Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB
Préposé fédéral à la protection des données et à la transparence PFPDT
Incaricato federale della protezione dei dati e della trasparenza IFPDT
Incumbensà federal per la protecziun da datas e per la transparenza IFPDT

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

GUIDE

du 1er décembre 2018

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

État: 1er juin 2019

Ce guide a été élaboré en collaboration avec les experts suivants:
Urs Maurer-Lambrou, avocat, et Adrian Vatter, politologue.

Pour des raisons de compréhension, il a été renoncé aux renvois vers des textes de loi spécifiques dans le présent document.

Feldeggweg 1, 3003 Berne
Tél. 058 463 74 84, fax 058 465 99 96
www.edoeb.admin.ch

Table des matières

1 Objet et destinataires du guide

La société numérique est une réalité globale dans laquelle sont notamment organisées des élections et des votations à tous les échelons de la Confédération. De nouveaux phénomènes apparaissent sans cesse en matière de traitement des données, avec des effets potentiels sur le comportement électoral. La communication en ligne permet aux acteurs du processus politique de formation d'opinion de véhiculer des messages auprès des électeurs, rapidement et à moindre coût, ou d'ouvrir un dialogue avec eux, en particulier lorsque ceux-ci évitent les médias traditionnels, pour des raisons financières notamment, privilégiant les plateformes numériques pour s'informer et échanger.

Le secteur du commerce en ligne se procure et traite de grandes quantités de données personnelles, qu'il analyse pour transmettre des messages publicitaires personnalisés à ses clients existants ou potentiels, et leur proposer ainsi des produits et services adaptés à leur profil. Les mêmes méthodes de traitement automatisé, à savoir le recours aux mégadonnées, aux outils d'analyse, au profilage et au «microtargeting» sont également utilisées pour adresser des messages ciblés aux électeurs et leur communiquer des informations avec lesquelles partis et groupements d'intérêts cherchent à influencer la formation de l'opinion politique en amont des élections et des votations.

Dans la mesure où ces méthodes de traitement établissent des liens avec des personnes identifiées ou identifiables et émanent de personnes privées ou d'autorités fédérales, elles sont soumises à la loi fédérale sur la protection des données (LPD) et à la surveillance du Préposé fédéral à la protection des données et à la transparence (PFPDT). Cependant, lorsque de tels traitements sont le fait d'autorités cantonales et communales assurant l'exécution des élections et des votations, ce sont les législations cantonales et la surveillance locale en matière de protection des données qui sont déterminantes, ce qui explique la double paternité du présent guide, partagée entre le PFPDT et la Conférence des Préposés cantonaux à la protection des données (Privatim).

Conformément à la Constitution fédérale, la garantie des droits politiques protège la libre formation de l'opinion des citoyennes et des citoyens ainsi que l'expression fidèle et sûre de leur volonté. Les autorités chargées de la protection des données contribuent à la constitutionnalité 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 en matière de 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 idéologiques bénéficient d'un niveau de protection plus élevé que les données comparables du domaine professionnel ou commercial.

Les autorités chargées de la protection des données rédigent le présent guide 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 permettant, dans l'environnement dynamique de la numérisation, d'appliquer la LPD de 1992 aux traitements de données liés aux élections et aux votations. Il s'adresse à tous les acteurs de la formation de l'opinion politique pour les inciter à rendre les méthodes de traitement numériques claires et compréhensibles. Il convient de distinguer de ce droit à la transparence du traitement des données deux domaines différents : la problématique de la véracité des contenus (thématique des «fake news»), qui n'est pas couverte par la législation relative à la protection des données, ainsi que le vote électronique en Suisse, qui n'est également pas abordé dans ce guide.

2 Partis politiques et groupements d'intérêts

Le traitement des données dans le processus politique, ainsi que les objectifs légitimes qui y sont liés pour influer sur la formation de l'opinion, sont principalement le fait de partis et de groupements d'intérêts qui poursuivent des objectifs politiques, religieux, sociaux, scientifiques et autres, sous des formes juridiques du droit privé telles que l'association ou la fondation.

