de contrôler l'application des principes de traitement en ce qui concerne les sites web.

- Les visiteurs du site sont-ils informés de manière explicite, facilement accessible et intelligible des différents outils de collecte des données utilisés et de la finalité de cette collecte (voir [ch. 6.1](#)) ?
- Est-ce que plusieurs niveaux d'information ont été mis en place afin de tenir compte des visiteurs qui souhaitent en savoir davantage, ou, pour le dire autrement, les explications simples et concises qui sont fournies sont-elles complétées par des informations plus techniques ?
- Les visiteurs peuvent-ils choisir précisément (de manière « granulaire ») quels outils de pistage des utilisateurs ils souhaitent autoriser ?



- Si le site contient des plug-ins sociaux de Facebook ou des services analogues, quelles sont les technologies qui garantissent que le pistage et la transmission des données ne sont possibles qu'avec l'accord de l'utilisateur (voir [ch. 7.3](#) et [7.4](#)) ?
- Les personnes concernées sont-elles informées de leurs droits, notamment de leur droit d'accès aux données qui les concernent ? Est-ce que toutes les mesures techniques et organisationnelles nécessaires pour pouvoir répondre aux demandes de renseignements ont été prises (voir [ch. 8.6](#)) ?
- Le pistage des utilisateurs récupère-t-il uniquement les données nécessaires pour l'utilisation prévue (voir [ch. 6.1](#) et [6.3](#)) ?
- Est-ce que des solutions pour le pistage des utilisateurs et l'analyse web excluant toute utilisation par des tiers à leurs propres fins ont été mises en place, par exemple en installant des outils d'analyse directement chez le responsable du traitement ou en anonymisant les adresses IP (voir [ch. 6.3](#)) ?
- Si des tiers sont mandatés, les personnes concernées en sont-elles informées ? Les tiers mandatés sont-ils tenus de démontrer qu'ils ont pris toutes les mesures techniques et organisationnelles nécessaires pour assurer la sécurité des données, et ces mesures font-elles l'objet de contrôles (voir [ch. 4.2](#) et [6.5](#)) ?
- Un éventuel transfert de données (par ex., envoi d'un formulaire de contact) est-il systématiquement chiffré ?
- Les personnes concernées sont-elles informées au préalable que leurs adresses électroniques seront éventuellement réutilisées, par ex. en vue de recueillir des informations sur les réseaux sociaux, et leur consentement est-il demandé spécifiquement à cet effet (voir [ch. 6.1](#), [7.3](#) et [7.4](#)) ?

10 Exemples pratiques

Exemple 1

Un parti politique se présente comme association pour recruter de nouveaux membres lors de manifestations ou sur son site web. Il propose aux visiteurs de s'abonner à une infolettre en échange de leur adresse électronique. L'association a l'intention de mettre toutes les adresses électroniques ainsi obtenues à la disposition des exploitants d'un média social et d'utiliser ainsi les techniques de ciblage et d'amplification de ce média pour adresser sa publicité politique de manière ciblée à des personnes présentant un profil de personnalité similaire.

Il n'y a pas de lien logique évident entre la finalité de la collecte, qui est d'envoyer aux visiteurs les informations actuelles du parti à caractère général, et la finalité supplémentaire, qui est de transmettre des messages politiques à caractère idéologique ciblant des personnes en fonction de profils de personnalité. Cette finalité supplémentaire ne répond donc pas aux attentes légitimes des destinataires de l'infolettre. L'association ne peut pas faire valoir d'intérêts privés et publics prépondérants suffisants pour justifier une telle atteinte à la personnalité.



Elle ne peut donc pas utiliser les adresses électroniques sans en informer préalablement les destinataires de l'infolettre et sans obtenir leur consentement explicite pour la finalité de traitement supplémentaire, à savoir faire de la publicité politique ciblée et personnalisée.

Exemple 2

Une agence de publicité travaille pour un parti politique. Elle propose par ailleurs sur les médias sociaux un test d'aptitude professionnelle, qui comprend une évaluation psychologique.

