Affaire C-60/22

Demande de décision préjudicielle

Date de dépôt :

1er février 2022

Juridiction de renvoi :

Verwaltungsgericht Wiesbaden (Allemagne)

Date de la décision de renvoi :

27 janvier 2022

Partie requérante :

UZ

Partie défenderesse :

Bundesrepublik Deutschland

[omissis]

VERWALTUNGSGERICHT WIESBADEN

(Tribunal administratif de Wiesbaden, Allemagne)

ORDONNANCE

Dans le cadre de la procédure administrative contentieuse

UZ, [omissis]

[omissis]

[omissis] Kelkheim (Taunus)

Partie requérante

[omissis]

contre

Bundesrepublik Deutschland (République fédérale d'Allemagne)
[omissis]

Partie défenderesse

concernant

le droit d'asile,

le Verwaltungsgericht Wiesbaden (tribunal administratif de Wiesbaden) [omissis]

[omissis]

a ordonné ce qui suit le 27 janvier 2022 :

I. Il est sursis à statuer.

II. La procédure est déférée à la Cour de justice de l'Union européenne, conformément à l'article 267 TFUE, en vue d'une décision à titre préjudiciel sur les questions suivantes :

1. Le manquement du responsable du traitement à tout ou partie de la responsabilité qui lui incombe conformément à l'article 5 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données ou RGPD), résultant, par exemple, de l'absence de registre – ou de registre complet – des activités de traitement au sens de l'article 30 du RGPD ou de l'absence d'accord définissant une procédure conjointe en application de l'article 26 du RGPD, a-t-il pour conséquence que le traitement des données est illicite au sens de l'article 17, paragraphe 1, sous d), du RGPD et de l'article 18, paragraphe 1, sous b), du RGPD, de sorte que la personne concernée dispose d'un droit à l'effacement ou d'un droit à la limitation du traitement ?

2. **En cas de réponse affirmative à la première question : L'existence d'un droit à l'effacement ou d'un droit à la limitation du traitement a-t-elle pour conséquence que les données traitées ne peuvent être prises en compte dans le cadre d'une procédure juridictionnelle ? Cette conséquence s'applique-t-elle en tout cas lorsque la personne concernée s'oppose à leur utilisation dans le cadre de la procédure juridictionnelle ?**

3. **En cas de réponse négative à la première question : La violation des articles 5, 30 ou 26 du RGPD par un responsable du traitement a-t-elle pour conséquence, s'agissant de la question de l'utilisation du traitement des données dans le cadre d'une procédure juridictionnelle, qu'une juridiction nationale n'est autorisée à prendre ces données en compte que si la personne concernée consent expressément à cette utilisation ?**

I.

1 Dans la présente affaire, le requérant conteste une décision de rejet du Bundesamt für Migration und Flüchtlinge (Office fédéral des migrations et des réfugiés, ci-après également l'« Office fédéral ») et sollicite l'octroi du statut de réfugié en application de l'article 3 de l'Asylgesetz (loi sur l'asile). La défenderesse a fondé sa décision sur le dossier électronique « MARIS », dossier de l'Office fédéral qui est également transmis au tribunal, dans le cadre d'une procédure conjointe au titre de l'article 26, via l'Elektronische Gerichts-und Verwaltungspostfach, la boîte postale électronique judiciaire et administrative (ci-après également l'« EGVP »). Nous renvoyons, s'agissant des questions concernant la transmission intégrale des dossiers, aux questions préjudicielles dont la Cour a déjà été saisie dans l'affaire C-564/21 par ordonnance 3 septembre 2021 du Verwaltungsgericht Wiesbaden (tribunal administratif de Wiesbaden) [omissis].

2 Le tribunal de céans doute en l'espèce de l'existence d'un registre (complet) des activités de traitement tenu par la défenderesse et concernant le dossier électronique « MARIS ». Il n'existe pas non plus d'accord ou de disposition de loi qui régirait la procédure de transmission électronique du dossier et la détermination des responsabilités dans le cadre de cette procédure. Ces documents ont été demandés par le tribunal de céans au cours de l'instance. La défenderesse a cependant refusé de les produire, dans la mesure notamment où aucun accord fondé sur l'article 26 du RGPD ne s'applique à l'EGVP.