Bien qu'il n'existe pas encore de jurisprudence complète sur le sujet, on peut partir du principe que les traitements numériques de données en relation avec le processus politique sont généralement soumis, ne serait-ce que parce qu'ils consistent à influencer l'opinion publique, à un niveau de protection correspondant à des données sensibles. C'est notamment le cas lorsque des méthodes d'analyse automatisées sont utilisées, aboutissant, via la comparaison d'une multitude de données sensibles ou non sensibles, à des profils de personnalité, qui nécessitent également une protection accrue des personnes concernées, conformément à la jurisprudence du Tribunal administratif fédéral dans l'affaire Moneyhouse[1]. Les partis politiques et groupements d'intérêts assumeront donc, en tant que «maîtres» privés de fichiers de données, leur responsabilité générale concernant notamment la collecte, la conservation, le suivi et la réutilisation des données ainsi traitées (cf. tableau A). Pour cela, ils doivent respecter le principe fondamental de la transparence (chiff. 7). Les partis et groupements d'intérêts ne peuvent obtenir un consentement approprié que s'ils indiquent les méthodes de traitement qu'ils appliquent, de manière suffisamment claire et compréhensible pour les citoyennes et les citoyens.

Les partis et les groupements d'intérêts 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. Dans le cadre de leur responsabilité générale de maîtres de fichiers, ils rendent transparents l'intervention et les rôles de ces tiers qui, en fonction des circonstances, agissent également en tant que maîtres ou seulement comme sous-traitants. Ils s'assurent que ces derniers respectent de leur côté la législation sur la protection des données (cf. tableau C).

3 Registres publics

Les cantons tiennent un registre électoral, qui repose sur le Contrôle des habitants. La législation relative au séjour et à l'établissement impose aux nouveaux arrivants et aux personnes quittant la commune de s'annoncer. 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. Celui-ci forme la base des élections et des votations au niveau de la Confédération, des cantons et des communes. Le droit fédéral prévoit que les électrices et les électeurs bénéficient d'un droit de consultation du registre électoral, sous une forme déterminée par les cantons (consultation sur place, remise de listes au format papier, remise sous forme numérique). Ceux-ci régissent également la possibilité et la forme d'un droit de consultation du Contrôle des habitants.

Certains cantons réunissent les services communaux du Contrôle des habitants dans un registre de tous les habitant(e)s du canton. Ces registres centralisés sont fréquemment enrichis de données supplémentaires (p. ex. adresse e-mail et numéro de téléphone portable provenant de la déclaration d'impôt).

[1] Arrêt TAF A-4232/2015 du 18 avril 2017

Dans le cadre de leur responsabilité générale de maîtres de fichiers publics, les services communaux compétents pour les registres publics doivent s'assurer que les données qui y sont traitées sont conservées de manière sûre et ne sont transmises à des tiers que si la loi l'autorise. Ils doivent garantir l'absence d'utilisations impropres ou de pertes de données incontrôlées (cf. tableau B).

Les mesures techniques et organisationnelles prises pour la protection de ces fichiers centralisés varient selon les communes. Les données d'adresses et de contact constituent certes des données personnelles qui entrent dans le champ d'application de la législation sur la protection des données, mais elles ne sont pas considérées comme des données sensibles.

Le droit cantonal peut autoriser les services communaux du Contrôle des habitants à communiquer à des partis, des personnes privées ou d'autres tiers intéressés, des données d'adresse sur les habitants classées selon certains critères (c.-à-d. au moyen de listes, p. ex. les jeunes citoyens). En règle générale, ces listes ne peuvent être utilisées par le demandeur qu'à des fins bien définies, souvent dans des buts idéaux, et ne peuvent être transmises à des tiers. Le service compétent de la commune vérifie si les conditions légales pour une communication des données sont remplies, et peut ensuite transmettre les données au demandeur. Les habitants de la commune qui souhaitent protéger leurs données personnelles détenues par le Contrôle des habitants ont généralement la possibilité de bloquer leurs données afin d'éviter toute communication de liste ou toute transmission à des tiers. Cela suppose que la commune informe les personnes concernées des conditions et de l'étendue de la communication et des possibilités de blocage. À ce jour, les autorités ne proposent guère de possibilités de blocage spécifiques pour la publicité réalisée à des fins politiques. Dans la pratique, on cherche à s'assurer par des moyens appropriés que les mesures de protection indiquées au niveau du Contrôle des habitants ou du registre électoral, telles que le droit de blocage au Contrôle des habitants, ne sont pas contournées par une consultation dans l'autre registre.

4 Processus de traitement des données

Conformément à la définition légale, le traitement de données correspond à toute opération relative à des données, indépendamment des moyens et procédés appliqués. Dans le contexte d'élections et de votations, ce processus se répartit entre la collecte, l'analyse et l'attribution d'informations.

