



COMMISSION FOR PERSONAL
DATA PROTECTION

CONSEILS SUR LE TRAITEMENT ET LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL DANS LE CADRE DU PROCESSUS ÉLECTORAL

*Adoptées conjointement par la commission électorale centrale et la commission pour la protection des
données à caractère personnel sur la base de l'article 57, paragraphe 1 (49) du code électoral*

TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL DANS LE CADRE DU PROCESSUS ÉLECTORAL

I. GÉNÉRALITÉS

Depuis le 25 mai 2018, de nouvelles règles relatives à la protection des données à caractère personnel s'appliquent dans l'Union européenne. Le règlement (UE) 2016/679 (règlement général sur la protection des données) est l'acte juridique qui définit les exigences et les obligations de toutes les autorités publiques, des entreprises privées et des responsables du traitement des données relatives à la protection des données à caractère personnel lors de leur traitement.

Le règlement général tient compte du fait que, aux fins du processus électoral, y compris au cours des activités électorales, les partis politiques, les institutions compétentes et les autres organes recueillent et/ou ont accès à des données à caractère personnel, y compris sur les opinions politiques des citoyens, qui sont généralement considérées comme des données sensibles et bénéficient d'une protection accrue. Les agents électoraux, les représentants des partis et les observateurs, ainsi que les médias, ont accès aux données à caractère personnel relatives à leur rôle dans le processus électoral et peuvent les traiter. C'est la raison pour laquelle les présentes lignes directrices visent à fournir des orientations à tous les participants au processus électoral sur les règles juridiques applicables ainsi que sur leurs droits et obligations spécifiques en ce qui concerne le traitement des données à caractère personnel.

Le document se fonde sur les dispositions du règlement (UE) 2016/679, sur les lignes directrices de la Commission européenne relatives à l'application de la législation de l'Union en matière de protection des données dans le contexte des élections de 12.09.2018¹, ainsi que sur la pratique de la Commission pour la protection des données à caractère personnel (CPDP).

¹ Le document COM(2018) 638 final

1. Droit applicable

Le traitement des données à caractère personnel dans le cadre du processus électoral devrait être conforme à plusieurs actes juridiques:

Premièrement, **le règlement (UE) 2016/679 (ci-après le «règlement»)** est directement applicable et obligatoire dans tous ses éléments. Les mesures nécessaires à sa mise en œuvre sont mises en œuvre par **la loi sur la protection des données à caractère personnel**.

Le code électoral régit explicitement les droits et obligations de tous les participants au processus électoral — partis politiques, coalitions de partis, comités d'initiative, candidats, représentants, agents électoraux, observateurs, représentants des médias et commissions électorales dans les différents types d'élections.

Le traitement des données à caractère personnel dans le cadre du processus électoral est conforme aux règles du règlement (UE) 2016/679, compte tenu des spécificités du processus électoral et de la législation qui lui est applicable.

2. Les responsables du traitement, les sous-traitants et les personnes qui traitent des données à caractère personnel dans le cadre du processus électoral sur instruction du responsable du traitement.

Il est essentiel de définir le rôle de chacun des participants au processus électoral du point de vue du règlement général afin de bien comprendre et de respecter les exigences en matière de protection des données.

Conformément au règlement (UE) no2016/679, on entend par **«responsable du traitement des données à caractère personnel»** la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel. Le responsable du traitement, ainsi que les finalités et les moyens du traitement, peuvent être déterminés par le droit de l'Union ou par le droit de la République de Bulgarie (article 4, paragraphe 7, du règlement général), comme c'est le cas pour le traitement de données à caractère personnel dans le cadre du processus électoral.

La qualité du responsable est une conséquence directe du fait qu'une personne physique ou morale spécifique ou une autre structure (par exemple, comité d'initiative, association civique, etc.) traite des données personnelles à des fins réglementées par la loi (par exemple dans le cadre de la commission électorale, pour le à des fins de rapport financier, pour préparer une liste de donateurs en respectant les restrictions pour les particuliers, etc.). La qualité du responsable est également acquise si les sujets respectifs ont choisi de traiter des données personnelles à d'autres fins légales, qu'elles soient directement

liées aux élections (en exécution d'un contrat, traitement des données personnelles conformément au Code du travail, pour à des fins comptables ou mise en place de vidéosurveillance à des fins de sécurité, etc.).