3 La question se pose donc de savoir comment le tribunal doit procéder, à tout le moins lorsque les données à caractère personnel du requérant ont fait l'objet d'un traitement (formellement) illicite de la défenderesse. En effet, en vertu de la directive 2013/32/UE du Parlement européen et du Conseil du 26 juin 2013 [relative à des procédures communes pour l'octroi et le retrait de la protection internationale (refonte)] (JO L 180 du 29 juin 2013, p. 60), le RGPD

s'applique aux procédures d'asile régies par le droit national. Ni la loi sur l'asile ni le code de procédure administrative ne contiennent de disposition à ce sujet.

II.

1. Charte des droits fondamentaux de l'Union européenne (ci-après la « Charte »)

4 Article 7 de la Charte

Respect de la vie privée et familiale

Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications.

5 Article 8 de la Charte

Protection des données à caractère personnel

1. Toute personne a droit à la protection des données à caractère personnel la concernant.

2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.

3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante.

2. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données – ci-après le « RGPD » ; JO du 4 mai 2016, L 119, p. 1).

6 Considérant 82

Afin de démontrer qu'il respecte le présent règlement, le responsable du traitement ou le sous-traitant devrait tenir des registres pour les activités de traitement relevant de sa responsabilité. Chaque responsable du traitement et sous-traitant devrait être tenu de coopérer avec l'autorité de contrôle et de mettre ces registres à la disposition de celle-ci, sur demande, pour qu'ils servent au contrôle des opérations de traitement.

7 Article 5 du RGPD

Principes relatifs au traitement des données à caractère personnel

1. Les données à caractère personnel doivent être :

a) traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence) ;

b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités ; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales (limitation des finalités) ;

c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ;

d) exactes et, si nécessaire, tenues à jour ; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude) ;

e) 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 ; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation) ;

f) traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité) ;

2. Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté (responsabilité).

8 Article 9 du RGPD

Traitement portant sur des catégories particulières de données à caractère personnel

1. Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des

données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits.

2. Le paragraphe 1 ne s'applique pas si l'une des conditions suivantes est remplie :

a) la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques, sauf lorsque le droit de l'Union ou le droit de l'État membre prévoit que l'interdiction visée au paragraphe 1 ne peut pas être levée par la personne concernée ;

b) le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale, dans la mesure où ce traitement est autorisé par le droit de l'Union, par le droit d'un État membre ou par une convention collective conclue en vertu du droit d'un État membre qui prévoit des garanties appropriées pour les droits fondamentaux et les intérêts de la personne concernée ;

c) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique, dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ;

d) le traitement est effectué, dans le cadre de leurs activités légitimes et moyennant les garanties appropriées, par une fondation, une association ou tout autre organisme à but non lucratif et poursuivant une finalité politique, philosophique, religieuse ou syndicale, à condition que ledit traitement se rapporte exclusivement aux membres ou aux anciens membres dudit organisme ou aux personnes entretenant avec celui-ci des contacts réguliers en liaison avec ses finalités et que les données à caractère personnel ne soient pas communiquées en dehors de cet organisme sans le consentement des personnes concernées ;

e) le traitement porte sur des données à caractère personnel qui sont manifestement rendues publiques par la personne concernée ;

f) le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ou chaque fois que des juridictions agissent dans le cadre de leur fonction juridictionnelle ;

g) le traitement est nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la

protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée ;

h) le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale sur la base du droit de l'Union, du droit d'un État membre ou en vertu d'un contrat conclu avec un professionnel de la santé et soumis aux conditions et garanties visées au paragraphe 3 ;

i) le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux, sur la base du droit de l'Union ou du droit de l'État membre qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel ;

j) le traitement est nécessaire à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, conformément à l'article 89, paragraphe 1, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée.

3. Les données à caractère personnel visées au paragraphe 1 peuvent faire l'objet d'un traitement aux fins prévues au paragraphe 2, point h), si ces données sont traitées par un professionnel de la santé soumis à une obligation de secret professionnel conformément au droit de l'Union, au droit d'un État membre ou aux règles arrêtées par les organismes nationaux compétents, ou sous sa responsabilité, ou par une autre personne également soumise à une obligation de secret conformément au droit de l'Union ou au droit d'un État membre ou aux règles arrêtées par les organismes nationaux compétents.