4.1 Collecte de données

Pour le traitement de données dans le processus politique, les partis et groupements d'intérêts peuvent d'abord s'appuyer sur des stocks de données qu'ils ont eux-mêmes constitués, tels que les adresses de membres, les listes d'adresses e-mail d'abonnés à des newsletters, et autres informations similaires. Souvent, ces données sont complétées par des informations que les partis et groupements d'intérêts demandent en collectant des signatures, en abordant personnellement la population sur des stands, lors de visites à domicile ou par téléphone. Par ce biais, les partis ou les groupes d'intérêt peuvent, en plus des données de contact des personnes abordées, requérir leurs préférences politiques individuelles ou d'autres informations pertinentes. En outre, des données peuvent être obtenues à partir de sources accessibles au public telles que les annuaires téléphoniques ou les registres publics.

Il est également possible d'utiliser des portails ou des sites web statistiques au moyen de web-mining («fouille du web») pour se procurer des données sur Internet, de confier de telles tâches à des tiers ou d'acquérir de telles informations contre rémunération. Les services de robots d'indexation (web crawlers) peuvent rechercher des contenus de sites web ou des adresses e-mail de manière systématique

et se procurer les informations souhaitées. Par ailleurs, les plateformes de données peuvent constituer des sources de données supplémentaires.

Les données collectées sont rassemblées par les partis ou les groupes d'intérêt et peuvent être exploitées à l'aide d'un logiciel dédié aux campagnes politiques et électorales. Ces logiciels fonctionnent comme un système de gestion de contenu (« content management system » ou CMS) flexible et relient les réseaux sociaux courants à un système unique qui permet des interactions avec certains groupes de personnes. Une fois qu'ils disposent d'une adresse électronique, les partis et groupes d'intérêt peuvent utiliser une certaine fonction pour rechercher la personne correspondante dans les réseaux sociaux (« social match ») et enrichir leur collecte de données avec les informations associées (voir chiffre 7).

Le logiciel de campagne soutient le parti ou le groupe d'intérêt dans la planification et la mise en œuvre de ses actions et permet de combiner le potentiel de la propre collecte de données avec les possibilités des réseaux sociaux, grâce à l'utilisation centralisée des possibilités d'analyse et de sélection des réseaux sociaux dans le logiciel.

Pour toute forme de collecte de données à des fins politiques, les responsables doivent respecter en particulier le principe de transparence (chiffre 7). Il convient de mentionner que la collecte d'informations telles qu'opinions philosophiques ou politiquesest soumise à une protection juridique qualifiée (chiffre 7).

4.2 Analyse

Dans le commerce en ligne, de grandes quantités de données hétérogènes («big data») sont traitées sur de longues périodes, agrégées et réunies à des fins d'analyse. Des méthodes d'analyse et des systèmes informatiques performants permettent d'exploiter des données et d'identifier les intérêts de personnes individuelles ou de petits groupes partageant les mêmes idées. À l'aide de modèles statistiques, des prédictions peuvent être réalisées afin de déterminer les produits ou services adaptés à tel ou tel groupe de profil de clients, nouveaux ou existants («predictive analytics»). Les clients existants ou potentiels sont ensuite démarchés via les messages publicitaires correspondant à leur profil, ou reçoivent par exemple des recommandations de produits personnalisées dans une boutique en ligne.

La constitution de profils dans le contexte politique vise à ce que chaque groupe de profil se distingue d'autres groupes par ses intérêts communs, mais aussi à ce que les personnes au sein de ces groupes se ressemblent davantage, dans leurs conceptions et positions politiques, que des personnes de groupes différents.

La segmentation des personnes sur la base de leurs caractéristiques démographiques, idéologiques, socio-économiques et psychiques ainsi que de diverses méthodes d'intelligence artificielle est utilisée pour prédire leur comportement. Ces profils peuvent être exploités pour aborder les personnes concernées de manière ciblée au travers de messages politiques.

Dès la collecte des données, le maître du fichier doit tenir compte du fait qu'une multitude de données sensibles – c.-à-d. devant faire l'objet d'une protection particulière –, ou de données non sensibles en soi, peuvent se condenser en profils de personnalité au sens de la loi sur la protection des données. Elles sont alors soumises à une protection légale qualifiée, ou accrue. Le Tribunal administratif fédéral s'est exprimé en détail sur le sujet dans l'arrêt Moneyhouse (chiff. 2). La protection qualifiée s'applique également au traitement de données sensibles, telles que les opinions politiques ou philosophiques (chiff. 7).

