GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES

17/FR

WP 258

Avis sur certaines questions clés de la directive (UE) 2016/680 (directive «police»)

Adopté le 29 novembre 2017

Ce groupe de travail a été institué par l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2002/58/CE.

Le secrétariat est assuré par la direction C (Droits fondamentaux et État de droit) de la direction générale de la justice et des consommateurs de la Commission européenne, B-1049 Bruxelles, Belgique, bureau MO-59 03/78

Site web: http://ec.europa.eu/justice/data-protection/index_en.htm

Introduction

La nouvelle directive (UE) 2016/680 (directive «police») vient compléter le nouveau règlement (UE) 2016/679 (règlement général sur la protection des données – RGPD).

Cette directive doit être transposée le 6 mai 2018 au plus tard et supervise: le traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données. Avec l'entrée en vigueur de la directive, la décision-cadre 2008/977/JAI du Conseil (décision-cadre relative à la protection des données) que les États membres devaient appliquer le 27 novembre 2010 au plus tard sera abrogée. La décision porte sur les domaines de la coopération judiciaire en matière pénale et de la coopération policière, mais contrairement à la directive, elle se limite au traitement des données à caractère personnel transmises ou mises à disposition entre les États membres et au traitement ultérieur de ces données en ce qui concerne également les transferts aux autorités compétentes des pays tiers.

Afin de proposer une compréhension et une approche cohérentes et compte tenu des différents stades de mise en œuvre et des discussions au sein des États membres, le GT29 a décidé de mettre l'accent dans son document d'orientation sur certaines questions clés, lorsque des orientations pratiques sont nécessaires, lorsque ces questions clés concernent directement les travaux des autorités de protection des données ou lorsque la mise en œuvre dans un ou plusieurs États membres laisse à penser que la transposition pourrait ne pas respecter pleinement les principes de la directive.

Selon cette approche, le GT29 souhaite fournir des orientations sous la forme de recommandations et de remarques sur les articles suivants:
Article 5 – Délais de conservation et d'examen
Article 10 – Traitement portant sur des catégories particulières de données à caractère personnel
Article 11 – Décision individuelle automatisée et profilage
Article 13-17 – Droits de la personne concernée
Article 25 – Journalisation
Article 47 – Pouvoirs des autorités de protection des données.

Dans le même temps, le GT29 souhaite souligner qu'il ne s'agit pas d'une liste exhaustive et que de nouvelles orientations pourraient être données à l'avenir si nécessaire.

Article 5
Délais de conservation et d'examen

Sujets clés
1. Délais de conservation maximaux et examens périodiques
2. Calendriers distincts
3. Protection des données dès la conception

1. Délais de conservation maximaux et examens périodiques

Lorsque le traitement des données à caractère personnel relevant du champ d'application de la directive «police» est effectué selon le droit des États membres, il convient de préciser – avec les objectifs et les données à caractère personnel qui feront l'objet d'un traitement ainsi que les finalités du traitement[1] – les délais prévus pour chaque type de traitement.

L'article 5 de la directive «police» laisse les législateurs nationaux libres de fixer des délais appropriés pour l'effacement des données à caractère personnel ou pour la vérification régulière de la nécessité de conserver les données à caractère personnel. Dans tous les cas, des règles procédurales garantissent le respect de ces délais.

Le GT29 considère que cette formulation prévoit la possibilité de mettre en place une sorte de système mixte permettant de combiner des délais maximaux généraux à la vérification régulière de la nécessité de conserver pour une nouvelle durée les données sous une forme permettant l'identification ou l'identifiabilité de la personne concernée. Il s'agit du meilleur moyen de garantir le plein respect des principes relatifs au traitement des données à caractère personnel définis à l'article 4 de la directive «police» selon lequel les données à caractère personnel devraient être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées; les données à caractère personnel doivent également être exactes et, si nécessaire, tenues à jour et conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées.

À cet égard, en principe, les données à caractère personnel ne devraient être traitées que si elles servent la finalité pour laquelle elles sont collectées et, lorsqu'elles ne sont plus nécessaires au regard de cette finalité, elles devraient être effacées, sauf si un traitement ultérieur est prévu par la loi et considéré comme pertinent au regard d'une finalité qui n'est pas incompatible avec la finalité originale du traitement[2]. Sinon, la

[1] Voir le considérant 33 et l'article 8, paragraphe 2, de la directive «police».
[2] À cet égard, voir l'article 4, paragraphe 3, de la directive «police» qui précise que «le traitement des données par le même ou par un autre responsable du traitement peut comprendre l'archivage dans l'intérêt public, à des

directive et le RGPD autorisent la conservation des données sous une forme qui ne permet pas d'identifier les personnes concernées. Les deux options devraient être envisagées.

La question de savoir si certaines données ont atteint leur finalité et ne sont plus nécessaires se pose notamment lorsque la conservation des données est autorisée à des fins préventives. Il est inhérent à de telles finalités que la conservation puisse uniquement reposer sur une évaluation des risques concernant une certaine personne concernée. Dans ces cas, il n'existe pas de moment de clôture, contrairement à une enquête pénale, qui implique automatiquement la décision d'effacer les données à caractère personnel collectées durant l'enquête. Toutefois, le principe de nécessité requiert de vérifier le pronostic après un délai adéquat. La décision de conserver les données pour une nouvelle durée devrait être motivée et le raisonnement devrait être documenté pour rendre compréhensible la décision.
Si les délais prévus pour l'effacement des données à caractère personnel dans des ensembles de données spécifiques ne sont pas directement fixés selon la législation nationale, la directive prévoit la vérification régulière de la nécessité de conserver les données.

La législation nationale devrait définir des critères clairs et transparents pour évaluer la nécessité de conserver les données à caractère personnel (comme la nécessité de tenir compte des mises à jour relatives à des décisions judiciaires ou en cas de réhabilitation des personnes condamnées, etc.) ainsi que des exigences procédurales, afin de respecter pleinement les principes relatifs à la qualité des données et d'éviter ainsi tout abus. À cette fin, quel que soit le moment où l'examen périodique est réalisé, le GT29 recommande que le délégué à la protection des données participe à l'application de ces critères - notamment en vue d'un éventuel audit interne - et les informations relatives à la décision de continuer à conserver les données et aux motifs de le faire devraient être conservées et mises à disposition de l'autorité de contrôle compétente[3].

---

fins scientifiques, statistiques ou historiques, aux fins énoncées à l'article 1er, paragraphe 1, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée». En outre, s'agissant du principe de limitation de la finalité, voir l'article 9 de la directive «police» selon lequel «les données à caractère personnel collectées par les autorités compétentes pour les finalités énoncées à l'article 1er, paragraphe 1, ne peuvent être traitées à des fins autres que celles énoncées à l'article 1er, paragraphe 1, à moins qu'un tel traitement ne soit autorisé par le droit de l'Union ou le droit d'un État membre. Lorsque des données à caractère personnel sont traitées à de telles autres fins, le règlement (UE) 2016/679 s'applique, à moins que le traitement ne soit effectué dans le cadre d'une activité ne relevant pas du champ d'application du droit de l'Union.»

[3] Par exemple, le règlement (UE) 2016/794 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) prévoit qu'Europol réexamine, en toute hypothèse, la nécessité de continuer à conserver les données à caractère personnel et peut décider de continuer à les conserver si leur conservation reste nécessaire pour lui permettre de remplir ses missions. Les raisons de prolonger la conservation des données sont justifiées et consignées. En l'absence de décision, les données devraient être effacées. Si les délais dépassent ceux fixés par la disposition, l'autorité de contrôle compétente (dans ce cas, le CEPD) en est informé (article 31).

De la même façon, les délégués à la protection des données doivent participer à la définition de la procédure afin de supprimer / d'effacer effectivement les données après l'expiration des délais de conservation.

Le GT29 considère que le fait de mettre à disposition du délégué à la protection des données et de l'autorité de contrôle, si nécessaire, les informations statistiques sur l'effacement des données et la procédure d'examen est une bonne pratique et un outil permettant de contrôler le respect des règles.

2. Calendriers distincts

Lorsqu'ils définissent des durées de conservation maximales et des examens périodiques, les États membres devraient tenir compte des principes de nécessité et de proportionnalité tels qu'ils sont interprétés par la Cour européenne des droits de l'homme et la Cour européenne de justice[4].

Les États membres devraient établir une distinction entre les catégories de données selon leur contribution effective aux finalités poursuivies et doivent utiliser des critères objectifs pour définir la durée de conservation maximale ou l'examen périodique.
Par exemple, le cas échéant, à la lumière de l'affaire en question, le type ou la gravité de l'infraction ou du risque sous-jacent doit être pris en compte.

En outre, l'article 5 de la directive «police» doit être interprété en lien avec son article 6, qui préconise d'établir des distinctions entre les différentes catégories de personnes concernées (les victimes, les suspects, les personnes reconnues coupables d'une infraction pénale, les témoins, les experts ou d'autres personnes impliquées). Les distinctions obligatoires doivent donner lieu à un régime progressif de différents calendriers à envisager par rapport aux différentes catégories de personnes concernées. Il convient également d'accorder une attention particulière à la protection des mineurs dans ce contexte. Les bases de données existantes et futures doivent être (ré-)organisées de façon à permettre d'établir les distinctions nécessaires entre les différentes catégories de personnes concernées.

[4] Pour un aperçu de l'application de ces deux principes dans le secteur répressif, voir l'avis 01/2014 du GT29 sur l'application des notions de nécessité et de proportionnalité et la protection des données dans le secteur répressif, WP 211, 27 février 2014 et, plus généralement, pour une «boîte à outils» utile en vue d'évaluer la nécessité et la proportionnalité d'une mesure juridique, voir le Contrôleur européen de la protection des données, «Guide pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel», 11 avril 2017.