4. Les États membres peuvent maintenir ou introduire des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement des données génétiques, des données biométriques ou des données concernant la santé.

9 Article 17 du RGPD

Droit à l'effacement (« droit à l'oubli »)

1. La personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais, lorsque l'un des motifs suivants s'applique :

a) les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière ;

b) la personne concernée retire le consentement sur lequel est fondé le traitement, conformément à l'article 6, paragraphe 1, point a), ou à l'article 9, paragraphe 2, point a), et il n'existe pas d'autre fondement juridique au traitement ;

c) la personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 1, et il n'existe pas de motif légitime impérieux pour le traitement, ou la personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 2 ;

d) les données à caractère personnel ont fait l'objet d'un traitement illicite ;

e) les données à caractère personnel doivent être effacées pour respecter une obligation légale qui est prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis ;

f) les données à caractère personnel ont été collectées dans le cadre de l'offre de services de la société de l'information visée à l'article 8, paragraphe 1.

2. Lorsqu'il a rendu publiques les données à caractère personnel et qu'il est tenu de les effacer en vertu du paragraphe 1, le responsable du traitement, compte tenu des technologies disponibles et des coûts de mise en œuvre, prend des mesures raisonnables, y compris d'ordre technique, pour informer les responsables du traitement qui traitent ces données à caractère personnel que la personne concernée a demandé l'effacement par ces responsables du traitement de tout lien vers ces données à caractère personnel, ou de toute copie ou reproduction de celles-ci.

10 Article 18 du RGPD

Droit à la limitation du traitement

1. La personne concernée a le droit d'obtenir du responsable du traitement la limitation du traitement lorsque l'un des éléments suivants s'applique :

a) l'exactitude des données à caractère personnel est contestée par la personne concernée, pendant une durée permettant au responsable du traitement de vérifier l'exactitude des données à caractère personnel ;

b) le traitement est illicite et la personne concernée s'oppose à leur effacement et exige à la place la limitation de leur utilisation ;

c) le responsable du traitement n'a plus besoin des données à caractère personnel aux fins du traitement mais celles-ci sont encore nécessaires à la personne concernée pour la constatation, l'exercice ou la défense de droits en justice ;

d) la personne concernée s'est opposée au traitement en vertu de l'article 21, paragraphe 1, pendant la vérification portant sur le point de savoir si les motifs légitimes poursuivis par le responsable du traitement prévalent sur ceux de la personne concernée.

2. Lorsque le traitement a été limité en vertu du paragraphe 1, ces données à caractère personnel ne peuvent, à l'exception de la conservation, être traitées qu'avec le consentement de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice, ou pour la protection des droits d'une autre personne physique ou morale, ou encore pour des motifs importants d'intérêt public de l'Union ou d'un État membre.

3. Une personne concernée qui a obtenu la limitation du traitement en vertu du paragraphe 1 est informée par le responsable du traitement avant que la limitation du traitement ne soit levée.

11 Article 26 du RGPD

Responsables conjoints du traitement

1. Lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement. Les responsables conjoints du traitement définissent de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences du présent règlement, notamment en ce qui concerne l'exercice des droits de la personne concernée, et leurs obligations respectives quant à la communication des informations visées aux articles 13 et 14, par voie d'accord entre eux, sauf si, et dans la mesure, où leurs obligations respectives sont définies par le droit de l'Union ou par le droit de l'État membre auquel les responsables du traitement sont soumis. Un point de contact pour les personnes concernées peut être désigné dans l'accord.

2. L'accord visé au paragraphe 1 reflète dûment les rôles respectifs des responsables conjoints du traitement et leurs relations vis-à-vis des personnes concernées. Les grandes lignes de l'accord sont mises à la disposition de la personne concernée.

3. Indépendamment des termes de l'accord visé au paragraphe 1, la personne concernée peut exercer les droits que lui confère le présent règlement à l'égard de et contre chacun des responsables du traitement.