Le règlement général impose un ensemble d'obligations au responsable du traitement. Il doit prendre les mesures techniques et organisationnelles appropriées en matière de sécurité des données, en tenant compte de la nature, de la portée, du contexte et des finalités du traitement, ainsi que des risques qui pèsent sur les droits et libertés des personnes concernées. **En outre, conformément au principe de responsabilité, le responsable du traitement devrait à tout moment être en mesure de démontrer qu'il respecte les exigences énoncées dans le règlement, c'est-à-dire de documenter le traitement des données à caractère personnel effectué par le responsable du traitement.**

Le règlement (UE) 2016/679 introduit également la notion de «**sous-traitant**». Selon la définition, un sous-traitant est toute personne physique ou morale, autorité publique, agence ou autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement (article 4, paragraphe 8, du règlement général).

La principale différence entre un responsable du traitement et un sous-traitant réside dans le fait que ce dernier agit non pas en toute indépendance, mais pour le compte du responsable du traitement. Leurs relations sont régies par un contrat ou un autre acte juridique (par exemple: l'accord instituant une coalition de partis), qui régit l'objet, la durée des opérations de traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les obligations et droits du responsable du traitement, y compris le contrôle du respect des exigences relatives au traitement des données à caractère personnel. Le règlement général introduit également des obligations spécifiques pour le sous-traitant qui ne se limitent pas à la seule sécurité des données. Par exemple, elle est uniquement tenue de traiter des données à caractère personnel sur des instructions documentaires (écrites ou autrement vérifiables) du responsable du traitement. Lorsqu'il est nécessaire d'associer un autre sous-traitant, celui-ci est soumis au consentement exprès écrit du responsable du traitement. En outre, dans un souci de clarté, le règlement prévoit expressément que si le sous-traitant commence à déterminer lui-même les finalités et les moyens du traitement, il devient automatiquement le seul responsable du traitement et est responsable. Contrairement à l'ancien régime, le règlement instaure une responsabilité solidaire pour les infractions au traitement des données à caractère personnel entre le responsable du traitement et le sous-traitant. Cela signifie que la personne dont les données à caractère personnel font l'objet d'un traitement illicite peut adresser sa demande à chacune d'entre elles de son choix.

La répartition des rôles et des responsabilités entre le responsable du traitement et le sous-traitant est évaluée au cas par cas. Il ne s'agit pas d'une formalité juridique et vise à garantir que le traitement des données à caractère personnel s'effectue conformément aux exigences du règlement et protège ainsi les droits des personnes concernées.

Compte tenu de ce qui précède, les principaux acteurs impliqués dans le processus électoral ont les rôles et responsabilités suivants en ce qui concerne le traitement des données à caractère personnel:

- **Les partis** — ils sont des acteurs clés du processus électoral. Les finalités et les moyens du traitement des données à caractère personnel par les partis politiques sont définis par la loi ou de manière indépendante par eux et ont donc le statut de **responsables du traitement des données**.

- **Coalitions**: la coalition de partis pourrait être un **responsable autonome du traitement des données à caractère personnel** dans les cas où elle persiste au fil du temps en tant qu'entité autonome et dispose de mécanismes de décision efficaces et solides en rapport avec le traitement des données à caractère personnel. Ces mécanismes devraient être définis par la conclusion d'un accord de coalition. Il peut établir qu'un ou plusieurs membres de la coalition traitent des données à caractère personnel aux fins de l'enregistrement de la coalition ou aux fins de la coalition en général. Dans ce dernier cas, la coalition, en tant que responsable du traitement des données, devrait exercer un contrôle interne sur les membres de la coalition, étant donné qu'il incombe à la coalition en tant qu'entité.

La répartition des rôles au sein d'une coalition varie au cours de la période précédant et après son enregistrement à la CEC:

- Entre la conclusion de l'accord de coalition et l'entrée en vigueur de la décision d'enregistrer la coalition, les parties à la coalition sont des **responsables conjoints** du traitement et partagent une responsabilité solidaire pour le traitement des données à caractère personnel au sens de l'article 26 du règlement général, même si l'accord de coalition en dispose autrement;

- Dès que la coalition est née, c'est-à-dire après l'entrée en vigueur de la décision de la CEC, elle est devenue un **administrateur autonome**.

En cas de disparition de la coalition dans l'ordre juridique ou de modification de sa forme originale (changement de nom, changement de membre, etc.), ses membres sont **conjointement responsables** du traitement au sens de l'article 26 du règlement général en ce qui concerne toutes les opérations de traitement de données à caractère personnel effectuées pendant la période d'existence, et même si l'accord de coalition en dispose autrement, étant donné que l'article 26 du règlement est obligatoire. Dans ce cas, la personne concernée peut exercer ses droits et le CPDP peut invoquer ses pouvoirs de sanction en vertu du règlement général contre l'une quelconque des parties à la coalition [article 26, paragraphe 3, du règlement (UE) 2016/679].