3. Protection des données dès la conception

Dans le cadre des durées de conservation des données, le principe de la protection des données dès la conception devrait être tout particulièrement appliqué afin de promouvoir le respect des principes relatifs à la qualité des données, notamment en soulignant la nécessité de procéder à un examen périodique et en effaçant automatiquement les données dont la durée de conservation maximale a déjà expiré.

À cet égard, les délais maximaux ainsi que les examens périodiques prévus par la législation nationale devraient être appliqués dans le cadre d'un système informatique bien structuré fondé sur la «protection des données dès la conception».

Les bases de données existantes et futures devraient être (ré-)organisées de façon à garantir que les examens périodiques ont lieu systématiquement et que les données sont effacées automatiquement après avoir atteint la durée de conservation maximale.

En cas de délais maximaux, le système devrait garantir que les données sont effacées automatiquement ou rendues anonymes dès que le délai de conservation des données est atteint. En fonction de la mise en œuvre de ce système, les autorités compétentes devraient appliquer des mesures organisationnelles afin d'empêcher toute utilisation ultérieure de ces données.

En cas d'examens périodiques, le système devrait rappeler automatiquement au responsable du traitement l'importance d'examiner la nécessité d'un traitement ultérieur. Si l'examen n'est pas effectué dans un délai déterminé, les données respectives devraient être automatiquement effacées ou pseudonymisées / masquées.

Dans tous les cas, compte tenu des principes de nécessité et de proportionnalité en matière de protection des données, on pourrait envisager de mettre en place, après un certain temps, des garanties spécifiques afin de limiter l'accès aux données à caractère personnel (par exemple, seul le personnel autorisé pourrait avoir accès à ces données aux fins d'opérations spécifiques dans le cadre d'enquêtes en cours et/ou certaines catégories de données pourraient être pseudonymisées / masquées).

Recommandations du GT29

1. Les législations nationales sur le traitement des données relevant du champ d'application de la directive devraient toujours prévoir des durées de conservation maximales ainsi que des vérifications régulières de la nécessité de conserver les données respectives. La procédure d'examen devrait être documentée et la décision de prolonger la durée de conservation des données devrait être dûment justifiée.

2. Le principe de la protection des données dès la conception devrait être tout particulièrement appliqué dans ce contexte afin de promouvoir le respect des principes relatifs à la qualité des données. Les bases de données existantes et futures devraient être (ré-)organisées de façon à garantir que les examens périodiques ont lieu systématiquement et que les données sont effacées automatiquement après avoir atteint la durée de conservation maximale.

3. L'évaluation de la nécessité de continuer à conserver les données, ainsi que la définition des durées de conservation maximales devraient tenir compte des différentes catégories de personnes concernées.

Article 10
Traitement portant sur des catégories particulières de données à caractère personnel

Sujets clés
1. Articulation entre l'article 10 et l'article 8 de la directive «police»
2. Stricte nécessité
3. Garanties appropriées
4. Accord volontaire
5. Données manifestement rendues publiques par la personne concernée

1. Articulation entre l'article 10 et l'article 8 de la directive «police»

L'article 10 de la directive «police» doit être interprété en lien avec son article 8. Par conséquent, le traitement de catégories particulières de données, s'il n'est pas prévu par le droit de l'Union, requiert toujours une base juridique spécifique dans la législation nationale [article 10, point a)], conformément au considérant 33. Cette base juridique spécifique doit satisfaire aux exigences supplémentaires définies par l'article 10 de la directive «police». Par rapport à l'article 8 de la directive «police», le traitement doit être «strictement nécessaire» et des «garanties appropriées» doivent être prévues.

Le GT29 recommande d'interpréter l'article 10, points b) et c), comme illustrant simplement des situations spécifiques, dans lesquelles la législation nationale pourrait prévoir un tel traitement. L'article 10, point b), illustre une situation où les intérêts vitaux de la personne concernée nécessitent le traitement de catégories particulières de données. L'article 10, point c), illustre une situation où la personne concernée elle-même a volontairement renoncé à la protection des données sensibles en les rendant publiques.

2. Stricte nécessité

La différenciation entre «nécessaire» (article 8) et «strictement nécessaire» (article 10) requiert une nouvelle interprétation dans la mesure où elle est absente de la jurisprudence de la CJUE. En fait, conformément à une jurisprudence constante de la CJUE, toute dérogation à la protection des données à caractère personnel ou limitation de celle-ci doit être «strictement nécessaire», comme indiqué dans l'affaire Digital Rights Ireland: *«S'agissant du droit au respect de la vie privée, la protection de ce droit fondamental exige, selon la jurisprudence constante de la Cour, en tout état de cause, que*

les dérogations à la protection des données à caractère personnel et les limitations de celle-ci doivent s'opérer dans les limites du strict nécessaire»[5].

Le GT29 conclut de ce raisonnement que l'expression «strictement nécessaire» est employée dans l'article 10 pour souligner l'importance d'accorder une attention particulière au principe de nécessité dans le cadre du traitement de catégories particulières de données, et de prévoir des motifs précis et particulièrement solides du traitement de ces données[6].

Pour déterminer si les responsables du traitement peuvent ou non traiter des données sensibles, et le cas échéant, dans quelle mesure, il convient de trouver le juste équilibre entre le droit au respect de la vie privée et l'intérêt public. À cet égard, le GT29 recommande, étant donné le champ d'application de la directive et la sensibilité des opérations de traitement concernées, que les autorités compétentes s'engagent à procéder à une analyse d'impact relative à la protection des données. Il convient d'évaluer et de démontrer si la finalité du traitement (par ex. une enquête pénale) ne peut être atteinte dans le cadre d'un traitement qui affecte moins les droits et les libertés de la personne concernée et si le traitement de catégories particulières de données ne représente pas un risque de discrimination de la personne concernée. Lors de l'évaluation du risque d'abus et de discrimination, les garanties prévues doivent être prises en compte.

3. Garanties appropriées

Le traitement de catégories particulières de données comporte toujours le risque que la personne concernée puisse être victime de discrimination en violation de l'article 21 de la charte des droits fondamentaux de l'Union européenne ou d'autres effets défavorables significatifs sur ses droits et libertés. Les garanties sont appropriées si elles suffisent à protéger la personne contre ces risques. Une liste des garanties possibles peut être consultée au considérant 37.

Des garanties juridiques peuvent être prévues dans le cadre d'exigences matérielles ou procédurales supplémentaires. Des exigences matérielles supplémentaires pourraient consister en des limitations supplémentaires aux fins du traitement (par ex. certaines catégories d'infractions) ou en cas de mesures préventives face à une certaine urgence

[5] Arrêt de la CJUE du 8 avril 2014, Digital Rights Ireland, affaires jointes C-293/12 et C-594/12, point 52; voir également l'arrêt de la CJUE du 6 octobre 2015, Schrems, C-362/14, point 92; s'agissant du recours à un critère de stricte nécessité pour évaluer les mesures juridiques, voir également le Contrôleur européen de la protection des données, Guide pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel, 11 avril 2017 et pour un aperçu de l'application de ces deux principes dans le secteur répressif, voir l'avis 01/2014 du GT29 sur l'application des notions de nécessité et de proportionnalité et la protection des données dans le secteur répressif, WP 211, 27 février 2014.

[6] Pour une approche similaire adoptée par la CJUE dans son avis sur le projet d'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers, voir l'avis 1/15 (grande chambre), 26 juillet 2017, points 141 et 165.

(par ex. un danger imminent avec des conséquences probablement graves pour les intérêts vitaux de nombreuses personnes). Le considérant 37 évoque également la possibilité de ne collecter ces données qu'en rapport avec d'autres données relatives à la personne physique concernée. Des garanties procédurales supplémentaires pourraient consister en l'autorisation préalable d'une cour ou d'un autre organe indépendant et en l'interdiction de la transmission de ces données.

Les garanties juridiques devraient généralement s'accompagner de/être mises en œuvre par des mesures techniques et organisationnelles comme des mesures supplémentaires de sécurité des données afin de garantir la confidentialité et l'intégrité des données, et de règles plus strictes pour l'accès du personnel de l'autorité compétente aux données.

4. Accord volontaire

L'accord de la personne concernée ne peut jamais constituer en soi une base juridique pour le traitement de catégories particulières de données dans le cadre de la directive. Il s'agit d'une différence majeure par rapport au RGPD et cette différence est explicitement soulignée au considérant 35, qui indique que les États membres peuvent prévoir par la loi que la personne concernée peut consentir au traitement de données à caractère personnel la concernant aux fins de cette directive[7].

À la lumière de ce qui précède, le GT29 conclut que l'accord volontaire devrait être uniquement envisagé en tant que garantie supplémentaire en vertu du droit dans les cas où un traitement qui est particulièrement intrusif pour la personne concernée est prévu par la loi. Par conséquent, il incombe au législateur national de décider si et dans quelle mesure il y a lieu d'autoriser le traitement des données à condition d'avoir l'accord volontaire de la personne concernée, et de décider d'inclure ou non des catégories particulières de données (voir à ce sujet le considérant 37[8]).