12 Article 30 du RGPD

Registre des activités de traitement

1. Chaque responsable du traitement et, le cas échéant, le représentant du responsable du traitement tiennent un registre des activités de traitement effectuées sous leur responsabilité. Ce registre comporte toutes les informations suivantes :

a) le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données ;

b) les finalités du traitement ;

c) une description des catégories de personnes concernées et des catégories de données à caractère personnel ;

d) les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales ;

e) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa, les documents attestant de l'existence de garanties appropriées ;

f) dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données ;

g) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, paragraphe 1.

2. Chaque sous-traitant et, le cas échéant, le représentant du sous-traitant tiennent un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement, comprenant :

a) le nom et les coordonnées du ou des sous-traitants et de chaque responsable du traitement pour le compte duquel le sous-traitant agit ainsi que, le cas échéant, les noms et les coordonnées du représentant du responsable du traitement ou du sous-traitant et celles du délégué à la protection des données ;

b) les catégories de traitements effectués pour le compte de chaque responsable du traitement ;

c) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa, les documents attestant de l'existence de garanties appropriées ;

d) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, paragraphe 1.

3. Les registres visés aux paragraphes 1 et 2 se présentent sous une forme écrite y compris la forme électronique.

4. Le responsable du traitement ou le sous-traitant et, le cas échéant, leur représentant mettent le registre à la disposition de l'autorité de contrôle sur demande.

5. Les obligations visées aux paragraphes 1 et 2 ne s'appliquent pas à une entreprise ou à une organisation comptant moins de 250 employés, sauf si le traitement qu'elles effectuent est susceptible de comporter un risque pour les droits et des libertés des personnes concernées, s'il n'est pas occasionnel ou s'il porte notamment sur les catégories particulières de données visées à l'article 9, paragraphe 1, ou sur des données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10.

13 Article 94

Abrogation de la directive 95/46/CE

1. La directive 95/46/CE est abrogée avec effet au 25 mai 2018.

2. Les références faites à la directive abrogée s'entendent comme faites au présent règlement. Les références faites au groupe de protection des personnes à l'égard du traitement des données à caractère personnel institué par l'article 29 de la directive 95/46/CE s'entendent comme faites au comité européen de la protection des données institué par le présent règlement.

3. DIRECTIVE 2013/32/UE DU PARLEMENT EUROPÉEN ET DU CONSEIL du 26 juin 2013 relative à des procédures communes pour l'octroi et le retrait de la protection internationale (JO L 338 du 30 décembre 2013, L 180 p. 60)

14 Considérant 52

La directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du

traitement des données à caractère personnel et à la libre circulation de ces données (7) régit le traitement des données à caractère personnel effectué dans les États membres en vertu de la présente directive.

4. Bundesdatenschutzgesetz (loi fédérale relative à la protection des données) ci-après également le « BDSG » [introduite par l'article 1er du Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (loi d'adaptation du droit de la protection des données au règlement (UE) 2016/679 et de transposition de la directive (UE) 2016/680 (Datenschutz-Anpassungs – und-Umsetzungsgesetz EU – DSAnpUG-EU du 30 juin 2017, BGBl. I, p. 2097)].

15 **Article 43, paragraphe 3, du BDSG**

Dispositions relatives aux amendes administratives

[…]

3. Aucune amende administrative ne peut être infligée aux autorités publiques et autres organismes publics au sens de l'article 2, paragraphe 1.

III.

16 Il ressort du considérant 52 de la directive 2013/32 que le traitement des données à caractère personnel effectué par les États membres en vertu de cette directive dans le cadre des procédures d'asile est régi par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. La directive 95/46 a été abrogée avec effet au 25 mai 2018 (voir article 94, paragraphe 1, du RGPD). Les références faites à la directive 95/46 abrogée s'entendent toutefois comme des références au RGPD (voir article 94, paragraphe [2], du RGPD). Par conséquent, le RGPD s'applique pleinement aux procédures d'octroi d'une protection internationale.

17 La directive 95/46 prévoyait déjà une documentation des traitements automatisés, qualifiée de « notification » (voir article 18 de la directive 94/46). Le contenu de cette notification, tel qu'il découlait de l'article 19 de la directive 95/46, correspondait pour l'essentiel à l'actuel article 30 du RGPD, la nouvelle norme s'appliquant à toutes les formes de traitement, et donc également aux systèmes de fichiers.