- **Commissions d'initiative** — Les commissions d'initiative désignent des candidats aux postes de députés, de président et de vice-président, de maires et de conseillers municipaux. Les comités directeurs prévus par le code électoral n'ont pas d'existence durable après la fin du type d'élection concerné. C'est

pourquoi le code électoral désigne **les membres du comité d'initiative comme responsables du traitement des données**.

Chaque membre du comité d'initiative qui signe la liste des données à caractère personnel des électeurs et qui est personnellement responsable du traitement et de la conservation des données, y compris lorsqu'il ne recueille pas les signatures en personne mais par l'intermédiaire de tiers.

La responsabilité du traitement des données de la liste incombe au comité d'initiative et à ses membres également après la transmission des listes à la CEC.

Dans toutes les autres actions, autres que les listes d'enregistrement, les membres du comité d'initiative ont le statut des **responsables conjoints** au sens de l'article 26 du règlement général, y compris lorsqu'ils travaillent avec des agences sociologiques, des médias sociaux, des agents électoraux, etc. Cela reste valable après la cessation d'existence du comité d'initiative, y compris lorsque son enregistrement au titre de l'article 155 du code électoral a été annulé. En cas de plainte ou de signalement, les personnes physiques qui en sont membres continuent d'être traitées comme des responsables conjoints du traitement.

- **Commissions électorales** — la commission électorale centrale (CEC), les commissions électorales des districts (CED), les commissions électorales sectionnelles (CES) à l'intérieur et à l'extérieur du pays et, dans le cas des élections locales, les commissions électorales municipales (CEM), sont des responsables indépendants du traitement des données à caractère personnel définis par la législation nationale.

- **Les entités privées** – au processus électoral participent sous une forme ou une autre et les entités privées – médias, agences sociologiques, agences de publicité, médias sociaux et autres. Compte tenu de leur rôle spécifique et de leurs relations juridiques avec les autres participants et du processus électoral, ils pourraient être des **responsables indépendants de données à caractère personnel** (par exemple, les médias imprimés ou électroniques couvrant la campagne électorale) ou des **sous-traitants de données à caractère personnel** (par exemple, Les services d'information AD en tant que sous-traitants). données de vote, sociétés de publicité qui traitent des données personnelles pour le compte d'un parti politique et sur son ordre documenté aux fins de la campagne électorale; agences sociologiques menant des sondages ciblés sur la base de données personnelles précédemment fournies par l'entité politique, etc.).

- **Les autres organismes publics** ayant des missions et des pouvoirs au titre du code électoral sont les organismes locaux autonomes, les autorités exécutives (Ministère de l'Intérieur, Ministère du développement régional et des travaux publics, etc.), d'autres institutions (ministère des affaires étrangères, représentations diplomatiques et consulaires, respectivement; Ministère de la justice, prisons et centres de détention, etc.). En règle générale, ils sont également des **responsables indépendants du**

traitement des données à caractère personnel, lorsque les finalités et les moyens du traitement dans le cadre du processus électoral sont déterminés par la loi de la République de Bulgarie.

■ **Les agents électoraux, les observateurs et les représentants des fonds politiques, des coalitions et des comités d'initiative.** Ces acteurs du processus électoral traitent des données à caractère personnel sur la base de l'article 29 du règlement général, c'est-à-dire agissent sous l'autorité des responsables du traitement susmentionnés et ont accès aux données à caractère personnel. Ils n'ont pas le statut de responsables du traitement ou de sous-traitants. Leurs droits et obligations en matière de traitement des données à caractère personnel sont limités dans la mesure où leurs droits et obligations dans le cadre du processus électoral sont exhaustifs et limités. Les cas dans lesquels ces entités traitent des données à caractère personnel sont explicitement définis dans la commission électorale (droit à la visibilité directe lors de l'établissement des résultats des votes, droit de recevoir une copie du compte rendu sectoriel, etc.). Lors du traitement de données à caractère personnel, ces entités ne peuvent aller au-delà des droits et obligations prévus dans la commission électorale.