---

[7] Considérant 35: *«Dans le cadre de l'exécution des missions de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales qui leur sont confiées de manière institutionnelle par la loi, les autorités compétentes peuvent demander ou ordonner aux personnes physiques de donner suite aux demandes qui leur sont adressées. Dans ce cas, le consentement de la personne concernée, au sens du règlement (UE) 2016/679, ne devrait pas constituer une base juridique pour le traitement de données à caractère personnel par les autorités compétentes. Lorsqu'elle est tenue de respecter une obligation légale, la personne concernée ne dispose pas d'une véritable liberté de choix; sa réaction ne pourrait dès lors être considérée comme une manifestation libre de sa volonté. Cela ne devrait pas empêcher les États membres de prévoir par la loi que la personne concernée peut consentir au traitement de données à caractère personnel la concernant aux fins de la présente directive.»*

[8] *Ce dernier point est possible, comme le précise le considérant 37, mais doit être explicitement prévu par la loi: «Il convient également que le traitement de pareilles données soit autorisé par la loi lorsque la personne concernée a expressément marqué son accord au traitement qui est particulièrement intrusif pour elle. Toutefois, l'accord de la personne concernée ne devrait pas constituer en soi une*

Dans ces cas, la personne concernée doit être informée clairement et sans ambiguïté par l'autorité compétente de la nature volontaire de son accord et doit avoir la possibilité de le retirer à tout moment (par exemple, dans le cas de la collecte d'empreintes digitales ou d'échantillons biologiques).

base juridique pour le traitement de ces données à caractère personnel sensibles par les autorités compétentes.»

5. Données manifestement rendues publiques par la personne concernée

Selon l'article 10, point c), les législateurs nationaux peuvent décider d'autoriser le traitement de catégories particulières de données s'il est strictement nécessaire et sous réserve de garanties appropriées, lorsque ces données ont été manifestement rendues publiques par la personne concernée.

Le GT29 souhaite souligner que cet article doit être interprété comme impliquant que la personne concernée a été informée du fait que les données respectives seront rendues publiques pour tout le monde, y compris les autorités. En cas de doute, une interprétation restrictive devrait prévaloir, dans la mesure où l'on suppose que la personne concernée a volontairement renoncé à la protection spéciale des données sensibles en les mettant à disposition du public, y compris des autorités.

Dans les cas comme la publication de données à caractère personnel dans une biographie, dans la presse ou sur un site web public, l'intention est claire. Dans d'autres cas, cela reste plus difficile à déterminer. L'inscription à un réseau social, par exemple, peut comprendre l'acceptation de certaines règles de protection des données en vertu desquelles tous les partenaires du fournisseur (y compris les forces de police nationales) ont accès à des données à caractère personnel. Dans ces cas, la plupart des utilisateurs ne prennent pas activement connaissance de ces règles et ignorent en fait que leurs données sont mises à la disposition des forces de police.

Recommandation du GT29

1. Le traitement de catégories particulières de données, s'il n'est pas prévu par le droit de l'Union, requiert une base juridique spécifique dans la législation nationale.

2. L'article 10 recommande d'accorder une attention particulière au principe de nécessité concernant le traitement de catégories particulières de données et de prévoir des motifs précis et particulièrement solides du traitement de ces données.

3. Les garanties sont appropriées si elles suffisent à protéger la personne concernée contre le risque de discrimination ou contre des effets défavorables significatifs sur les droits et libertés de la personne concernée comme l'interdit l'article 21 de la charte.

4. Dans le champ d'application de la directive, l'accord volontaire devrait uniquement être envisagé comme une garantie supplémentaire en vertu du droit dans les cas où un traitement qui est particulièrement intrusif pour la personne concernée est prévu par la loi. Par conséquent, il incombe au législateur national de décider si et dans quelle mesure il y a lieu d'autoriser le traitement des données à condition

d'avoir l'accord volontaire de la personne concernée, et de décider d'inclure ou non des catégories particulières de données.

5. L'article 10, point c), implique que la personne concernée a été informée du fait que les données respectives seront rendues publiques pour tout le monde, y compris les autorités. En cas de doute, il devrait être interprété de manière restrictive.

Article 11
Décision individuelle automatisée et profilage

Sujets clés
1. Définitions
2. Concepts clés de décisions fondées exclusivement sur un traitement automatisé, y compris le profilage
3. Obligations d'information

Le profilage et la prise de décision automatisée sont plus en plus développés dans de nombreux secteurs, y compris dans le domaine couvert par la directive.

S'ils peuvent être utiles dans le cadre des activités des autorités compétentes destinées aux fins spécifiques couvertes par l'article 1er, ils peuvent représenter des risques significatifs pour les droits et libertés des personnes concernées, et nécessitent donc des garanties appropriées,

Tout comme le RGPD, la directive traite spécifiquement du profilage et de la prise de décision individuelle automatisée, y compris le profilage.

Avec les lignes directrices adoptées le 3 octobre 2017, le groupe de travail «Article 29» a apporté des éclaircissements sur les dispositions pertinentes du RGPD relatives à la prise de décision automatisée et au profilage et des recommandations de meilleures pratiques. Ces orientations sont également pertinentes pour la directive 2016/680, malgré d'importantes réserves et certaines précisions.

1. Définitions

La directive «police» définit le «profilage» à l'article 3, paragraphe 4, à l'aide d'une formulation qui correspond entièrement à celle utilisée dans le RGPD, rendant ainsi applicables les considérations déjà exprimées par le GT29 dans lesdites lignes directrices.

La «prise de décision exclusivement automatisée» est la capacité de prendre des décisions par des moyens technologiques sans intervention humaine dans le processus décisionnel.

Bien que le profilage et la prise de décision automatisée puissent être des activités combinées du même processus, ils peuvent également être effectués séparément. Dans certains cas, les décisions automatisées sont prises avec (ou sans) profilage et le profilage a lieu sans prendre de décisions automatisées. Le profilage doit impliquer une certaine forme de traitement automatisé – bien que la participation humaine n'exclue pas nécessairement l'activité de la définition.

2. *Concepts clés de décisions fondées exclusivement sur un traitement automatisé, y compris le profilage*

Décisions individuelles exclusivement automatisées

L'article 11 établit une interdiction générale des «décisions individuelles exclusivement automatisées», y compris le profilage, ayant des «effets juridiques défavorables» ou «affectant de manière significative» la personne concernée. La seule exception à cette interdiction est qu'une telle décision automatisée soit autorisée par le droit de l'Union ou le droit d'un État membre qui fournit des garanties appropriées pour les droits et libertés des personnes concernées9.

Compte tenu de la nature spéciale du traitement réalisé à des fins répressives, l'article 11 de la directive «police» ne contient aucune référence aux autres exceptions prévues par l'article 22, paragraphe 2, du RGPD, à savoir: a) un traitement nécessaire à la conclusion ou à l'exécution d'un contrat; b) un traitement fondé sur le consentement explicite de la personne concernée. Dans ce contexte, le GT29 souhaite rappeler que l'accord de la personne concernée ne peut jamais constituer la base juridique dans la mesure où il existe un net déséquilibre entre la personne concernée et le responsable du traitement (comme dans ce cas).

Contrairement au RGPD, la directive précise que cette interdiction s'applique à la prise de décision individuelle automatisée qui ne produit pas seulement des «effets juridiques» sur la personne concernée, mais des effets juridiques «défavorables». Typiquement, un effet défavorable découlant d'une décision automatisée pourrait être

[9] À cet égard, la décision-cadre 2008/977/JAI du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, abrogée par la directive 680/2016, ne donnait pas de définition du «profilage». Toutefois, l'article 7 encadrait la décision individuelle automatisée en indiquant qu'une «décision qui produit des effets juridiques défavorables pour la personne concernée ou qui l'affecte de manière significative et qui est prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité n'est autorisée que si la sauvegarde des intérêts légitimes de la personne concernée est assurée par la loi».

l'application de mesures de sécurité ou d'une surveillance accrues par les autorités compétentes.

Cependant, le même article considère que cette interdiction est également valable en ce qui concerne une décision qui «affecte de manière significative» la personne concernée, comme par exemple dans le cas où un passager n'est pas autorisé à embarquer car il figure sur une liste noire, élargissant ainsi le champ d'application de l'article 11.

L'expression «de manière significative» exclut le fait que des effets négligeables puissent être considérés comme suffisants pour mettre en œuvre l'interdiction: l'effet doit être suffisamment significatif pour mériter l'attention et l'influence de la personne concernée.

Droit d'obtenir une intervention humaine

La directive indique que le législateur national des États membres, lorsqu'il autorise la décision prise sur le seul fondement d'un traitement automatisé en vertu de l'article 11, doit fournir aux personnes concernées le droit d'obtenir une intervention humaine de la part du responsable du traitement.

Bien que l'article 11 ne fasse référence qu'au droit d'obtenir une intervention humaine et non «d'exprimer son point de vue et de contester la décision» comme prévu par l'article 22 du RGPD, il convient de souligner que selon le considérant 38 de la directive, dans tous les cas, ce traitement devrait être assorti de garanties appropriées, y compris «le droit d'obtenir une intervention humaine, en particulier d'exprimer son point de vue, d'obtenir une explication quant à la décision prise à l'issue de ce type d'évaluation ou de contester la décision».

Comme le souligne le GT29 dans ses lignes directrices sur le profilage, l'intervention humaine est un élément clé: elle permet à la personne concernée de ne pas faire l'objet de décisions automatisées indéchiffrables qui pourraient contenir des erreurs ou être biaisées et lui permet d'avoir un échange avec le responsable du traitement ouvert aux éléments supplémentaires ou à la contestation que la personne concernée pourrait souhaiter soulever.

À cet égard, il convient de rappeler que, pour être significative, l'intervention humaine doit être effectuée par une personne qui a l'autorité et la capacité nécessaires pour changer la décision et qui examinera toutes les données pertinentes, y compris les éléments supplémentaires fournis par la personne concernée.