4.3 Attribution d'informations

En supposant que les personnes constituant un groupe de profil commun réagissent de manière particulièrement marquée à certains messages, des informations ciblées doivent être communiquées à ce groupe via une liste de diffusion par e-mail ou les réseaux sociaux. À travers cette méthode, les partis et les groupements d'intérêts cherchent à influencer la formation de l'opinion politique en amont d'élections et de votations. Avec le «microtargeting», on individualise non seulement des messages ou des contenus, mais aussi la manière dont ils sont adressés. Cela suppose que la connaissance des personnes cibles, sur la base des données collectées, soit suffisamment précise pour pouvoir lui transmettre des messages politiques lui correspondant par ses canaux de communication préférés.

Le «microtargeting» peut notamment déployer l'effet d'influence visé lors de votations, où l'on sait d'expérience qu'un grand nombre d'électeurs n'a pas encore d'opinion fixe sur un sujet donné. En revanche, lors de scrutins proportionnels comme les élections au Conseil national, on observe souvent un comportement électoral stable, fondé sur la tradition et l'habitude. Il peut encore en aller autrement lors des élections au Conseil des États, lorsque des candidats sont soutenus au-delà du cadre des partis.

Des messages attribués de manière personnalisée dans le contexte politique ne visent pas toujours nécessairement à influencer les comportements électoraux par leur contenu. Ils peuvent également avoir pour effet d'inciter au vote ou au contraire d'en dissuader leurs destinataires, selon que les données analysées les désignent plutôt comme des alliés ou des adversaires politiques. Une autre possibilité consiste à n'envoyer ces messages que de manière sélective, en négligeant les adversaires politiques supposés, afin d'inciter les destinataires à aller voter.

5 Autres acteurs du traitement de données

5.1 Commerçants de données

Des commerçants de données professionnels et fournisseurs de prestations similaires se procurent des informations de toutes sortes, qu'ils traitent et commercialisent de manière systématique et aussi structurée que possible sur la base de caractéristiques personnelles. Les données proposées proviennent d'une multitude de demandes, d'inscriptions, de commandes et de déclarations, qui ont été effectuées dans le contexte de commandes de biens et de services, de conditions commerciales ou de concours. Des informations publiées par les autorités, telles que les statistiques sur les résultats électoraux ou les taux de chômage, ainsi que les communiqués publics, registres du commerce et listes de débiteurs sont également utilisés comme sources de données. D'autres données sont obtenues auprès des consommateurs au moyen de sondages ou collectées via l'exploitation de sources généralement accessibles. En combinant des données issues de sources différentes, ces prestataires professionnels enrichissent par exemple des adresses privées d'informations complémentaires variées relatives aux comportements d'achat, à la socio-démographie, au logement ou encore à la composition du ménage.

Les commerçants de données traitent des données personnelles dans le contexte du processus politique en tant que maîtres de fichier assumant une responsabilité générale (cf. remarque au tableau A) ou en tant que sous-traitant (cf. tableau C).

5.2 Sociétés d'analyse de données

Les sociétés d'analyse de données peuvent assurer en tant que mandataires la gestion et l'analyse des données pertinentes des partis ou groupements d'intérêts. Il peut par exemple s'agir d'agences de communication ou d'autres entreprises qui se sont spécialisées dans certains procédés d'analyse (p. ex. analyse de sites web, agences d'indexation).

Les sociétés d'analyse de données peuvent également être des commerçants de données qui se procurent des informations de manière indépendante à partir de différentes sources, les analysent et les mettent ensuite à la disposition des groupes intéressés contre rémunération.

Les sociétés d'analyse de données privés traitent des données personnelles dans le contexte du processus politique en tant que maîtres de fichier assumant une responsabilité générale (cf. remarque au tableau A) ou en tant que sous-traitant (cf. tableau C).

5.3 Plateformes de données

Les plateformes de données d'opérateurs de moteurs de recherche tels que Google ou les réseaux sociaux facilitant la communication et les rencontres virtuelles, comme Facebook ou Twitter, collectent des attributs personnels (p. ex. nom, sexe et âge) indiqués par les utilisateurs enregistrés disposant d'un compte. À cela s'ajoutent de nombreuses pistes de données enregistrées automatiquement et laissées par les utilisateurs d'Internet, enregistrés ou non, lors de leur visite de plateformes de données. Cela comprend des données techniques comme les adresses IP ou les identifiants d'appareils, ainsi que les informations sur les pages marquées d'un «J'aime», les publications partagées, etc. Sont également collectées des informations d'applications ou de sites web externes qui sont associées aux plateformes concernées au travers de partenariats publicitaires.