■ **Médias de masse** Elles traitent des données à caractère personnel de manière licite aux fins de la mise en œuvre de la liberté d'expression et du droit à l'information tout en respectant la vie privée (article 25 h, paragraphe 1, de la Loi sur la protection des données personnelles). Les médias en tant que médias de masse sont des administrateurs au sens du règlement général. Les journalistes et les opérateurs qui sont employés des médias agissent sur instruction du responsable du traitement au sens de l'article 29 du règlement général et ne sont pas seuls responsables en tant que responsables du traitement ou sous-traitants de données à caractère personnel. Dans les cas où ces journalistes, opérateurs vidéo ou photographes sont indépendants et déterminent eux-mêmes les finalités et les moyens du traitement des données à caractère personnel (sans agir pour le compte et sur instruction d'un responsable du traitement des données), ils deviennent responsables du traitement ou sous-traitant, avec les obligations et responsabilités qui en découlent. Ces entités ne traitent des données à caractère personnel qu'aux fins de l'exercice de leurs droits lors de l'ouverture du jour des élections (article 230, paragraphe 1, du code électoral) et lors de l'ouverture des boîtes électorales (article 272 du code électoral). Compte tenu de leur finalité consistant à fournir des informations conformément au principe de la liberté d'expression, les médias traitent des données à caractère personnel, y compris des enregistrements vidéo, tout en respectant la vie privée des personnes et le secret des votes.

II. INSTRUCTIONS AUX RESPONSABLES DU TRAITEMENT

1. Absence d'obligation d'enregistrement auprès du CPDP

Depuis le 25 mai 2018, date à laquelle le règlement (UE) 2016/679 est devenu applicable, l'obligation pour tous les responsables du traitement de s'enregistrer auprès du CPDP a cessé

d'exister. Elle a été remplacée par l'obligation de respecter le principe de responsabilité, y compris en établissant et en tenant à jour une documentation interne, en particulier un registre des activités de traitement des données à caractère personnel au titre de l'article 30 du règlement général.

2. Principes du traitement des données à caractère personnel

Tous les participants au processus électoral, qu'il s'agisse d'autorités publiques ou d'entités juridiques privées, sont tenus de traiter des données à caractère personnel conformément aux principes énoncés à l'article 5 du règlement (UE) 2016/679:

- Légalité, équité et transparence;
- Limitation de la finalité — les données collectées ne sont traitées qu'aux fins pour lesquelles elles ont été collectées (par exemple, les données à caractère personnel collectées aux fins de la conclusion d'un contrat de travail ou d'un contrat civil ou de la fourniture de biens et de services ne peuvent pas être utilisées aux fins de l'inscription ou de la liste électorale);
- Minimisation des données — l'objectif doit être atteint avec le minimum de données à caractère personnel nécessaire à cet effet (par exemple, les données à caractère personnel collectées aux fins de l'enregistrement dans la CEC ne peuvent pas dépasser celles spécifiées dans la commission électorale);
- Limitation de la durée de conservation — les données ne peuvent être traitées une fois que le motif de leur traitement a cessé d'exister;
- Exactitude, intégrité et confidentialité (par exemple, pour s'assurer que les données correctes sont traitées, les dernières modifications et ajouts à la commission électorale prévoient la vérification de l'identité du signataire de la liste d'enregistrement);
- Obligation de rendre compte — documenter clairement les mesures prises en matière de traitement des données.

3. Fondement juridique du traitement des données à caractère personnel

Le traitement de données à caractère personnel par les responsables du traitement tant dans le domaine public que privé n'est licite que s'il existe l'un des motifs juridiques énumérés de manière exhaustive à l'article 6, paragraphe 1, du règlement (UE) 2016/679:

- consentement;
- la conclusion ou l'exécution d'un contrat;
- une obligation légale pour le responsable du traitement;
- le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique;

- l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement;

- intérêts légitimes du responsable du traitement ou d'un tiers lorsqu'ils prévalent sur les intérêts ou les libertés et droits fondamentaux de la personne concernée (*non applicable aux autorités publiques*).

Il est important de garder à l'esprit **que lorsque des données à caractère personnel sont collectées ou traitées d'une autre manière en vertu d'un acte juridique, tel que le code électoral, il n'y a pas lieu d'exiger le consentement des personnes concernées**. Ces hypothèses incluent l'établissement, la publication et la publication de la liste électorale, la vérification de l'identité de l'électeur par le CEC et l'enregistrement de son vote, etc.

Il existe également **des cas où le consentement est la raison principale ou unique possible pour le traitement de données à caractère personnel**, par exemple lors de la **collecte de signatures à l'appui de l'enregistrement d'une entité politique** dans le type de choix pertinent, de la réalisation d'enquêtes sociologiques ou de l'envoi de courriels personnels par une entité politique ou une entreprise qu'elle recrute par courrier électronique, par téléphone, par SMS ou par télécopie à des fins électorales. Lorsque le consentement est utilisé comme base juridique, le règlement général exige qu'il soit donné au moyen d'un acte positif clair et qu'il soit donné et informé librement. En tout état de cause, la possibilité pour le participant de retirer son consentement à tout moment devrait être clairement indiquée. L'absence d'une telle possibilité constitue une violation des règles relatives au traitement des données à caractère personnel. Dans le même temps, en vertu du règlement général, le retrait du consentement n'a qu'un effet prospectif et n'affecte pas la licéité du traitement antérieur.