18 Sous l'empire de la directive 95/46, la défenderesse disposait uniquement, à titre de notification au sens de la directive 95/46 (article 4e du BDSG ancienne version), d'un registre de traitement très rudimentaire concernant le dossier électronique MARIS. À l'époque, le registre de traitement (la notification) ne contenait aucune règle spécifique sur le traitement de catégories particulières de

données à caractère personnel conformément à l'article 9 du RGPD (article 8 de la directive 95/46). Il n'existe probablement pas non plus, à ce jour, de règles spécifiques concernant le traitement des données conformément aux articles 9 et 10 du RGPD. En effet, les données relatives à la santé, ainsi que celles concernant les convictions religieuses, de même que les condamnations pénales, sont intégrées de façon générale au dossier électronique MARIS en tant que « documents normaux ». Il n'apparaît pas que la sécurité des données fasse l'objet d'une protection particulière, si ce n'est qu'il existe probablement un système de journalisation des accès. Cependant, le dossier d'un demandeur d'asile peut être consulté dans toute l'Allemagne, depuis n'importe quelle antenne extérieure de la défenderesse de même que depuis les services centraux.

19 S'agissant précisément de la tenue des dossiers et de leur production en justice, le tribunal de céans doute sérieusement que la défenderesse respecte les dispositions combinées de l'article 5, paragraphe 1, du RGPD, et, notamment, des articles 26 et 30 du RGPD. Contrairement à ce qu'avait exigé le tribunal de céans, le registre des activités de traitement n'a pas été produit. Il est prévu à cet égard d'entendre le directeur de l'administration responsable, c'est-à-dire de la défenderesse, sur la question de sa responsabilité en vertu de l'article 5, paragraphe 2, du RGPD, après que la Cour aura statué.

20 Avant de procéder à une audition, il convient cependant de déterminer si le non-respect des obligations prévues par le RGPD et l'illicéité du traitement des données qui en découle doivent être sanctionnés, notamment par l'effacement des données, conformément à l'article 17, paragraphe 1, sous d), du RGPD ou par une limitation du traitement, conformément à l'article 18, paragraphe 1, sous b), du RGPD. Cette possibilité de sanction doit à tout le moins être envisagée s'il s'agit d'une demande de la personne concernée, en l'occurrence le requérant. En effet, le tribunal se verrait autrement contraint de participer à un traitement illicite de données dans le cadre de la procédure juridictionnelle. L'administration serait en mesure d'enfreindre le RGPD sans jamais être sanctionnée.

21 Dans un tel cas, seule l'autorité de contrôle pourrait agir en vertu de l'article 58 du RGPD. Il n'est cependant pas possible, aux termes du droit national, d'imposer une amende administrative aux autorités publiques. Conformément à l'article 43, paragraphe 3, du BDSG – fondé sur l'article 83, paragraphe 7, du RGPD – aucune amende administrative ne peut être infligée aux autorités publiques et autres organismes publics. Rien n'inciterait l'administration à respecter les règles. Cela aurait pour conséquence que les prescriptions de la directive 2013/32 ne seraient pas plus respectées que le RGPD lui-même.

22 La Cour a déjà eu l'occasion de juger que la « notification » (c'est-à-dire, désormais, le registre des activités de traitement) complète doit être prête au moment du traitement, mais pas avant (arrêt du 9 novembre 2011, Volker und Markus Schecke et Eifert, C-92/09 et C-93/09, EU:C:2010:662, points 95 et suivants). En l'espèce, le traitement des données à caractère personnel du requérant par la défenderesse remonte déjà à la date d'introduction de la demande

d'asile, le 7 mai 2019. Par conséquent, si l'on s'en tient en tout cas à la jurisprudence de la Cour, un registre complet des activités de traitement concernant le dossier MARIS (et donc les dossiers d'asile du requérant) devrait avoir été établi au moment du traitement, c'est-à-dire au moment où le requérant a introduit sa demande d'asile ; ce n'est cependant pas le cas.

23 La Cour n'a pas encore précisé quelles étaient les règles applicables dans un tel cas, que ce soit sur le fondement de la directive 95/46 ou sur le fondement du RGPD. Dès lors que pour démontrer qu'il se conforme au RGPD, le responsable du traitement ou le sous-traitant doit tenir des registres pour les activités de traitement relevant de sa responsabilité (considérant 82 du RGPD), on ne peut que s'interroger sur les conséquences d'un manquement de l'entité responsable du traitement à cet égard. En effet, dans ce cas, la responsabilité énoncée à l'article 5 du RGPD ne peut être respectée.