D'autres plateformes spécialisées dans la collecte de signatures pour des votations collectent de grandes quantités de données, y compris les adresses électroniques et postales et les préférences politiques. Ces plateformes sont soit gérées par les partis ou les groupes d'intérêt eux-mêmes, soit mettent à disposition leurs données en tant que fournisseurs tiers.

Dans la mesure où des plateformes privées traitent des données personnelles dans le contexte du processus politique en tant que maîtres de fichier assumant une responsabilité générale, il convient de tenir compte des remarques indiquées au tableau A et au tableau D. Si elles traitent ou transmettent de telles données en tant que sous-traitants, les remarques du tableau C s'appliquent.

5.4 Personnes individuelles (destinataires)

Les destinataires d'informations traitées à des fins de formation de l'opinion politique en amont d'élections et de votations sont les titulaires du droit de vote. Alors que la publicité politique est interdite à la radio et à la télévision, et que les médias imprimés transmettent des annonces politiques sans interaction préalable avec des lecteurs individuels, les plateformes de données permettent de véhiculer des messages politiques de manière ciblée à des personnes ou groupes de personnes, qui peuvent alors commenter ou diffuser les contenus en question. Par les échanges de milliards d'utilisateurs dans le monde sur les principales plateformes, les opérateurs de réseaux mais aussi leurs clients accumulent

de grandes quantités de données d'adresses, de texte, sonores et visuelles, qui concernent leur famille, leurs amis et leurs connaissances, et peuvent fournir des indications sur leur vision du monde et leurs préférences politiques. 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 ainsi que le comportement électoral d'autres personnes. Comme les maîtres de fichiers professionnels, les différents destinataires assument également, en tant que particuliers, une responsabilité de traitement concernant les données personnelles qu'ils traitent dans le contexte politique (cf. tableau E). Et pour pouvoir assumer cette responsabilité, il faut avant toute chose qu'ils en aient conscience.

6 Principes de traitement généralement applicables

Chaque protagoniste traitant des données personnelles dans le contexte d'élections ou de votations doit respecter les principes généraux de traitement de la législation sur la protection des données:

Par «données personnelles», on entend ici l'ensemble des informations qui se rapportent à une personne identifiée ou identifiable. Les données qui fournissent des indications sur les opinions politiques ou philosophiques sont considérées comme sensibles, et leur traitement bénéficie d'une protection légale spéciale. Au travers de l'analyse ou de l'enrichissement de données, la mise en relation de données non sensibles en soi peut générer des données sensibles ou des profils de personnalité soumis à une protection légale spéciale, conformément à la jurisprudence du Tribunal administratif fédéral dans l'affaire Moneyhouse (chiff. 2).

Le traitement de données personnelles doit être effectué conformément au principe de bonne foi. Cela signifie que les données ne peuvent être collectées et traitées d'une manière que la personne concernée ne saurait supposer sur la base des circonstances et avec laquelle elle ne serait probablement pas d'accord. Autrement dit: la collecte et chaque traitement des données doivent être clairs pour la personne concernée. Cela s'applique également au but de chaque traitement de données, à l'identité du responsable du traitement et – en cas de transmission des données à des tiers – aux catégories de destinataires potentiels des données. De même, la collecte de données personnelles auprès de tiers tels que des commerçants de données doit être claire pour les personnes concernées.

En outre, le traitement doit respecter le principe de proportionnalité concernant la quantité des données personnelles traitées et leur durée de traitement. La proportionnalité signifie également qu'un responsable de traitement ne peut traiter que les données qui se révèlent appropriées et objectivement nécessaires pour atteindre un objectif (légitime). À cet égard, il doit exister une relation raisonnable entre l'objectif poursuivi et les moyens utilisés pour le traitement des données, et les droits des personnes concernées doivent être respectés. Le traitement de données doit être raisonnable pour les personnes concernées, tant dans sa finalité que dans les moyens utilisés.