4. Traitement des données à caractère personnel sensibles

Certaines catégories de données à caractère personnel sont, par nature, particulièrement sensibles du point de vue des libertés et droits fondamentaux des personnes et sont spécifiquement protégées. Il s'agit notamment **des avis politiques** [article 9, paragraphe 1, du règlement (UE) 2016/679]. Leur traitement n'est autorisé que si l'une des conditions énoncées à l'article 9, paragraphe 2, du règlement général est remplie.

Conformément à l'article 9, paragraphe 2, point d), du règlement (UE) 2016/679, les partis politiques peuvent traiter ces données sensibles sous réserve de garanties appropriées et si toutes les conditions suivantes sont remplies:

- le traitement porte uniquement sur les membres ou anciens membres du parti ou sur des personnes qui ont des contacts réguliers avec elle en rapport avec l'activité et les finalités, et
- les données à caractère personnel ne sont pas divulguées à des tiers sans le consentement des personnes concernées.

Toutefois, cette disposition ne peut être utilisée par un parti politique pour traiter les données de membres potentiels, de sympathisants ou d'électeurs, étant donné qu'il n'existe en l'espèce aucun lien clair et permanent avec l'entité politique. Dans de tels cas, il devrait exister une autre base juridique valable, comme le consentement explicite de la personne concernée.

Dans le contexte des élections, la principale base juridique du traitement des données sensibles est l'existence d'un intérêt public important, sur la base du droit de l'Union ou du droit de la République de Bulgarie (Constitution, code électoral), qui est proportionné à l'objectif poursuivi, respecte l'essence du droit à la protection des données et prévoit des mesures appropriées et spécifiques pour protéger les droits fondamentaux et les intérêts de la personne concernée (article 9, paragraphe 1. 2 g) du règlement (UE) 2016/679).

D'autres raisons possibles sont que la personne a donné son consentement explicite ou a rendu les données publiques (article 9, paragraphe 1). 2, «a» et «e» du règlement (UE) 2016/679).

5. Délais de conservation des données à caractère personnel

Conformément au principe général de «limitation de la conservation» énoncé à l'article 5, paragraphe 1, point e), du règlement général, les données à caractère personnel ne devraient pas être conservées plus longtemps que nécessaire pour atteindre les finalités pour lesquelles elles sont traitées et devraient ensuite être effacées.

En règle générale, les délais de conservation des données à caractère personnel collectées aux fins des élections ou du référendum concernés sont fixés dans le code électoral (par exemple, les articles 135 et 142 du code électoral) et tous les responsables du traitement des données participant au processus électoral sont tenus de les respecter.

Dans certains cas, les données peuvent également être conservées pour une durée plus longue lorsque cela est justifié par un intérêt public ou un intérêt légitime du responsable du traitement qui prime les intérêts de la personne concernée. Les hypothèses suivantes sont similaires:

- la constatation, l'exercice ou la défense de droits en justice — par exemple, légitimes et proportionnés — il appartiendrait au responsable du traitement concerné participant au processus électoral de conserver les données à caractère personnel lors de l'introduction d'une réclamation dans l'attente de l'issue de la procédure administrative ou judiciaire pertinente;
- à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, en fournissant des garanties suffisantes pour protéger les droits des personnes concernées, par exemple par l'anonymisation des données (par exemple, la production de statistiques internes des partis sur les résultats des élections par circonscription électorale);

- afin d'exercer le droit à la liberté d'expression et le droit à l'information, les médias couvrant le processus électoral peuvent, en principe, bénéficier de ce motif de préservation.

6. Sécurité des données

La sécurité revêt une importance particulière dans le contexte électoral, compte tenu du grand nombre de données à caractère personnel traitées et de leur caractère sensible. Le règlement général exige à la fois des responsables du traitement et des sous-traitants qu'ils mettent en œuvre des mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté aux risques que le traitement présente pour les droits et libertés des personnes physiques.

Le règlement introduit l'obligation pour les responsables du traitement de notifier les violations de données à caractère personnel au CPDP dans un délai de 72 heures. Lorsque la violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement doit également prendre des mesures pour informer les personnes concernées par la violation.