En remplissant le test, les participants donnent à l'exploitant des médias sociaux, en plus de leur adresse électronique et leurs coordonnées, des informations sur leur formation, leur activité professionnelle, leur statut d'emploi, leur âge, leurs hobbies. L'agence achète ces informations à l'exploitant des médias sociaux et s'en sert pour cibler au mieux les personnes à qui elle envoie la publicité politique pour le compte du parti qui l'a mandatée.

Le traitement des données au moyen de telles techniques de ciblage est contraire aux principes de finalité et de bonne foi. Aucun intérêt privé ou public prépondérant ne peut être invoqué dans ce cas et les personnes concernées, qui sont des électeurs potentiels, doivent donc être informées avant la collecte des informations demandées que leurs données seront également traitées à des fins de marketing politique ciblé et que leur consentement explicite est requis pour ce traitement supplémentaire.



11 Résumé

| | |
|---|--|
| <p>A Partis politiques et groupes d'intérêt</p> | <p>Les partis politiques et les groupes d'intérêt qui assument une responsabilité générale en qualité de responsable du traitement (anciennement maître de fichier) (ch. 4.1 et 4.2) doivent tenir compte des remarques suivantes.</p> <ul style="list-style-type: none">• La légalité du traitement et le respect des principes inscrits dans la LPD (ch. 6) sont garantis, qu'un tiers soit impliqué ou non.• Les tiers mandatés qui assument une responsabilité commune doivent prouver qu'ils respectent l'ensemble des prescriptions légales en matière de protection des données (ch. 6)• Les tiers mandatés en tant que sous-traitants doivent signer un contrat par lequel ils s'engagent à respecter toutes les prescriptions légales en matière de protection des données, et notamment à prouver qu'ils prennent des mesures organisationnelles et techniques appropriées pour assurer la sécurité des données (ch. 6.5) et qu'ils ne traitent les données personnelles qu'aux fins convenues dans le contrat.• Le droit des électeurs à la transparence (ch. 6.1 et 9) est assuré par des informations disponibles sur un site web concernant :<ul style="list-style-type: none">- l'identité des responsables du traitement,- les catégories de données traitées,- la collecte de données avec renvoi vers les sources tierces,- la finalité actuelle et, si nécessaire, le motif justificatif du traitement,- les méthodes de traitement, y compris la finalité et le fonctionnement des méthodes d'analyse utilisées (intelligence artificielle comprise),- les catégories de destinataires éventuels des données,- les rôles, les obligations et les responsabilités des fournisseurs, des sociétés d'analyse ou des plateformes de données,- les conditions d'utilisation déterminantes de tiers et leurs références.• Le traitement doit respecter les principes de finalité (ch. 6.3) et de proportionnalité (ch. 6.2), selon lesquels un traitement supplémentaire des données doit toujours être conforme au but défini lors de la collecte et ne durer que jusqu'à ce que ce but soit atteint.• Les personnes concernées doivent avoir donné leur consentement explicite au traitement de leurs données dans le contexte du processus politique (ch. 7.4).• L'exactitude des données doit être garantie même lorsqu'un tiers est impliqué et les données devenues inutiles sont effacées (ch. 6.4).• Les risques relatifs à la protection des données sont évalués et des mesures organisationnelles et techniques appropriées sont prises pour y remédier (ch. 6).• Une documentation interne indique comment la sécurité des différentes catégories de données est garantie (ch. 6).• Lorsque des services ou des applications de tiers (par ex., services d'infolettres ou planification et gestion de visites de porte-à-porte) sont utilisés, les directives concernant la communication de données à des tiers et la transmission de données personnelles vers l'étran- |
|---|--|