Selon le principe de finalité, les données personnelles ne doivent être traitées que dans le but qui est indiqué lors de leur collecte, qui ressort des circonstances ou qui est prévu par la loi. Sans justification particulière, les données ne peuvent être traitées ultérieurement d'une manière non compatible avec le but initialement indiqué. Le principe de finalité s'applique également en cas d'intégration de services ou d'applications de tiers (par ex. services de newsletter ou logiciels pour la planification et la gestion de visites de porte à porte) ; les tiers ne sont pas autorisés à utiliser les données à leurs propres fins sans autre formalité (voir également chiffre 7).

Le maître d'un fichier doit également s'assurer de l'exactitude des données dans la mesure où elles se rapportent à des personnes. Le responsable du traitement doit prendre toutes les mesures qui s'imposent pour corriger ou détruire les données personnelles qui sont inexactes ou incomplètes au regard du but de leur collecte ou de leur traitement. Les données purement factuelles, sans lien avec des personnes identifiées ou identifiables, n'entrent pas dans le champ d'application du droit de la protection des données, ce qui signifie que la véracité des contenus politiques et la problématique des «fake news» ne sont pas l'objet du droit de la protection des données.

Enfin, le principe de sécurité des données exige que les données personnelles soient protégées contre les traitements non autorisés au moyen de mesures techniques et organisationnelles appropriées. Sont tenus de garantir la protection des données le maître du fichier, mais aussi chaque responsable de traitement, et ce, même si les données personnelles concernées ne représentent pas un fichier. L'obligation englobe ainsi chaque acteur traitant des données personnelles dans le contexte d'élections et/ou de votations. Il convient d'évaluer les risques organisationnels et techniques spécifiques en matière de droit de la protection des données et de prendre des mesures de protection appropriées. Cela suppose l'existence d'une documentation interne indiquant la manière dont ces obligations sont respectées pour les différentes catégories de données traitées.

7 Droit des électeurs à la transparence

Par ailleurs, tous les acteurs doivent prêter une attention particulière au principe de transparence. Celui-ci confère aux électeurs le droit de connaître les méthodes et technologies de traitement numérique par l'intermédiaire desquelles ils sont abordés et politiquement influencés.

Les **organes étatiques** qui mettent à disposition des données dans le contexte d'élections et de votations satisfont au droit à la transparence en matière de protection des données en accomplissant leur mission dans le cadre des bases légales.

Le traitement de données personnelles par des **acteurs privés** tels que partis et groupements d'intérêts peut également reposer sur le consentement des personnes concernées ou sur un intérêt privé ou public prépondérant. Dans la pratique, le traitement dans le contexte politique ne repose souvent que sur le consentement des personnes concernées, qui doit être donné de plein gré et après une information appropriée. Comme indiqué, les données personnelles sur les opinions politiques ou philosophiques qui sont traitées dans le contexte politique entrent généralement dans la catégorie des données personnelles sensibles. Des profils de personnalité peuvent être créés en reliant les données que les personnes concernées laissent par exemple sur des sites web ou des réseaux sociaux. En l'absence de justification légale ou d'intérêt public ou privé prépondérant, le traitement de profils de personnalité ou de données personnelles sensibles requiert le consentement explicite des personnes concernées. Dans le contexte politique, les données relatives à des personnes peuvent donc être traitées si ces dernières l'ont expressément approuvé, en toute indépendance et après avoir été suffisamment informées sur l'utilisation des données.

Les acteurs du processus de formation de l'opinion politique ne traitent des données qu'aux fins, dans la limite et avec les méthodes qui ont été approuvées. On considère qu'un consentement exprès a été donné si les personnes concernées se sont enregistrées sur le site web d'un acteur et se sont expressément déclarées d'accord (p. ex. en cochant une case correspondante) avec le traitement de leurs données sauvegardées. En revanche, les déclarations par lesquelles les personnes n'acceptent des conditions d'utilisation que de manière générale ne constituent pas des consentements explicites. Il en va de même des déclarations ressortant d'abonnements ou de commentaires liés aux contenus des acteurs, par exemple sur des réseaux sociaux. En outre, les consentements ne peuvent se rapporter

qu'aux propres données. Le traitement des données de tiers exige également le consentement de ceux-ci.

Le consentement est donné en toute indépendance si les personnes concernées peuvent approuver de manière différenciée l'activation ou la désactivation de certains aspects et fonctionnalités des applications numériques (p. ex. en cochant des cases correspondantes), et peuvent ainsi véritablement choisir si, mais aussi dans quelle mesure ils communiquent leurs données. En outre, les personnes concernées doivent pouvoir à tout moment révoquer leur consentement et demander la suppression de leurs données. Pour satisfaire ces exigences, les acteurs doivent investir dans des technologies favorables à la protection des données.