7. Conscience des personnes concernées

Les principes de traitement loyal et transparent exigent que les personnes physiques soient informées de l'existence de traitements portant sur leurs données à caractère personnel et de leurs finalités. Le règlement général clarifie les obligations des responsables du traitement à cet égard. Ils doivent informer les personnes concernées des principaux aspects liés au traitement de leurs données à caractère personnel, tels que:

- identification du responsable du traitement — nom et moyens de contact;
- quelles catégories de données à caractère personnel sont traitées (uniquement si les données ne sont pas collectées directement auprès de la personne concernée);
- à quelles fins elles sont traitées (telles que déterminées par la commission électorale ou par le responsable du traitement lui-même);
- les catégories de destinataires des données à caractère personnel (CEC, CED, CEM, CES, Cour des comptes, administration régionale, etc.);
- la durée de conservation des données;
- l'existence de droits spécifiques des personnes concernées (droit d'accès, de rectification ou d'effacement des données à caractère personnel, limitation du traitement ou objection au traitement) et les modalités de leur exercice;

- le droit des personnes concernées d'introduire une réclamation auprès du CPDP ou du tribunal;
- si la fourniture de données à caractère personnel est obligatoire en vertu de la loi ou par contrat, et les conséquences éventuelles de la non-communication de ces données;
- (le cas échéant) s'il existe une prise de décision automatisée, y compris le profilage.
- toute autre information nécessaire pour assurer un traitement équitable et transparent.

En outre, le règlement général sur la protection des données exige que les informations soient fournies sous une forme concise, transparente, intelligible et facilement accessible, dans un langage clair et compréhensible. Les informations doivent être fournies aux personnes à chaque étape du traitement et pas uniquement lors de la collecte des données.

Le règlement général prévoit également des exceptions à l'obligation d'information, en particulier lorsque:

- la personne concernée dispose déjà de ces informations;
- la fourniture de ces informations est impossible ou nécessite des efforts disproportionnés (par exemple, la fourniture d'informations nouvelles ou supplémentaires aux signataires de la liste d'enregistrement);
- l'obtention ou la divulgation de données à caractère personnel est expressément autorisée par le droit de l'UE ou le droit bulgare (par exemple, publication de la liste électorale, communication de données au CPDP ou au tribunal compétent, etc.).

8. Droits des personnes concernées

Le règlement (UE) 2016/679 accorde aux personnes des droits supplémentaires et renforcés, y compris, dans le cadre des élections, particulièrement pertinents:

- le droit d'accès à ses propres données à caractère personnel traitées par le responsable du traitement ou le sous-traitant;
- le droit de demander l'effacement de leurs données à caractère personnel si le traitement est fondé sur le consentement et si le consentement est retiré si les données ne sont plus nécessaires ou si le traitement est illicite. Le retrait du consentement produit des effets à l'avenir, de sorte que le traitement avant cette date reste licite;
- droit de rectification des données à caractère personnel inexacts, inexacts ou incomplètes;
- le droit de s'opposer à une forme particulière de traitement par une entité politique (par exemple, les données collectées dans la liste d'inscription sont traitées à d'autres fins, telles que la campagne électorale);

- le droit de former un recours devant le CPDP ou directement devant la juridiction compétente.

Toutefois, il convient de garder à l'esprit que les droits des personnes concernées ne sont pas absolus et devraient être mis en relation et mis en balance avec les droits des autres personnes concernées ainsi qu'avec l'intérêt public, le cas échéant. Par exemple, le responsable du traitement pourrait refuser une demande d'effacement (droit à l'oubli) si les données à caractère personnel sont nécessaires:

- pour le respect d'une obligation légale prévue par le droit de l'Union ou par la législation de la République de Bulgarie (par exemple, le code électoral) ou pour l'exécution d'une mission d'intérêt public ou relevant de l'exercice de pouvoirs publics dont est investi l'administrateur (CEC, CED, administration municipale et régionale, ministère de l'intérieur, ministère de l'intérieur, ministère des affaires étrangères, etc.);

- pour la constatation, l'exercice ou la défense d'actions en justice (par exemple, pour défendre l'administrateur en cas de plainte contre lui devant le CPDP ou devant un tribunal);

- pour l'exercice du droit à la liberté d'expression et du droit à l'information (médias, etc.).

La CEC et tous les responsables du traitement des données impliqués dans le processus électoral doivent informer les personnes concernées/électeurs de la manière dont ils peuvent exercer les droits décrits ci-dessus.

9. Traitement de données à caractère personnel par enregistrement vidéo et/ou diffusion (enregistrement et/ou transmission en direct)

Les médias traitent les données à caractère personnel par filmage et/ou diffusion vidéo uniquement dans les cas visés aux articles 230, 232 et 272 du code électoral (ouverture du jour d'élection, clôture du jour d'élection et établissement des résultats des votes) et tirage au sort pour déterminer les numéros séquentiels des bulletins de vote. Le tournage vidéo/diffusion est effectué après l'élection, sous réserve des instructions du président du CES et d'une manière qui n'interfère pas avec le vote et l'établissement des résultats des élections.