L'interdiction de la discrimination à la suite d'une prise de décision automatisée

Le paragraphe 2 de l'article 11 établit l'interdiction de fonder des décisions automatisées sur des catégories particulières de données (article 10) à moins que des

mesures appropriées pour la sauvegarde des droits et des libertés et des intérêts légitimes de la personne concernée ne soient mises en place par les États membres.

Compte tenu de la nature spéciale des données et des risques évidents de discrimination découlant des décisions automatisées fondées sur ces données, il est particulièrement important que les États membres, lors de la mise en œuvre de la directive, fournissent des garanties strictes pour protéger les droits des personnes concernées.

La création de profils entraînant une discrimination sur la base des catégories particulières de données est interdite en soi par l'article 11, paragraphe 3, conformément au droit de l'Union.

La discrimination est sans conteste un exemple d'une décision qui affecte la personne concernée de manière significative et peut comporter également des effets juridiques défavorables. Par conséquent, les États membres devraient considérer que la législation nationale ne peut pas, en toutes circonstances, autoriser le profilage qui entraîne une discrimination s'il est fondé sur le traitement de données sensibles (article 11, paragraphe 3), tandis que la prise de décision automatisée fondée sur des données sensibles est autorisée, mais uniquement en présence d'une base juridique dans le droit national ou de l'Union - qui fournit les garanties mentionnées ci-après (voir l'article 11, paragraphes 1 et 2)[10].

Analyse d'impact relative à la protection des données

Il convient de rappeler que l'obligation de procéder à une analyse d'impact relative à la protection des données en vertu de l'article 27, paragraphe 1, de la directive «police» est formulée exactement comme la disposition correspondante à l'article 35, paragraphe 1, du RGPD. En outre, les considérants 51 et 52 soulignent expressément que le profilage en soi et même le simple traitement de données sensibles par nature comportent des risques pour les droits et libertés des personnes concernées, qui pourraient se traduire par un risque élevé selon le considérant 52 s'il existe le risque particulier de «porter atteinte aux droits et aux libertés des personnes concernées». Compte tenu des considérations qui précèdent sur les «effets juridiques défavorables» pouvant être dus à une prise de décision automatisée et sur la «discrimination» dans le cas d'une prise de décision automatisée «affectant de manière significative» les personnes concernées, le GT29 recommande aux législateurs nationaux d'obliger les responsables du traitement à procéder à une analyse d'impact relative à la protection des données en lien avec ces opérations de traitement. Ces analyses d'impact relatives à la protection des données peuvent notamment permettre d'identifier les garanties et

[10] À cet égard, voir par exemple la directive (UE) 2016/681 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, article 6, paragraphe 4, et considérant 15.

mesures d'atténuation spécifiques qui n'ont pas été définies dans des mesures législatives (plus générales) autorisant cette prise de décision automatisée; à cette fin, la consultation préalable de l'autorité de contrôle compétente conformément à l'article 28 jouera un rôle essentiel.

3. Obligations d'information

En général, il convient de rappeler que les garanties prévues par le considérant 38 devraient être fournies par les législations des États membres conformément à l'article 12 qui renvoie clairement à l'obligation, pour le responsable du traitement, de faciliter l'exercice des droits de la personne concernée en vertu de l'article 11 et à l'importance, pour les États membres, de garantir qu'«aucun paiement n'est exigé pour fournir les informations sur «toute communication relative au traitement ayant trait à l'article 11» (article 12, paragraphes 2 et 4). De même, la fourniture d'informations appropriées, notamment au sujet de l'existence d'une décision automatisée, y compris le profilage, et d'informations pertinentes sur la logique sous-jacente à la personne concernée est particulièrement importante aussi en ce qui concerne la loyauté du traitement qui devrait être garantie selon l'article 4, paragraphe 1, point a).

S'agissant des exigences spécifiques concernant la façon et le moment d'apporter de la transparence au traitement des données effectué à des fins répressives, voir le paragraphe 2 sur les droits des personnes concernées du présent document d'orientation.

Contrairement au RGPD, la directive ne mentionne pas explicitement la nécessité d'inclure l'existence d'une décision automatisée, y compris le profilage, dans les informations à fournir à la personne concernée en vertu de l'article 13. Cependant, étant donné que les décisions automatisées et le profilage sont souvent «opaques» et peuvent être effectués à l'insu de la personne concernée, l'article 13, paragraphe 2, point d) – aux termes duquel «au besoin, des informations complémentaires, en particulier lorsque les données à caractère personnel sont collectées à l'insu de la personne concernée» doivent être fournies – peut s'appliquer sous réserve des dispositions prises au paragraphe 3 de l'article 13. Ces dispositions sont identiques à celles citées à l'article 23, paragraphe 1, points a), c), d) et i), du RGPD, à condition que les États membres «puissent» (en vertu de l'article 13, paragraphe 4) déterminer les catégories de traitements faisant l'objet des restrictions citées à l'article 13, paragraphe 3. Le GT29 prie instamment les États membres souhaitant introduire de telles restrictions de fournir la base juridique appropriée dans le cadre de mesures législatives (voir l'article 11, paragraphe 1).

Il convient également de rappeler aux responsables du traitement qu'ils doivent tenir un registre des opérations de traitement (conformément à l'article 24) précisant s'ils ont recours au profilage. Il s'agit d'une obligation importante, qui n'est pas prévue dans

le RGPD de manière aussi générale et que les États membres doivent particulièrement veiller à respecter.

Recommandations du GT29

1. L'interdiction générale des «décisions individuelles exclusivement automatisées», y compris le profilage, ayant des «effets juridiques défavorables» ou «affectant de manière significative» la personne concernée devrait être respectée. Les législations nationales prévoyant des exceptions à cette interdiction en vertu de l'article 11, paragraphe 1, doivent fournir des garanties appropriées pour les droits et libertés des personnes concernées, y compris le droit d'obtenir une intervention humaine, en particulier d'exprimer son point de vue, d'obtenir une explication quant à la décision prise à l'issue de ce type d'évaluation ou de contester la décision.

2. La législation nationale ne peut, en aucune circonstance, autoriser un profilage qui entraîne une discrimination s'il est fondé sur le traitement de données sensibles (article 11, paragraphe 3). La prise de décision automatisée fondée sur des données sensibles peut uniquement être effectuée en présence d'une base juridique dans le droit national ou de l'Union qui fournit les garanties mentionnées ci-après (voir l'article 11, paragraphes 1 et 2).

3. Les législateurs nationaux devraient obliger les responsables du traitement à procéder à une analyse d'impact relative à la protection des données en lien avec des décisions automatisées.

4. Les États membres (sans préjudice des mesures possibles limitant la fourniture d'informations à la personne concernée selon l'article 13, paragraphe 3) doivent obliger les responsables du traitement à fournir des informations appropriées à la personne concernée, en particulier lorsque les données à caractère personnel sont collectées à son insu [article 13, paragraphe 2, point d)], ce qui peut être souvent le cas dans le cadre du profilage et des décisions automatisées.

Articles 13 à 17
Droits de la personne concernée

Sujets clés
1. Droits de la personne concernée
2. Informations à mettre à la disposition de la personne concernée (article 13)
3. Accès direct en règle générale (article 14)
4. Accès limité (article 15)
5. Droit de rectification ou d'effacement et limitation du traitement (article 16)
6. Accès indirect (article 17)

1. Droits de la personne concernée

Premièrement, il est important d'observer l'articulation des droits des personnes concernées telle qu'elle est décrite par les articles 13 à 17 de la directive.

Ces articles prévoient différents cas où des informations devraient être fournies et certaines exceptions. L'article 13 de la directive «police» décrit l'obligation active des responsables du traitement de fournir certaines informations aux personnes concernées. Certaines informations doivent être rendues publiques (article 13, paragraphe 1). Des informations plus détaillées doivent être données à une certaine personne concernée dans des cas particuliers (article 13, paragraphe 2). Des exceptions à l'article 13, paragraphe 2, peuvent être prévues par la loi dans certaines conditions (article 13, paragraphes 3 et 4).

L'article 14 de la directive «police» établit en tant que règle générale le droit de la personne concernée d'avoir accès aux données à caractère personnel la concernant, à savoir le droit d'obtenir directement du responsable du traitement la confirmation positive ou négative du traitement des données à caractère personnel la concernant (également connu comme le droit d'«accès direct» de la personne concernée). Dans les cas positifs, cela comprend l'accès aux données à caractère personnel et certaines informations.

Des limitations du droit d'accès direct peuvent être adoptées par la législation nationale selon les conditions établies à l'article 15 de la directive «police». Dans ces cas, la personne concernée a généralement le droit d'être informée de la limitation et de la possibilité d'introduire une réclamation auprès de l'autorité de contrôle.

La transparence du traitement des données garantie par le droit d'accès n'est pas seulement un «droit de connaître», mais est encore renforcée par le droit de rectification, d'effacement ou de limitation du traitement prévu par l'article 16 de la directive «police».

Si la loi autorise à limiter les droits d'information, d'accès ou de rectification/d'effacement, la personne concernée a un droit d'«accès indirect», conformément à l'article 17 de la directive «police». Dans ces cas, la législation nationale doit prévoir la possibilité d'exercer les droits d'information, d'accès ou au moins d'information sur le refus de rectification ou d'effacement par le responsable du traitement également par l'intermédiaire de l'autorité de contrôle compétente. Ce droit doit être distinct du droit d'introduire une réclamation auprès de l'autorité de contrôle et constitue un droit supplémentaire dans le cadre de la directive.