Un consentement éclairé suppose que les personnes intéressées ont obtenu, avant l'enregistrement, des informations justes et complètes sur le traitement de leurs données et le fonctionnement des méthodes d'analyse utilisées, y compris sur le recours à des programmes automatisés et à l'intelligence artificielle. Elles doivent également être informées de leurs droits, comme celui de révoquer à tout moment le consentement donné. Une information appropriée est une information claire, facile à trouver et formulée dans un langage compréhensible. Sont jugés complets les textes en ligne qui exposent les finalités et le fonctionnement des technologies et méthodes de traitement numériques avec un niveau de précision adapté à des destinataires multiples, et qui indiquent notamment la durée de traitement et l'éventuelle transmission de données à des tiers. La cascade des informations commence par une information brève, bien visible sur la page d'enregistrement, qui précise les points essentiels du traitement des données. Chacun de ces points contient des liens complémentaires qui guident le lecteur vers les passages pertinents des dispositions sur la protection des données et des règlements de traitement déterminants. Une information appropriée implique, en particulier dans le contexte politique, que les personnes concernées ne soient pas trompées par des informations erronées ou mensongères sur les expéditeurs et les sources ou, dans le cas de communications individuelles, puissent savoir avec certitude si elles interagissent avec des êtres humains ou avec un programme informatique. En outre, elles doivent pouvoir déterminer si l'envoi d'une information en ligne est personnalisé ou adressé à tout le monde. Le cas échéant, les conditions d'utilisation doivent permettre de connaître les technologies et critères qui déterminent les attributions personnalisées. Une information complète comprend également des indications sur le traitement de données qui sont analysées et enrichies au moyen d'informations issues des réseaux sociaux («social match»).

8 Résumé

A **Partis politiques et groupements d'intérêts**	Dans la mesure où les partis et groupements d'intérêts assument une responsabilité générale en qualité de ***maître de fichier*** (cf. chiff. 2), ils tiennent compte des remarques suivantes: • Le traitement a lieu de manière ***conforme au droit***, indépendamment de l'intervention de tiers et dans le respect des principes généraux de la LPD (chiff. 6). • Les ***tiers mandatés*** sont encouragés à démontrer qu'ils prennent les mesures organisationnelles et techniques appropriées pour la sécurité des données (chiff. 6). • Le droit des électeurs à la ***transparence*** (chiff. 7) est assuré par des **informations disponibles sur le site web** concernant: - l'identité du maître de fichier responsable; - les catégories de données traitées; - la collecte de données, avec renvoi vers les sources tierces; - la finalité effective et la justification du traitement; - les méthodes de traitement, y compris le but et le fonctionnement des méthodes d'analyses utilisées, en incluant l'intelligence artificielle; - les catégories de destinataires éventuels des données; - les rôles, obligations et responsabilités de fournisseurs de données, de sociétés d'analyse de données ou de plateformes de données; - les conditions d'utilisation déterminantes de tiers et leurs sources. • Le traitement est assuré dans le respect des principes de ***finalité*** (chiff. 6) et de ***proportionnalité*** (chiff. 6), selon lesquels tout traitement ultérieur respecte toujours le but sous-jacent à la collecte ainsi que la durée jusqu'à la réalisation de ce but; • Les ***consentements*** nécessaires pour le traitement de données personnelles dans le contexte du processus politique sont ***expressément*** obtenus (chiff. 7); • L'***exactitude des données*** est garantie même en cas de recours à des tiers et les données qui ne sont plus nécessaires sont supprimées (chiff. 6); • Une ***estimation des risques*** organisationnels et techniques relatifs à la protection des données est effectuée et des mesures de protection appropriées sont prises (chiff. 6); • Il existe une ***documentation*** interne indiquant comment la sécurité des différentes catégories de données traitées est garantie (chiff. 6); • En cas d'utilisation de ***services ou d'applications de tiers*** (par ex. services de newsletter ou planification et gestion de visites de porte à porte), les exigences légales concernant communication de données à des tiers et la transmission de données personnelles à l'étranger sont respectées (cf. notre feuillet thématique « La transmission de données à l'étranger en 24 questions » et les « Explications