24 L'article 83, paragraphe 5, sous a), du RGPD prévoit certes qu'une violation des dispositions relatives à la responsabilité énoncées à l'article 5 du RGPD peut être sanctionnée par une amende administrative d'un montant maximal de 20 000 000 EUR. Cependant, comme nous l'avons déjà indiqué, cette possibilité est exclue pour les autorités administratives fédérales, en vertu de l'article 43, paragraphe 3, du BSDG. L'article 17, paragraphe 1, sous d), du RGPD prévoit néanmoins que les données ayant fait l'objet d'un traitement illicite doivent être effacées dès lors que la personne concernée le demande.

25 La juridiction de céans estime que l'absence de registre des activités de traitement ou son caractère incomplet doivent, à tout le moins à la lumière de l'article 5 du RGPD, être qualifiés de traitement « formellement » illicite des données. La question se pose donc de savoir s'il n'y aurait pas lieu, dans un tel cas, de sanctionner ce manquement, en vertu des dispositions combinées de l'article 5 du RGPD et de l'article 30 du RGPD, par l'effacement ou, à tout le moins, l'inaccessibilité des données. À défaut, en effet, si aucune sanction n'était possible, le RGPD ne pourrait être appliqué de façon effective.

26 Il convient de relever que la République française, par exemple, avait prévu – à notre connaissance – dans son droit national, sous l'empire des articles 18 et suivants de la directive 95/46, une stricte interdiction légale d'utiliser, dans le cadre de procédures juridictionnelles, les données à caractère personnel n'ayant pas fait l'objet d'une notification par le responsable du traitement à l'autorité de contrôle (CNIL), car l'utilisation des données était illicite en l'absence de documentation. Ces dispositions instauraient donc déjà au moins une sanction : l'impossibilité pour le tribunal de traiter et d'utiliser ces données. Sous l'empire du RGPD, au Portugal et [dans] d'autres États membres, l'absence de registre des activités de traitement semble également entraîner une interdiction d'utilisation. Ce mécanisme n'existe pas en République fédérale d'Allemagne dans le cadre de la transposition de la directive 95/46 ni sous l'empire du RGPD. C'est au contraire en Allemagne qu'a été posée la première pierre de l'approche consistant à « tolérer » l'absence de notification.

27 La transmission électronique du dossier et des mémoires de la défenderesse constitue également un traitement des données au sens de l'article 4, point 2, du RGPD, qui doit obéir aux principes du traitement des données énoncés à l'article 5 du RGPD. C'est pourquoi on peut s'interroger, également dans ce contexte, sur la licéité formelle du traitement des données consistant en leur transfert, [en ce qui concerne] le mode de transmission du « dossier électronique » de l'Office fédéral et des mémoires de la défenderesse. Il n'existe pas non plus dans ce cas de registre des activités de traitement ni de disposition régissant la responsabilité conjointe. On peut certes mentionner un règlement, le Verordnung über die technischen Rahmenbedingungen des elektronischen Rechtsverkehrs und über das besondere elektronische Behördenpostfach (règlement sur les conditions techniques de la justice en ligne et la boîte postale électronique spéciale des autorités publiques (BGBl. I p. 3803, tel que modifié par l'article 6 de la loi du 5 octobre 2021, BGBl. I p. 4607). Ce règlement régit la transmission de documents électroniques aux juridictions des Länder et de l'État fédéral. Dans ce cadre, les plus hautes autorités de l'État fédéral ou des gouvernements des Länder peuvent, pour leur domaine d'action, vérifier auprès d'organismes de droit public l'identité des autorités ou personnes morales de droit public afin de les autoriser à accéder à la boîte postale électronique spéciale des autorités publiques (dite « BeBPo »). Les plus hautes autorités de l'État fédéral ou plusieurs gouvernements de Länder peuvent également désigner conjointement un organisme de droit public pour leurs domaines d'action. Le règlement en question ne désigne pas concrètement ces instances. Cela vise vraisemblablement en définitive le groupe de travail des ministères de la justice de l'État fédéral et des Länder (Bund-Länder-Kommission für Informationstechnik in der Justiz [BLK] groupe de travail sur le standard IT dans la justice). L'identité de l'autorité ou des autorités responsables du service d'annuaire de la boîte postale électronique judiciaire et administrative (EGVP) ou de la boîte postale électronique spéciale des autorités publiques (BeBPo), voire de l'infrastructure de serveurs nécessaire, n'est ni connue ni documentée.