2. Informations à mettre à la disposition de la personne concernée (article 13)

Mettre à disposition les informations et être transparent avec les personnes concernées sur la manière dont leurs informations seront utilisées contribue à garantir que le traitement licite des données à caractère personnel est loyal et que les responsables du traitement sont eux-mêmes tenus responsables. Le traitement des données relevant du champ d'application de la directive peut parfois être utilisé d'une manière qui pourrait porter préjudice à la personne concernée. Cet aspect est important car le traitement des données dans le cadre de la directive entraîne des limitations des droits et libertés des personnes concernées et est parfois effectué à l'insu des personnes concernées. En outre, fournir des informations sur le traitement répondrait aux attentes raisonnables des personnes concernées.

L'article 13, paragraphe 1, points a) à e), définit les informations que le responsable du traitement doit mettre à la disposition des personnes concernées. Il convient de souligner que la formulation de l'article 13, paragraphe 1, évoque le fait de «mettre à disposition» les informations, tandis que l'article 13, paragraphe 2, parle de «fournir» des informations «dans des cas particuliers». Il s'agit d'une approche différente, où on peut considérer que cette obligation ne s'applique pas à une certaine personne concernée, mais à une certaine procédure de traitement et toutes les personnes concernées pouvant être affectées par cette dernière. Par conséquent, cette obligation implique que les informations doivent être réellement mises à disposition afin de garantir que toute personne potentiellement concernée les connaît.

Concernant l'article 13, paragraphe 1, le considérant 42 donne des exemples de la manière dont ces informations peuvent être fournies, notamment sur le site web de l'autorité compétente. Les forces de police peuvent par exemple souhaiter publier leur politique de confidentialité concernant l'utilisation d'images de surveillance, les vidéos issues de caméras corporelles ou l'enregistrement des armes à feu.

Les informations énumérées à l'article 13, paragraphe 1, devraient être toujours mises à disposition. Lorsqu'ils donnent les coordonnées du délégué à la protection des données, le GT29 recommande aux responsables du traitement de préciser également que le délégué à la protection des données est l'un des points de contact des personnes concernées pour adresser leurs demandes. L'article 13, paragraphe 1, point c), indique que les finalités du traitement devraient figurer sur la liste des informations fournies. Le GT29 souligne que les responsables du traitement devraient donc être aussi transparents et précis que possible sur les finalités répressives auxquelles est destiné le traitement des données.

Les responsables du traitement devraient combiner les diverses techniques les plus efficaces pour mettre à la disposition de la personne concernée les informations

requises. Le GT29 recommande de recourir pour ce faire, dans la mesure du possible, au même moyen utilisé pour collecter les données à caractère personnel.

Comme expliqué ci-dessus, si l'article 13, paragraphe 1, concerne les informations générales à mettre à la disposition du public, l'article 13, paragraphe 2, porte sur les informations à fournir en complément à une certaine personne concernée dans des cas particuliers, par exemple lorsque les données sont collectées directement auprès de la personne concernée ou indirectement à l'insu de la personne concernée.

Les États membres peuvent adopter des mesures législatives visant à retarder ou à limiter la fourniture à la personne concernée des informations énumérées à l'article 13, paragraphe 2, ou à ne pas fournir ces informations, dans la mesure où il s'agit d'une mesure nécessaire et proportionnée pour éviter les préjudices énumérés à l'article 13, paragraphe 3. Toute mesure législative doit tenir dûment compte des droits fondamentaux et des intérêts légitimes de la personne concernée.

Le GT29 recommande aux législateurs nationaux de définir des critères objectifs pour déterminer dans quels cas et selon quelles conditions les informations complémentaires énumérées à l'article 13, paragraphe 2, peuvent ne pas être divulguées par les responsables du traitement. L'article 13, paragraphe 4, autorise les États membres à adopter des mesures législatives afin de déterminer quelles catégories de traitement sont susceptibles de relever, dans leur intégralité ou en partie, de l'article 13, paragraphe 3.

L'article 13, paragraphe 4, et l'article 15, paragraphe 2, n'autorisent pas de restrictions générales des droits d'information et d'accès des personnes concernées.

3. Accès direct en règle générale (article 14)

En vertu de la directive, les législateurs nationaux doivent prévoir que la personne concernée a le droit d'obtenir du responsable du traitement la confirmation du traitement des données à caractère personnel la concernant et l'accès auxdites données. Ce droit est également consacré par l'article 8, paragraphe 2, de la charte des droits fondamentaux de l'Union européenne.

Le GT29 souligne qu'il existe un droit de confirmation négative découlant de l'article 14. Une politique consistant à «ni confirmer, ni démentir» est également possible dans le cas des dérogations prévues à l'article 15.

Ces informations devraient être communiquées gratuitement dans les meilleurs délais. La directive ne précisant pas ce que signifie «dans les meilleurs délais», le GT29 considère donc que les responsables du traitement devraient fournir à la personne concernée les informations en réponse à une demande faite dans le cadre de l'article 14 dès que possible et si possible dans un délai d'un mois. Les autorités de contrôle devraient rendre, si nécessaire, une décision concernant la conformité fondée sur la représentation et les éléments de preuve apportés par le responsable du traitement et par les personnes concernées.

La législation nationale doit également garantir que le responsable du traitement fournit et communique les informations à la personne concernée d'une façon concise, compréhensible et aisément accessible, en des termes clairs et simples conformément à l'article 12, paragraphe 1.

En outre, la liste des informations devant être incluses en réponse au droit d'accès comprend des informations sur les destinataires ou les catégories de destinataires à qui les données à caractère personnel ont été divulguées. La directive n'indique pas clairement le degré de précision avec lequel le responsable du traitement doit fournir ces informations. Le GT29 souhaite rappeler aux législateurs nationaux et aux responsables du traitement l'essence du droit d'accès, qui consiste à confirmer la base juridique à la personne concernée et à lui permettre de vérifier la licéité du traitement. Par conséquent, les responsables du traitement devraient s'assurer que les informations fournies sont précises, claires et suffisantes pour atteindre cette finalité.

Dans les cas où le droit d'accès est respecté, le GT29 souhaite rappeler aux législateurs nationaux et aux responsables du traitement que l'article 14, point g), englobe non seulement la source des données, mais également toutes les informations pertinentes sur la manière et les circonstances dans lesquelles le responsable du traitement les a reçues. Il convient également de rappeler que les personnes concernées ont un intérêt légitime à connaître la source de leurs données et, si possible, les finalités pour lesquelles les données ont été transmises.

4. Limitations du droit d'accès (article 15)

L'article 15 prévoit comme seule possibilité pour les États membres celle d'adopter des mesures législatives pour limiter, de manière partielle ou complète, le droit d'accès de la personne concernée tel qu'il est décrit à l'article 14, aussi longtemps qu'une telle limitation constitue une mesure nécessaire et proportionnée pour les motifs énumérés à l'article 15, paragraphe 1.

Le GT29 souhaite rappeler aux législateurs nationaux que toute exemption des droits fondamentaux et des intérêts légitimes de la personne physique devrait être appliquée comme l'exception et non la règle et que le fait de ne pas fournir les informations peut être autorisé dans le cadre d'une enquête uniquement aussi longtemps qu'une telle restriction constitue une mesure nécessaire et proportionnée. Conformément à la jurisprudence de la Cour de justice de l'Union européenne, les informations qui ne sont pas fournies doivent être communiquées lorsqu'elles ne sont plus responsables de compromettre les enquêtes en cours[11].

Sous réserve de l'article 15, si le droit d'accès de la personne concernée n'a été limité que partiellement et qu'une réponse peut être fournie, le responsable du traitement devrait donner accès aux données à caractère personnel qui sont traitées et aux informations énumérées à l'article 14. Si possible, les informations devraient être fournies sous la même forme que la demande. Si l'article 14 n'indique pas explicitement que le responsable du traitement devrait fournir une copie, sur demande et si possible, elle devrait être fournie dans le cadre d'une demande d'accès. En outre, le considérant 43 précise qu'un aperçu des données en possession du responsable du traitement devrait être fourni.

Si les États membres décident d'autoriser les responsables du traitement à limiter complètement le droit d'accès aux informations énumérées à l'article 14, à condition qu'une exemption puisse être appliquée au titre de l'article 15, paragraphe 1, il est possible qu'aucune information ne soit communiquée à la personne concernée. Par conséquent, il peut être envisagé de recourir au concept consistant à «ni confirmer, ni démentir», mais de nouveau, le GT29 souhaite rappeler aux législateurs nationaux et aux responsables du traitement l'importance d'appliquer une exemption uniquement lorsque cette mesure est strictement nécessaire et proportionnée, au cas par cas, et de ne pas accorder d'exemptions «générales».

Même si le responsable du traitement souhaite limiter complètement le droit d'accès, les États membres doivent prévoir que le responsable du traitement informe la

[11] Cour de justice de l'Union européenne, avis 1/15 de la Cour (grande chambre) relatif au projet d'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers, 26 juillet 2017; voir, par analogie, l'arrêt du 21 décembre 2016, Tele2 Sverige et Watson et Autres, affaires jointes C-203/15 et C-698/15, EU:C:2016:970, point 121 et jurisprudence citée.

personne concernée, dans les meilleurs délais, par écrit, en confirmant le refus ou la limitation de l'accès et les motifs. De nouveau, comme pour l'article 14, une réponse à la personne concernée devrait être fournie dans un délai d'un mois civil à compter de la réception de la demande, si possible.

En réponse, les responsables du traitement peuvent ne pas indiquer les motifs du refus ou de la limitation lorsqu'une exemption est appliquée au titre de l'article 15, paragraphe 1. Les États membres devraient s'assurer que les responsables du traitement fournissent toujours une réponse à une demande de droit d'accès et que si le droit d'accès est limité ou refusé, la personne concernée reçoit des informations concernant le droit d'introduire une réclamation auprès d'une autorité de contrôle et les coordonnées de cette dernière ou la possibilité de former un recours juridictionnel.