	relatives à la communication de données personnelles à l'étranger »); • Le droit d'information des personnes concernées ainsi que les éventuelles obligations de déclaration de fichiers ou les devoirs d'annonce de transmission de données personnelles à l'étranger à l'égard des autorités chargées de la protection des données sont respectés.
B **Registres publics**	Pour exploiter des ***registres d'habitants et d'électeurs*** (chiff. 3), les autorités compétentes s'assurent que: • le traitement des données n'outrepasse pas les ***dispositions légales*** en termes de but, de contenu, d'étendue et de durée; • les données personnelles ne sont transmises que si une base légale l'autorise expressément ou si les données ont été préalablement rendues anonymes; • les personnes enregistrées disposent de ***possibilités de blocage*** si la transmission de leurs données à des fins de publicité politique n'est pas d'emblée exclue par la loi; • les ***risques*** en matière de sécurité technique et organisationnelle, y compris les procédures de réidentification, sont ***analysés et documentés***, et les mesures de protection nécessaires sont prises (chiff. 6); • les pertes de données sont notifiées en temps utile aux autorités compétentes en matière de protection des données.
C **Commerçants de données et sociétés d'analyse de données**	Dans la mesure où des commerçants de données (chiff. 5.1) ou des sociétés d'analyse de données (chiff. 5.2) traitent des données dans le contexte du processus politique en tant que ***maîtres de fichier*** assumant une responsabilité générale, ils tiennent compte des remarques établies au tableau A. Dans la mesure où ils interviennent en tant que ***responsables de traitement*** et traitent des données dans le contexte du processus politique: • ils s'assurent avant la conclusion du contrat que leur donneur d'ordre est disposé et en mesure, tant sur le plan technique qu'organisationnel, de réaliser le traitement à convenir conformément à la loi et au contrat; • ils respectent la jurisprudence du cas Moneyhouse (chiff. 2) concernant la formation de profils par la combinaison de données issues de différentes sources (chiff. 4.2); • ils garantissent la sécurité des données en estimant et en documentant les risques, et en prenant les mesures de protection nécessaires (chiff. 6); • ils notifient les éventuelles pertes de données à leur donneur d'ordre et le soutiennent, à sa demande, dans l'élimination des risques. Ils fournissent dans leurs conditions d'utilisation ou conditions contractuelles écrites des indications sur: • la manière, les sources, les méthodes et les finalités de la collecte des données transmises; • l'éventuel consentement par les personnes concernées de la transmission et du traitement ultérieur de leurs données, et le cas échéant, la finalité et la forme de cette transmission et de ce traitement.

D **Plateformes de données**	Que des plateformes de données (chiff. 5.3) traitent des informations dans le contexte du processus politique en tant que maîtres de fichiers assumant une responsabilité générale ou dans un rapport de sous-traitance, le traitement est généralement régi par les **conditions générales de vente et d'utilisation**. • Elles respectent le droit des électeurs à un ***traitement des données transparent*** (chiff. 7) et investissent donc régulièrement dans des ***technologies favorisant la protection des données*** afin d'offrir aux utilisateurs des ***informations*** *à plusieurs niveaux et de* ***vraies options numériques faciles à utiliser***. • Elles désignent, à l'intention des autorités compétentes en matière de protection des données, des ***personnes de contact*** dûment informés et autorisés qui sont disponibles pour fournir des renseignements en cas de pertes de données ou d'autres incidents relatifs à la protection des données avec des conséquences potentielles sur des élections ou votations. Dans la mesure où des plateformes de données traitent des informations en tant que ***maîtres de fichier*** assumant une responsabilité générale, elles tiennent également compte des remarques établies au tableau A. Dans la mesure où elles traitent des données dans un ***rapport de sous-traitance***, elles respectent également les remarques du tableau C.
E **Personnes individuelles**	Avant que des personnes individuelles publient, évaluent ou partagent des contenus et opinions politiques sur des réseaux sociaux, elles veillent à préserver la sphère privée et d'autres aspects relevant des droits de la personnalité, tels que l'honneur ou la vie familiale, de leurs destinataires. Avant de ***transmettre des informations*** à des partis, groupements d'intérêts, commerçants de données, sociétés d'analyse de données ou plateformes de données, concernant des amis, parents ou autres personnes identifiables, elles obtiennent ***le consentement explicite préalable*** de ces personnes. Elles s'assurent que les logiciels utilisant ces données proviennent de sources fiables.