| | |
|--|--|
| | <p>ger s'appliquent. Pour plus d'information sur ce sujet, voir en particulier le site du PFPDT (Transmission à l'étranger (admin.ch)) et les documents suivants :</p> <ul style="list-style-type: none">- Prise de position sur la transmission de données personnelles vers les États-Unis et d'autres États n'offrant pas un niveau de protection des données adéquat au sens de l'art. 6 al. 1 LPD (lien : Prise de position PDF),- Guide pour l'examen de la licéité de la communication transfrontalière de données (lien : Guide PDF) <ul style="list-style-type: none">• Les droits d'accès aux données, les éventuelles obligations de déclarer les fichiers et les devoirs d'annoncer la transmission de données personnelles à l'étranger doivent être respectés vis-à-vis des autorités chargées de la protection des données. |
| B Registres publics | <p>Lors de la gestion des registres de contrôle des habitants et des registres des électeurs (ch. 4.3), les autorités compétentes s'assurent :</p> <ul style="list-style-type: none">• que le traitement des données se déroule conformément aux dispositions légales concernant son but, son contenu, son ampleur et sa durée,• que des données personnelles sont transmises uniquement si une base légale suffisante le permet ou que les données ont été pseudonymisées efficacement au préalable,• que les personnes enregistrées disposent de possibilités de blocage, si la loi n'interdit pas a priori la transmission de leurs données à des fins de publicité politique,• que les risques concernant la sécurité technique et organisationnelle, réidentification comprise, sont évalués et documentés et les mesures de protection nécessaires prises (ch. 6.5),• que les fuites ou pertes de données sont annoncées sans délai aux autorités chargées de la protection des données compétentes. |
| C Vendeurs et sociétés d'analyse de données | <p>Les sociétés d'analyse des données (ch. 4.4) et les vendeurs de données (ch. 4.5) qui traitent des données personnelles dans le contexte du processus politique et en assument la responsabilité générale au titre de responsable du traitement tiennent compte des remarques du tableau A. S'ils agissent en qualité de sous-traitants qui traitent des données personnelles dans le contexte du processus politique,</p> <ul style="list-style-type: none">• ils respectent les obligations contractuelles qu'ils ont envers le responsable du traitement,• ils s'assurent, avant de conclure un contrat, que leur mandant a la volonté et les capacités techniques et organisationnelles de sous-traiter les données reçues conformément à la loi et au contrat,• ils tiennent compte de la jurisprudence dans l'affaire Moneyhouse relative au profilage par combinaison de données issues de différentes sources (ch. 5),• ils assurent la sécurité des données conformément à leurs obligations contractuelles (ch. 6.5),• à la demande de leur mandant, ils l'aident à éliminer les risques et lui annoncent toute perte de données. <p>Ils établissent des conditions d'utilisation et des conditions contractuelles écrites dans lesquelles ils expliquent</p> |



| | |
|---|---|
| | <ul style="list-style-type: none">• comment les données transmises ont été collectées, à partir de quelles sources, par quelles méthodes et dans quel but,• si les personnes concernées ont pu donner leur consentement à la transmission et au traitement de leurs données, dans quel but et sous quelle forme. |
| D Plateformes de données | <p>Les plateformes de données privées (ch. 4.6) qui traitent des informations dans le contexte du processus politique en qualité de responsable du traitement assumant une responsabilité générale ou en qualité de sous-traitant se conforment en général à des conditions générales de vente et d'utilisation.</p> <ul style="list-style-type: none">• Elles respectent le droit des électeurs à la transparence dans le traitement de leurs données (ch. 6.1 et 8.4) et investissent donc constamment dans des technologies favorables aux exigences de la protection des données, afin d'offrir aux utilisateurs des informations à différents niveaux et de vraies options numériques faciles à utiliser.• Elles fournissent aux autorités chargées de la protection des données compétentes des interlocuteurs dûment informés et autorisés, qui sont en mesure de donner des renseignements en cas de pertes de données ou d'autres incidents en lien avec la protection des données qui pourraient avoir des conséquences sur des élections ou des votations. <p>Les plateformes de données qui traitent des informations en qualité de responsable du traitement, tiennent aussi compte des remarques du tableau A. Si elles le font en qualité de sous-traitant, elles tiennent compte des remarques du tableau C.</p> |
| E Particuliers | <p>Les particuliers qui partagent, évaluent ou publient des contenus et des opinions politiques sur des réseaux sociaux veillent à préserver la vie privée et d'autres aspects des droits de la personnalité des personnes concernées, tels que l'honneur et la vie familiale.</p> <p>Ils ne transmettent pas d'informations sur leurs amis, sur les membres de leur famille ou sur toute autre personne identifiable à des partis politiques, des groupes d'intérêt, des vendeurs de données, des sociétés d'analyse de données ou des plateformes de données, sans leur consentement explicite préalable. Ils s'assurent que les logiciels qui accèdent à ces données proviennent de sources fiables.</p> |