Le traitement de données à caractère personnel dans le cadre du processus électoral par filmage et/ou diffusion vidéo a pour but de garantir la transparence, l'objectivité, la licéité du processus électoral, l'égalité de traitement des personnes qui y sont soumises, ainsi que la liberté d'expression et le droit à l'information.

Lorsqu'ils traitent des données à caractère personnel dans le cadre du processus électoral, les médias de masse, les photographes, les journalistes et les opérateurs de vidéo indépendants respectent les règles et principes du règlement (UE) 2016/679 et de la Loi sur la protection des données personnelles et assument la responsabilité qui y est prévue.

Tous les autres participants au processus électoral ne peuvent traiter des données à caractère personnel par filmage et/ou diffusion vidéo en raison de l'incompatibilité de leur rôle dans le processus électoral avec la finalité du traitement de données à caractère personnel par filmage vidéo dans le cadre du processus électoral. Les fonctions et rôles de ces acteurs dans le processus électoral sont explicitement et plafonnés dans la commission électorale.

10. Sanctions en cas d'infraction aux règles en matière de protection des données

10.1. Sanctions au niveau national

Le règlement (UE) 2016/679 prévoit des sanctions administratives très élevées pour les **infractions aux règles en matière de protection des données à caractère personnel**, d'un montant maximal de 20 millions d'EUR. Il est important de savoir qu'avant d'infliger une «amende» à un responsable du traitement ou à un sous-traitant, à une personne physique ou à une «amende» infligée à un responsable du traitement ou à un sous-traitant, le CPDP évalue un certain nombre de facteurs et de circonstances, notamment:

- la nature, la gravité et la durée de l'infraction, compte tenu de la portée et de la finalité du traitement concerné, ainsi que du nombre de personnes concernées et du degré de préjudice qui leur est causé;
- du fait que la violation a été commise délibérément ou par négligence;
- toute mesure prise par le responsable du traitement ou le sous-traitant pour atténuer le dommage subi par les personnes concernées;
- le degré de responsabilité du responsable du traitement ou du sous-traitant, compte tenu des mesures techniques et organisationnelles prises par le responsable du traitement ou le sous-traitant;
- violation antérieure commise par le responsable du traitement ou le sous-traitant;
- le degré de coopération établi avec CPDP en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs;
- la manière dont l'autorité de contrôle a eu connaissance de la violation, notamment si, le responsable du traitement ou le sous-traitant a notifié la violation à lui-même;
- d'autres circonstances aggravantes ou atténuantes applicables au cas d'espèce.

10.2. Sanctions au niveau de l'UE

Le règlement n° 1141/2014 du Parlement européen et du Conseil du 22 octobre 2014 relatif au statut et au financement des partis politiques européens et des fondations politiques européennes

visé à renforcer la visibilité, la reconnaissance, l'efficacité et la transparence des partis politiques européens et des fondations politiques qui leur sont affiliées, ainsi que l'obligation qui leur est faite de rendre des comptes. Il institue au niveau de l'UE une **Autorité indépendante pour les partis politiques européens et les fondations politiques européennes**, chargée d'enregistrer, de surveiller et, le cas échéant, de sanctionner les partis politiques européens et les fondations politiques européennes.

III. ORIENTATIONS COMPLÉMENTAIRES DE LA COMMISSION EUROPÉENNE

En septembre 2018, la Commission européenne a publié ses **lignes directrices sur l'application de la législation de l'Union en matière de protection des données dans le contexte des élections**, qui définissent certaines obligations supplémentaires pour les partis politiques et les autres participants au processus électoral. Ces nouveaux engagements découlent du règlement général sur la protection des données ainsi que des risques liés à l'utilisation des nouvelles technologies.

1. Utilisation du profilage, de la prise de décision automatique et des réseaux sociaux

Selon le règlement général, le «profilage» est une forme de traitement automatisé de données relatives à une personne physique qui est utilisée pour analyser et prédire certains aspects personnels de la personne, tels que les préférences personnelles, les intérêts, la situation économique, le comportement, etc. (article 4, paragraphe 4, du règlement général).

Par «décision automatisée» au sens du règlement général, on entend l'adoption, par un responsable du traitement, d'une décision fondée uniquement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques à l'égard de la personne concernée ou l'affectant de manière significative de manière similaire (article 22 du règlement général).