En outre, en vertu de l'article 15, paragraphe 4, si le droit d'accès est limité ou refusé, les États membres doivent prévoir que les responsables du traitement consignent les motifs de fait ou de droit sur lesquels se fonde la décision et ces informations doivent être mises à la disposition des autorités de contrôle sur demande.

5. Droit de rectification ou d'effacement et limitation du traitement (article 16)

En vertu de l'article 16, paragraphe 1, les États membres prévoient le droit pour la personne concernée d'obtenir la rectification des données à caractère personnel la concernant qui sont inexactes, en particulier lorsque cela touche aux faits (considérant 47) et, compte tenu des finalités du traitement, le droit d'obtenir que les données soient complétées, y compris en fournissant à cet effet une déclaration complémentaire. Les responsables du traitement doivent veiller à répondre à ces demandes dès que possible et si possible dans un délai d'un mois.

Si des données inexactes sont traitées par les responsables du traitement dans le cadre de la directive, la possibilité que ce traitement ait des effets défavorables sur les personnes concernées est grande. Par conséquent, le GT29 souhaite rappeler aux législateurs nationaux et aux responsables du traitement la nécessité de garantir, dans la mesure du possible, que des données précises sont traitées et que les demandes fondées de rectification des données sont traitées avec l'urgence nécessaire.

S'agissant de l'effacement des données, les États membres exigent également, en vertu de l'article 16, paragraphe 2, que les responsables du traitement effacent les données à caractère personnel et accordent aux personnes concernées le droit d'obtenir du responsable du traitement l'effacement des données à caractère personnel les concernant lorsque le traitement constitue une violation de la directive (considérant 47). L'effacement des données à caractère personnel est requis lorsque le traitement de ces données constitue une violation des principes relatifs au traitement des données à caractère personnel, lorsqu'il est illégal, lorsqu'il constitue une violation

des dispositions de la directive relatives au traitement des catégories particulières de données ou lorsque les données à caractère personnel doivent être effacées pour respecter une obligation légale à laquelle est soumis le responsable du traitement.

La liste des traitements exigeant l'effacement des données au titre de l'article 16, paragraphe 2, ne devrait pas être considérée comme exhaustive; les législateurs nationaux et les responsables du traitement devraient tenir compte de l'essentiel du droit tel qu'il est énoncé au considérant 47.

Dans le cas où, à la suite d'une demande d'effacement des données à caractère personnel, les responsables du traitement considèrent que les données à caractère personnel doivent être conservées à des fins probatoires et lorsque l'exactitude des données à caractère personnel est contestée par la personne concernée et qu'il ne peut être déterminé si ces données sont exactes ou non, la directive prévoit le droit d'obtenir du responsable du traitement la limitation du traitement, plutôt que l'effacement. Cette limitation peut être réalisée dans le cadre des moyens techniques énoncés au considérant 47. Dans ce cas, le GT29 recommande de documenter ces limitations et de préciser, par exemple, quand la limitation a commencé et quand elle a pris fin. En outre, le GT29 recommande, dans le cas d'une limitation du traitement, de ne pas envoyer les données à d'autres responsables du traitement tant que la limitation n'est pas levée.

Le GT29 souligne également que même si la directive ne prévoit pas expressément un droit à la limitation du traitement à l'article 16 distinct du droit d'effacement, comme à l'article 18 du RGPD, les considérants 47 et 48 évoquent ce droit distinctement. Par conséquent, le GT29 encourage les États membres à prévoir la création de ce droit pour les personnes concernées dans leur législation nationale, à la fois comme corollaire du droit d'effacement et comme droit distinct pour les personnes concernées qui devraient pouvoir demander la limitation du traitement dans d'autres cas que les deux situations prévues au paragraphe 3 de l'article 16, notamment dans les cas où l'effacement aura été refusé par le responsable du traitement sans limitation du traitement.

Si une demande d'effacement ou de rectification est refusée, la législation nationale doit contraindre les responsables du traitement à fournir des informations écrites concernant le refus et ses motifs. L'article 16, paragraphe 4, donne la possibilité aux États membres d'adopter des mesures législatives pour limiter, en tout ou partie, les informations écrites à fournir à la personne concernée au sujet du refus, par le responsable du traitement, de rectifier ou d'effacer les données ou de limiter le traitement et les motifs de ce refus.

Bien que la directive ne prévoie que la possibilité de limiter la fourniture de ces informations à la personne concernée en cas de refus du responsable du traitement, le GT29 souligne qu'il devrait être précisé que dans les cas où il est établi que les données sont inexactes ou incomplètes, ou que les données sont traitées en violation des

articles 4, 8 ou 10 de la directive «police», le responsable du traitement ne peut pas refuser de rectifier ou d'effacer les données. En outre, le GT29 recommande aux États membres de définir également les catégories de traitement et les situations où les responsables du traitement ne seront jamais autorisés, partiellement ou complètement, à refuser de rectifier ou d'effacer les données ou à limiter le traitement. En effet, sans ces mesures nationales, les responsables du traitement seraient en position de décider eux-mêmes, sans d'autres critères, quand refuser de rectifier ou d'effacer les données, ou de limiter le traitement.

Les États membres devraient s'assurer que les responsables du traitement répondent toujours à une demande d'effacement ou de rectification et que si le droit est limité ou refusé, la personne concernée reçoit des informations concernant le droit d'introduire une réclamation auprès d'une autorité de contrôle ou la possibilité de former un recours juridictionnel. Étant donné que ces informations donneront lieu au seul droit applicable dans les cas où le droit à l'information selon laquelle les droits de rectification ou d'effacement ont été limités aura été lui-même limité, les informations fournies aux personnes concernées à ce sujet doivent l'être dans un délai raisonnable et de manière claire et compréhensible.

Le GT29 souhaite de nouveau rappeler aux législateurs nationaux que toute exemption des droits fondamentaux et des intérêts légitimes de la personne physique devrait être appliquée comme l'exception et non la règle et être interprétée de manière restrictive, comme le rappelle régulièrement la Cour européenne des droits de l'homme y compris en ce qui concerne les limitations des droits des personnes concernées dans le cadre d'un traitement relevant du champ d'application de la directive[12].

Lorsqu'un responsable du traitement constate que des données à caractère personnel sont inexactes, il doit s'assurer que la rectification de ces données est communiquée au responsable du traitement original qui a collecté les données à caractère personnel. En outre, le GT29 recommande que le responsable du traitement informe également la personne concernée de la rectification, de l'effacement ou de la limitation des données la concernant, conformément à ce qui est prévu à l'article 12, paragraphe 3.

Lorsque des données à caractère personnel sont rectifiées, effacées ou que le traitement est limité, le responsable du traitement doit en informer les destinataires de ces données. Ces destinataires doivent également rectifier, effacer ou limiter le traitement de ces données à caractère personnel. Étant donné que la directive n'indique pas le moment où ces informations devraient être envoyées, le GT29 souligne que ces informations devraient être communiquées le plus tôt possible afin d'éviter tout effet défavorable pour la personne concernée qui a exercé ses droits.

[12] Voir par exemple S. et Marper c. Royaume-Uni, CEDH, 2008, ou M.K c. France, CEDH, 2013.

6. *Accès indirect (article 17)*

Conformément à l'article 17, paragraphe 1, la législation nationale doit prévoir la possibilité que les droits d'information, d'accès ou d'information au sujet du refus de rectification ou d'effacement par le responsable du traitement soient exercés par l'intermédiaire de l'autorité de contrôle compétente quand ces droits ont été limités par le responsable du traitement sur la base des mesures législatives autorisant les limitations, et non lorsque ces droits pourraient être exercés directement auprès du responsable du traitement.

En outre, le GT29, conformément à sa recommandation de définir des catégories de traitement et des situations où le droit de rectification ou d'effacement sera limité complètement ou partiellement par les responsables du traitement (voir l'article 16, paragraphe 4, susmentionné) dans le cadre de mesures nationales, bien que ce ne soit pas expressément prévu par la directive, souhaite souligner que dans ces cas, la législation nationale devrait aussi prévoir que l'autorité de contrôle compétente puisse également exercer ces droits supplémentaires pour les personnes concernées.

Ce droit de faire exercer leurs droits par l'intermédiaire de l'autorité compétente doit être considéré comme une garantie supplémentaire offerte aux personnes concernées dans le cadre de la directive, lorsque le RGPD ne prévoit pas cette possibilité quand les droits auront été limités. Toutefois, le GT29 souligne que ce moyen supplémentaire d'exercer leurs droits vient compléter leur droit d'introduire une réclamation auprès d'une autorité de contrôle ou de former un recours juridictionnel.

Les responsables du traitement doivent informer les personnes concernées de la possibilité d'exercer leurs droits par l'intermédiaire de l'autorité de contrôle (article 17, paragraphe 2), et donc, afin de faciliter l'exercice de ce droit, ces informations devraient être claires, compréhensibles, communiquées le plus tôt possible par le responsable du traitement à la personne concernée, et comprendre les coordonnées de l'autorité de contrôle compétente.

En outre, les responsables du traitement devraient tenir des registres des demandes. Ces registres pourraient être tenus soit par le délégué à la protection des données, soit par l'autorité de protection des données. En outre, les autorités de protection des données devraient également consigner toutes les demandes d'accès indirect, par exemple dans un registre, afin de garder une trace de ces dernières et de collecter des données statistiques.

