Commission européenne

ÉTAT DE L'UNION
2018

Protéger les données personnelles des Européens en période électorale

#SOTEU

12 septembre 2018

«En mai prochain, je veux que les Européens soient en mesure de faire leurs choix politiques dans le cadre d'élections européennes régulières, sécurisées et transparentes. Dans notre monde connecté, le risque d'interférences et de manipulations n'a jamais été aussi grand. Afin de protéger la démocratie européenne, il est temps d'adapter nos règles électorales à l'ère numérique.»

Jean-Claude Juncker, 12 septembre 2018

Il est de plus en plus fréquent, en période électorale, que les partis politiques utilisent des données à caractère personnel pour cibler des citoyens sur les médias sociaux. Les révélations dans l'affaire Cambridge Analytica sont un exemple du risque que les technologies modernes peuvent constituer pour le processus électoral. La Commission a fourni aujourd'hui des orientations sur la manière dont les règles actuelles de l'Union devraient être utilisées pour parer à ce risque et garantir la régularité du processus électoral, notamment dans la perspective des élections au Parlement européen de 2019.

Le règlement général de l'Union sur la protection des données, entré en application en mai 2018, prévoit pour chaque acteur du processus électoral des règles claires à respecter pour satisfaire à la nouvelle réglementation en matière de protection des données.

Obligations incombant aux partis politiques et aux fondations

Les partis politiques et les fondations sont des responsables du traitement des données puisqu'ils décident de la finalité et des modalités du traitement des données à caractère personnel.

À faire :

- Choisissez la **base juridique appropriée** au traitement des données personnelles et tenez compte des conditions spécifiques applicables au traitement des données sensibles;
- Assurez-vous que les systèmes que vous utilisez sont **sécurisés** et, en cas de violation de données, informez-en sans tarder les personnes concernées;
- Lorsque vous commencez à traiter des données, y compris lorsque vous les collectez auprès de tiers, informez les personnes concernées;
- Assurez-vous que les données que vous traitez sont exactes, en particulier lorsque vous les collectez auprès de différentes sources;
- Si vous utilisez les services d'un **tiers**, par exemple d'une société d'analyse de données, vérifiez si les données qu'il vous a transmises ont été obtenues légalement..

À éviter :

- Si des personnes vous ont transmis des données personnelles pour une **finalité** autre que le contexte électoral en question, ne les traitez pas
- N'accordez pas de droits **d'accès** élargis aux données personnelles en votre possession. Vous devriez vérifier qui dans votre organisation a accès aux données et à quelles fins légitimes.

Sociétés d'analyse de données / Courtiers en données

Les sociétés d'analyse de données/courtiers en données sont, selon le degré de contrôle qu'ils exercent sur le traitement, soit des responsables du traitement, soit des sous-traitants. Une société d'analyse de données qui traite, par exemple, des données personnelles sur instruction d'un parti politique est un sous-traitant..

À faire :

- Choisissez la **base juridique appropriée** au traitement des données personnelles;

  Le texte ci-dessous s'applique uniquement dans les cas où la société d'analyse de données/le courtier en données est un responsable du traitement des données.

- Pour traiter des données **sensibles** concernant une personne (son origine ethnique, par exemple), vous devez avoir obtenu le consentement explicite de cette personne, ou appliquer d'autres exceptions prévues par le règlement général sur la protection des données;

  Assurez-vous que les systèmes que vous utilisez sont sécurisés et, en cas de violation de données, informez-en sans tarder les personnes concernées;

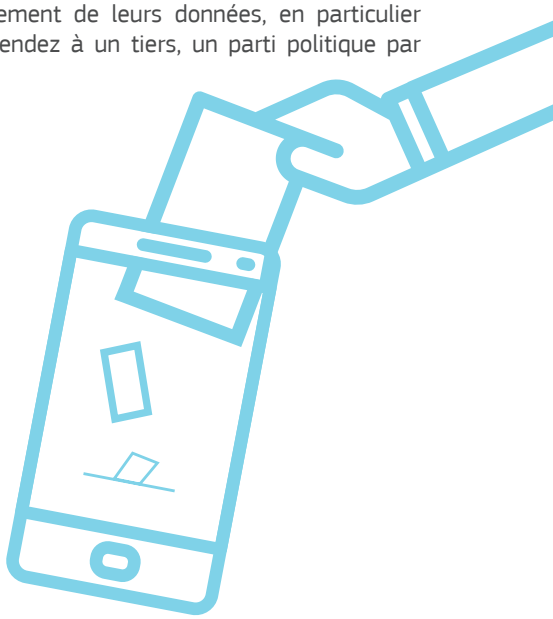
- Si vous combinez différents **ensembles de données** sur des personnes, veillez à le faire correctement et légalement;

  Le dernier point ne vaut que si la société d'analyse de données/le courtier en données est un sous-traitant.

- Si un **tiers** avec lequel vous travaillez, tel qu'un parti politique, a besoin de votre aide pour, par exemple, élaborer une analyse d'impact relative à la protection des données, apportez-lui votre soutien.

À éviter :

- Si des personnes vous ont transmis des données personnelles pour une **finalité** autre que le contexte électoral en question, ne les traitez pas;
- Vous devriez informer les personnes concernées de chaque finalité d'un traitement de leurs données, en particulier lorsque vous le vendez à un tiers, un parti politique par exemple.



Autorités électorales nationales

Les autorités électorales nationales sont des **responsables du traitement des données** étant donné qu'elles contrôlent les listes électorales.

À faire :

- Avant de commencer à traiter des données personnelles, effectuez une **analyse d'impact** relative à la protection des données afin d'évaluer les risques;
- La **base juridique** pour traiter des données personnelles permettra, de manière générale, de se conformer à une obligation légale ou d'exécuter une mission d'intérêt public fondée sur la législation.

Plates-formes de médias sociaux

Les plates-formes de médias sociaux sont des responsables du traitement des données étant donné que le traitement des données personnelles se fait sur leurs plates-formes.

À faire :

- Choisissez la **base juridique appropriée** au traitement des données personnelles;
- Pour traiter des données **sensibles** concernant une personne (son origine ethnique, par exemple), vous devez avoir obtenu le consentement explicite de cette personne, ou appliquer d'autres exceptions prévues par le règlement général sur la protection des données;
- Proposez aux utilisateurs différents **contrôles et réglages** pour qu'ils puissent effectivement exercer leurs droits, par exemple demander la correction ou la suppression de données les concernant;
- Assurez-vous que les systèmes que vous utilisez sont **sécurisés** et, en cas de violation de données, informez-en sans tarder les personnes concernées;

À éviter :

- Ne partagez pas les données avec un **tiers**, par exemple une société d'analyse de données, sauf si les utilisateurs vous ont donné leur consentement explicite.
- Si vous partagez les données de vos utilisateurs avec des tiers, précisez-le clairement dans les conditions générales de votre plate-forme.