Le développement dynamique des technologies et l'utilisation croissante de différents algorithmes, y compris l'intelligence artificielle, créent des possibilités d'intrusion sans précédent dans la vie privée et la vie privée des individus. Le cas de Cambridge Analytica et Facebook a révélé les défis particuliers liés aux méthodes de microciblage sur les réseaux sociaux. Les organisations tant commerciales que politiques peuvent effectuer une analyse intelligente des données collectées par les utilisateurs des médias sociaux afin de créer des profils électoraux. Cela permettrait à ces organisations d'identifier les électeurs qui peuvent être plus facilement influencés et, partant, d'influencer les résultats des élections.

En principe, le règlement (UE) 2016/679 n'interdit pas le recours au profilage et à la prise de décision automatisée, mais compte tenu du niveau élevé de risque que présentent ces formes de traitement pour les droits et libertés des personnes physiques, il existe des exigences et des obligations spécifiques accrues pour les responsables du traitement, ainsi que des droits spécifiques des personnes concernées.

La prise de décision automatisée et le profilage fondés sur des catégories particulières de données à caractère personnel, y compris les opinions politiques, sont soumis à des conditions encore plus strictes, à savoir l'existence d'un consentement explicite de la personne concernée ou d'un intérêt public important sur la base du droit de l'Union ou du droit bulgare, qui est proportionné à l'objectif poursuivi.

Compte tenu de l'absence de réglementation légale de ces formes de traitement des données à caractère personnel dans la législation électorale et de garanties appropriées et efficaces pour les droits et libertés des personnes physiques, le recours éventuel au profilage et à la prise de décision automatique dans le cadre du processus électoral en République de Bulgarie constituerait un traitement hautement risqué des données à caractère personnel et, en cas de non-respect des conditions accrues de traitement des données à caractère personnel, serait contraire aux règles relatives au traitement des données.

2. Analyse d'impact relative à la protection des données

Le règlement (UE) 2016/679 introduit une nouvelle obligation pour les responsables du traitement, y compris ceux qui participent au processus électoral, **une analyse d'impact sur la protection des données à caractère personnel** de certaines opérations de traitement. Une telle évaluation doit être effectuée lorsqu'un type de traitement est susceptible, compte tenu de sa nature, de sa portée, de son contexte et de ses finalités, d'engendrer un **risque élevé** pour les droits et libertés des personnes physiques [article 35, paragraphe 1, du règlement (UE) 2016/679].

Les orientations de la Commission européenne sur l'application de la législation de l'Union en matière de protection des données dans le contexte électoral imposent à tous les partis politiques et autres acteurs électoraux de procéder à une telle analyse d'impact sur la protection des données.

L'analyse d'impact doit contenir au moins les éléments suivants:

- une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement;
- une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités;
- une évaluation des risques pour les droits et libertés des personnes concernées; et
- les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées.

Le règlement général part du principe que l'une des situations dans lesquelles un tel risque existe est le traitement à grande échelle de catégories particulières de données, y compris de croyances politiques.

Une exception à l'obligation d'effectuer une analyse d'impact est autorisée si le traitement est effectué en vertu d'une obligation légale ou pour l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement, et qu'une telle analyse a déjà été effectuée dans le cadre de l'analyse d'impact générale dans le cadre de l'adoption de l'acte juridique pertinent [article 35, paragraphe 10, du règlement (UE) 2016/679]. À cet égard, on peut supposer que la **CEC et d'autres commissions électorales, ainsi que d'autres organismes publics ayant des obligations électorales spécifiques, relèvent de l'exception et ne sont pas tenus de procéder à une analyse d'impact sur la protection des données à caractère personnel.** Les autres participants au processus électoral, y compris les partis, ne sont pas exemptés de cette obligation.

3. Marketing direct et communications commerciales non sollicitées

Contrairement aux élections précédentes, le règlement général traite l'envoi de courriels *personnels* par courrier électronique, téléphone, SMS ou télécopie comme un marketing direct. La Commission européenne prévoit des exigences renforcées pour ce type de traitement des données à caractère personnel et les assimile aux «communications commerciales non sollicitées» au sens de l'article 6 de **la loi sur le commerce électronique** et de l'article 261 de **la loi sur les communications électroniques**. Le consentement préalable de la personne est requis pour ce type de communication, y compris dans les cas où ils sont envoyés à des fins électorales conformément à l'article 181 du code électoral. Les partis politiques doivent respecter les règles générales en matière de marketing direct et de communications commerciales non sollicitées et offrir une possibilité simple et efficace de refuser de recevoir ces communications ou de retirer leur consentement, soit en envoyant un courriel, au moyen d'un message court, en utilisant un «lien» vers un site web, soit par tout autre moyen approprié.