En vertu de l'article 17, paragraphe 3, les autorités de contrôle compétentes qui ont participé à l'exercice de ces droits doivent informer au moins la personne concernée du fait qu'elles ont procédé à toutes les vérifications nécessaires ou à un examen et que la personne concernée a le droit de former un recours juridictionnel. Le GT29

recommande que dans des circonstances ordinaires, ces informations soient fournies conjointement, y compris si possible les informations précises sur l'autorité judiciaire compétente, soit en donnant ses coordonnées et/ou la référence de la disposition juridique pertinente afin de faciliter les demandes des personnes concernées.

En outre, le GT29 rappelle que la possibilité, pour les personnes concernées, d'exercer leurs droits par l'intermédiaire de l'autorité de contrôle reste distincte du droit d'introduire une réclamation auprès de l'autorité de contrôle, dont doivent toujours disposer les personnes concernées, et doit être prévue en plus de ce dernier.

Recommandations du GT29

1. La directive prévoit une nouvelle architecture des droits des personnes concernées, le principe étant qu'elles ont un droit d'information, d'accès, de rectification, d'effacement ou de limitation du traitement, sauf si ces droits sont limités. Ces limitations sont possibles dès lors qu'elles constituent une mesure nécessaire et proportionnée et qu'elles sont interprétées de manière restrictive. Lorsque ces droits auront été limités, les États membres donneront la possibilité aux personnes concernées d'exercer leurs droits par l'intermédiaire de l'autorité de contrôle compétente, ce qui constitue une garantie supplémentaire pour les personnes concernées.

2. En vertu de la directive, les États membres doivent prévoir que la personne concernée a le droit d'obtenir du responsable du traitement la confirmation du traitement des données à caractère personnel la concernant et l'accès auxdites données. La directive n'autorise pas de limitations générales des droits de la personne concernée.

3. Les législateurs nationaux et les responsables du traitement devraient veiller à garantir dans la mesure du possible que des données précises sont traitées et que les demandes fondées de rectification des données sont traitées avec l'urgence nécessaire.

4. En plus du droit d'obtenir la limitation du traitement au lieu de l'effacement, les États membres devraient également prévoir un droit autonome à la limitation du traitement pour les personnes concernées dans leur législation nationale, notamment dans les cas où l'effacement aura été refusé par le responsable du traitement.

5. Les limitations du droit de rectification, d'effacement ou la limitation du traitement devraient être documentées et en cas de limitation du traitement, les données ne

devraient pas être envoyées à d'autres responsables du traitement tant que la limitation n'est pas levée.

6. Dans les cas où il est établi que les données sont inexactes ou incomplètes, ou que les données sont traitées en violation des articles 4, 8 ou 10 de la directive, le responsable du traitement ne peut pas refuser la rectification ou l'effacement des données.

7. La directive ne prévoit expressément que la possibilité, pour les États membres, de limiter les informations à fournir par le responsable du traitement en cas de refus de rectifier ou d'effacer les données ou de limiter le traitement. Toutefois, les États membres devraient également définir les catégories de traitement et les situations où les responsables du traitement ne seront jamais autorisés, partiellement ou complètement, à refuser de rectifier ou d'effacer les données ou à limiter le traitement.

8. La possibilité pour les personnes concernées d'exercer leurs droits reste complémentaire de leur droit d'introduire une réclamation auprès d'une autorité de contrôle ou de former un recours juridictionnel.

9. Les responsables du traitement et les autorités de protection des données devraient tenir des registres des demandes.

10. Lorsque les autorités de contrôle compétentes exercent leurs droits pour le compte des personnes concernées, elles doivent informer au moins la personne concernée du fait qu'elles ont procédé à toutes les vérifications nécessaires ou à un examen et que la personne concernée a le droit de former un recours juridictionnel. Dans des circonstances ordinaires, ces informations devraient être données conjointement.

Article 25
Journalisation

Sujets clés

1. Objectif des journaux
2. Contenu des journaux et motif de l'accès
3. Utilisation des journaux pour les procédures pénales
4. Durée de conservation des journaux
5. Archivage des journaux

1. Objectif des journaux

Selon l'article 25, les législations nationales devraient prévoir l'obligation d'établir des journaux au moins pour les opérations de traitement telles que la collecte, la modification, la consultation, la communication, y compris les transferts, l'interconnexion et l'effacement effectués dans des systèmes de traitement automatisé.

En outre, pour les opérations de consultation et de communication, les journaux permettent d'établir le motif, la date et l'heure de celles-ci et, dans la mesure du possible, l'identification de la personne qui a consulté ou communiqué les données à caractère personnel, ainsi que l'identité des destinataires de ces données à caractère personnel.

La mise en œuvre des journaux est un outil essentiel pour contrôler la protection des données, et donc pour contrôler toutes les opérations pertinentes de traitement des données. Pour ce faire, il devrait être possible de suivre l'activité des utilisateurs afin de détecter les cas d'utilisation abusive. Les législations nationales devraient ensuite renforcer les exigences en matière de journalisation: sur le contenu, sur les durées de conservation, sur les mesures techniques, sur l'auto-audit et sur les politiques internes en vue d'encourager le respect des règles.
Compte tenu de l'objectif des journaux, les législations nationales devraient prévoir l'adoption de mesures techniques afin de garantir l'intégrité des journaux; ils pourraient sinon devenir inutiles.

La journalisation a un double objectif dans la mesure où elle peut servir de mesure dissuasive d'une utilisation non autorisée, qui peut être uniquement efficace si une règle d'analyse des journaux est appliquée, et de mesure punitive en cas d'infraction. Par conséquent, il convient de tenir compte d'un autre aspect, à savoir le renforcement de l'activité d'auto-audit des responsables du traitement dans le cadre de rapports périodiques d'analyse des journaux, qui pourrait être effectuée de manière automatisée et adaptée à des domaines spécifiques des opérations de répression.

2. Contenu des journaux et motif de l'accès

Les contenus nécessaires des journaux des opérations de consultation et communication devraient permettre d'établir non seulement la date et l'heure de celles-ci, mais également le motif et l'identification de la personne qui a consulté ou communiqué les données et l'identité du destinataire en cas de communication.

Le GT29 considère que l'identification de l'utilisateur individuel ne devrait pas se limiter aux opérations de consultation et de communication, mais être prévue pour toutes les opérations de traitement et comprendre toutes les personnes impliquées, par exemple les activités d'une organisation extérieure qui participe à la résolution des problèmes ou aux activités judiciaires.

Concernant l'obligation de permettre d'établir le motif des opérations de consultation et de communication, le contenu des journaux dépendra dans une certaine mesure du système ou de l'application les générant. Étant donné que cet aspect sera déterminé dans le cadre de différentes configurations nationales, la directive ne donne pas plus de précisions. Toutefois, au final, les journaux doivent contenir des éléments expliquant

pourquoi un individu a eu accès à ce journal ou registre. Le GT29 considère que la meilleure façon de remplir cette obligation consiste à garantir que les systèmes de traitement automatisé et leurs éléments de journalisation respectifs sont développés conformément aux exigences de «protection des données dès la conception» définies à l'article 20 de la directive. Les exigences en matière de journalisation de l'article 25 devraient donc être prises en compte dans la conception du système d'accès à la base de données, au système ou à l'application. La personne qui consulte des données spécifiques pourrait être contrainte de donner une explication avant d'obtenir l'accès, de sorte que le contenu de cette explication puisse être transféré dans les journaux en tant que motif. Dans tous les cas, cette obligation est compliquée d'un point de vue technique et nécessite une certaine préparation. C'est la raison pour laquelle le législateur a prévu un délai d'application plus long pour se conformer aux dispositions de l'article 25, paragraphe 2.

3. Utilisation des journaux pour les procédures pénales

L'article 25, paragraphe 2, définit les seules finalités pour lesquelles les journaux peuvent être utilisés. Hormis la vérification de la licéité du traitement, l'autocontrôle et la garantie de l'intégrité et de la sécurité des données à caractère personnel, les journaux peuvent également être utilisés à des fins de procédures pénales.

Compte tenu de l'utilisation très limitée et précise des journaux et, par conséquent, du système d'accès très limité aux journaux, le GT29 interprète la disposition prévoyant l'utilisation des journaux à des fins de procédures pénales pour tous les cas où ces procédures sont liées aux finalités des journaux susmentionnées. Il s'agit d'une hypothèse logique dans la mesure où toute pratique illicite en matière de traitement des données détectée dans le cadre de l'analyse des journaux est susceptible de faire l'objet de procédures pénales.

Par conséquent, sans préjudice des pouvoirs des autorités judiciaires dans l'exercice de leurs capacités, il devrait être considéré comme approprié d'utiliser les journaux dans des procédures pénales lorsque la licéité d'une opération de traitement des données - par exemple la consultation ou la communication des données - est contestée, lorsqu'il existe une violation de la sécurité ou si l'intégrité des données est en jeu.

En conclusion, l'article 25, paragraphe 2, devrait être interprété de manière restrictive concernant l'utilisation des journaux, en gardant à l'esprit les objectifs réels de ces derniers et la nécessité potentielle de mener des enquêtes et des poursuites en cas de violation des données.

4. Durée de conservation des journaux

La directive ne prévoit aucune exigence concernant la durée de conservation des journaux. Par conséquent, le GT29 considère que les législateurs nationaux devraient prévoir des durées de conservation appropriées en définissant des critères clairs ou des délais fixes.

Il convient d'établir la durée de conservation appropriée des journaux à partir des finalités de la journalisation, conformément à l'article 25, paragraphe 2, et de garantir qu'il est possible d'atteindre ces finalités. Cela vaut particulièrement pour la vérification de la licéité du traitement, qui figure parmi les tâches des autorités de protection des données. Par conséquent, la durée de conservation des journaux devrait donner suffisamment de temps aux autorités de protection des données pour retracer et examiner le traitement des données.

Le GT29 considère que le contrôle de l'accès aux données, c'est-à-dire la consultation et la communication, devrait être effectué régulièrement et dans de brefs délais. En général, il n'est pas nécessaire de tenir des journaux sur l'accès tant que les données sous-jacentes sont conservées.

S'agissant des journaux sur l'historique des données, c'est-à-dire la collecte, la modification, l'interconnexion et l'effacement, une approche différente peut être appropriée en fonction de la base de données en question[13].

Pour définir des durées de conservation appropriées, il convient de tenir compte du fait qu'une longue durée de conservation des journaux permettra de garder une trace de l'historique du traitement (ce qui profitera à la personne concernée, à la qualité des données et aux mesures de sécurité). Dans les procédures pénales ou à des fins préventives, les données sous-jacentes sont généralement conservées longtemps et la personne concernée n'est souvent informée du traitement qu'à un stade ultérieur. À ce stade, il devrait être possible de retracer le traitement des données au moyen des journaux. Par ailleurs, conserver les journaux après la suppression des données sous-jacentes implique de conserver également une partie des informations plus longtemps que la durée de conservation prévue, ce qui nécessiterait de raccourcir la durée de conservation des journaux. En conclusion, il convient de trouver le juste équilibre au cas par cas.

5. Archivage des journaux

[13] Par exemple, dans le cadre du système SIS II, il existe un régime différent de durées de conservation des journaux concernant les alertes et de ceux concernant l'accès effectué par des personnes. Les journaux concernant l'accès effectué par des personnes doivent être supprimés au plus tôt un an après leur création, et au plus tard après trois ans. En revanche, les journaux sur l'historique des alertes doivent être effacés entre un et trois ans après la suppression de l'alerte concernée. La convention Europol a choisi une autre approche, qui prévoit la suppression de tous les journaux après trois ans, quelle que soit l'opération de traitement sous-jacente.

En outre, il est possible que la durée de conservation appropriée des journaux soit différente de celle que la source originale des journaux peut assurer. Dans ces cas, il convient d'envisager l'archivage des journaux et - en fonction du contexte - ce dernier peut même être requis (pour satisfaire, par exemple, à d'autres exigences de la directive). Il peut exister, par exemple, une durée limitée de conservation des journaux dans le cadre d'un système ou d'une application en particulier avant qu'ils ne soient écrasés, soit en raison du temps ou de l'espace de stockage; archiver ce qui est nécessaire aux fins de la directive peut donc être un moyen de garantir que les responsables du traitement conservent les informations requises le temps nécessaire.

Recommandations du GT29

1. Les législations nationales devraient renforcer les exigences en matière de journalisation: sur le contenu, sur les durées de conservation, sur les mesures techniques, sur l'auto-audit et sur les politiques internes en vue d'encourager le respect des règles.

2. Le GT29 considère que l'identification de l'utilisateur ne devrait pas se limiter aux opérations de consultation et de communication, mais être prévue pour toutes les opérations de traitement. L'exigence de journalisation concernant le motif de consultation et de communication devrait être appliquée lors de la conception technique du système source et de son système d'accès (protection des données dès la conception).

3. Sans préjudice des pouvoirs des autorités judiciaires dans l'exercice de leurs capacités, il devrait être considéré comme approprié d'utiliser les journaux dans des procédures pénales uniquement lorsque la licéité d'une opération de traitement des données - par exemple la consultation ou la communication des données - est contestée, lorsqu'il existe une violation de la sécurité ou si l'intégrité des données est en jeu. L'utilisation des journaux pour tout autre type de procédures pénales serait excessive et pourrait nuire aux objectifs réels de l'activité de journalisation.

4. Pour décider de durées de conservation appropriées, il convient de trouver le juste équilibre, au cas par cas, en fonction de la base de données en question et en tenant compte, d'une part, du fait qu'une longue durée de conservation des journaux permettra de garder une trace de l'historique du traitement et, de l'autre, qu'en cas de conservation des journaux plus longtemps que les données sous-jacentes, une partie des informations est conservée encore plus longtemps.

5. L'utilisation de l'archivage des journaux devrait être prévue lorsque la source originale des journaux ne peut assurer la durée de conservation appropriée des journaux.

Article 47
Pouvoirs des autorités de protection des données

Sujets clés
1. Pouvoirs effectifs
2. Contrôle commun de la directive et du RGPD

1. Pouvoirs effectifs

Selon l'article 47, les États membres doivent prévoir, par la loi, que les autorités de protection des données disposent de pouvoirs d'enquête effectifs (article 47, paragraphe 1), de pouvoirs effectifs en matière d'adoption de mesures correctrices (article 47, paragraphe 2) et de pouvoirs consultatifs effectifs (article 47, paragraphe 3), ainsi que du pouvoir de porter les violations des dispositions adoptées en vertu de la présente directive à la connaissance des autorités judiciaires et, le cas échéant, d'ester en justice d'une manière ou d'une autre, en vue de faire respecter les dispositions adoptées en vertu de la présente directive.

Contrairement au RGPD, la directive n'énumère ni ne définit les pouvoirs d'enquête, les pouvoirs en matière d'adoption de mesures correctrices et les pouvoirs consultatifs. Le GT29 considère que le RGPD et la directive devraient néanmoins fournir un niveau de protection similaire et donc des règles équivalentes sur les questions clés. Par conséquent, le GT29 recommande que les législations nationales transposant la directive réglementent ces pouvoirs de la même façon que le RGPD, dans la mesure du possible.

S'agissant des pouvoirs en matière d'adoption de mesures correctrices, l'article 47, paragraphe 2, ne cite que des exemples de la nature possible de ces pouvoirs, à savoir le pouvoir d'ordonner l'effacement ou la rectification des données ou de limiter ou d'interdire un traitement, et l'attribut essentiel consistant à être «effectifs». Le GT29 considère que cet attribut nécessite des pouvoirs contraignants des autorités de protection des données pour prévenir, imposer ou ordonner certaines mesures correctrices et émettre des décisions contraignantes à l'encontre des responsables du traitement. Les autorités de protection des données ne sont généralement pas limitées à des actes non contraignants et non applicables tels que des réclamations ou objections pures. Dans ces cas, la mise en œuvre nationale de la directive doit être considérée comme insuffisante.

Le GT29 estime que l'absence de mesures correctrices ne peut être compensée par le fait de prévoir que chaque autorité de contrôle ait le pouvoir de porter les violations des dispositions adoptées en vertu de la présente directive à la connaissance des autorités

judiciaires et, le cas échéant, d'ester en justice d'une manière ou d'une autre, conformément à l'article 47, paragraphe 5. Ces procédures judiciaires sont censées être des instruments complémentaires, et non alternatifs à des pouvoirs effectifs en matière d'adoption de mesures correctrices.

En outre, le GT29 souhaite rappeler l'arrêt Schrems de la CJUE du 6 octobre 2015, C-362/14. Selon le paragraphe 65 de cet arrêt, lorsqu'elle examine une réclamation contre des transferts de données fondés sur une décision d'adéquation et qu'elle estime les griefs fondés, l'autorité nationale de contrôle compétente doit avoir le pouvoir de faire valoir ces griefs devant les juridictions nationales afin que ces dernières procèdent, si elles partagent les doutes de cette autorité quant à la validité de la décision de la Commission, à un renvoi préjudiciel aux fins de l'examen de la validité de cette décision. À la lumière de cet arrêt, lorsque des réclamations concernent la validité des décisions d'adéquation, le législateur national doit prévoir que les autorités de contrôle disposent du pouvoir de porter l'affaire devant une juridiction. Cela vaut également pour les décisions d'adéquation fondées sur l'article 36 de la directive «police».

2. Contrôle commun de la directive et du RGPD

Un autre aspect pouvant affecter considérablement l'efficacité du contrôle est la décision nationale de chaque État membre d'établir une autorité de protection des données distincte pour la directive. Conformément à l'article 41, paragraphe 3, les États membres peuvent prévoir qu'une autorité de contrôle instituée au titre du RGPD est l'autorité de contrôle visée dans la directive. Le GT29 considère qu'une telle approche devrait être fortement encouragée.

Confier à une seule autorité de protection des données le contrôle du RGPD et de la directive garantira que les principes et concepts communs aux deux actes juridiques sont interprétés de manière homogène et assurera la cohérence de la politique et de la pratique en matière de protection des données. En outre, le choix d'une seule autorité de contrôle assouplira le fonctionnement du comité européen de la protection des données et évitera le risque de mobiliser davantage les ressources financières et humaines limitées des autorités de protection des données.

Cela n'affecte en rien la possibilité, pour certains États membres, d'établir plusieurs autorités de contrôle afin de refléter leur structure constitutionnelle, à savoir les États fédéraux.

Recommandations du GT29

1. Les législations nationales doivent prévoir des pouvoirs d'enquête, des pouvoirs en matière d'adoption de mesures correctrices et des pouvoirs consultatifs effectifs, ainsi que le pouvoir de porter les violations à la connaissance des autorités

judiciaires et, le cas échéant, d'ester en justice d'une manière ou d'une autre. Le GT29 recommande que les législations nationales détaillent les pouvoirs des autorités de protection des données conformément aux pouvoirs prévus dans le RGPD. Lorsque des réclamations concernent la validité des décisions d'adéquation fondées sur l'article 36 de la directive, le législateur national doit prévoir un moyen direct de porter l'affaire devant une cour.

2. Les États membres devraient confier à une seule autorité de protection des données le contrôle du RGPD et de la directive. Cela n'affecte en rien la possibilité, pour certains États membres, de refléter leur structure constitutionnelle, à savoir les États fédéraux.