28 Il n'existe pas non plus, entre les juridictions et les autorités administratives, de règlementation à cet égard, issue de la loi ou d'autres dispositions écrites, comme l'exigerait l'article 26 du RGPD, pour organiser les responsabilités. Même les Länder dont les gouvernements ont choisi le modèle de la procédure conjointe (par exemple le Land de Hesse, Verordnung über den elektronischen Rechtsverkehr bei hessischen Gerichten und Staatsanwaltschaften v. 26.10.2007, règlement du 26 octobre 2007 sur les services de justice en ligne auprès des juridictions et parquets du Land de Hesse, GVBl. I 699) n'ont pas prévu à cet égard une mise en œuvre respectant la protection des données. Dans le Land de Hesse, le règlement en question prévoit même que la boîte à lettre électronique est gérée exclusivement sur les serveurs du « centre de calcul » de la justice, c'est-à-dire au sein de la Hessische Zentrale für Datenverarbeitung (Centrale du traitement des données du Land de Hesse, ci-après « HZD »). La HZD n'est justement pas rattachée à la justice et est tout au plus, en tant qu'intermédiaire, un sous-traitant au sens de l'article 28 du RGPD.

29 Le seul élément connu concerne le Landesamt für Datensicherheit in Nordrhein-Westfalen (Office de la sécurité des données du Land de Rhénanie-du-Nord-Westphalie), lequel est censé être concrètement responsable de l'administration et de l'exploitation du serveur d'enregistrement central et national S.A.F.E., en tant qu'« intermédiaire ». Les clients d'enregistrement suivants sont actuellement disponibles : client EGVP pour la création d'une boîte postale pour la communication utilisant le standard OSCI, client d'enregistrement ZTR pour l'enregistrement en vue de l'utilisation du registre central des testaments du Bundesnotarkammer (chambre fédérale allemande des notaires), client d'enregistrement Zentrales Vollstreckungsportal (portail central de l'exécution [mettant à disposition les données du registre des débiteurs] pour l'enregistrement en vue de l'utilisation de ce portail. Le « SAFE-ID » (identifiant SAFE) doit être inaltérable et n'être attribué qu'une seule fois (voir à ce sujet SAFE – http://www.egvp.de/Drittprodukte/SAFE_Abbildungsvorschrift_SAFE_ID_Stand_Dec_2014.pdf). Il existe en outre un « Govello-ID » (identifiant Govello). Les boîtes postales électroniques judiciaires et administratives (EGVP) sont désignées par un numéro d'identification unique (Govello-ID). Celui-ci est composé de l'identifiant « safe-sp1 » ou « govello » et de deux séries de chiffres. Ces identifiants sont censés être enregistrés dans un service d'annuaire, qui est probablement géré par le Land de Rhénanie-du-Nord-Westphalie (IT-NRW). Il n'existe aucune disposition désignant le responsable concret de l'attribution de l'identifiant Govello au sein du réseau Fédération-Länder.

30 La disposition du droit de la protection des données censée constituer la base juridique du système de l'EGVP n'est pas connue. Interrogée sur l'existence d'un accord au sens de l'article 26 du RGPD, la défenderesse s'est refusée à s'expliquer à ce sujet et à produire un quelconque accord. On peut également s'interroger, à cet égard, sur la licéité du transfert des données opéré via la boîte postale électronique spéciale des autorités publiques, dès lors que les responsabilités n'ont pas été définies conformément à l'article 26 du RGPD. Cela vaut également pour la sécurité des données, étant donné qu'aucun des documents n'est chiffré lors du transfert.

31 Certains affirment que le droit positif n'exige pas, à l'heure actuelle, que la boîte postale électronique spéciale des avocats soit conçue et exploitée avec un chiffrement de bout en bout [Anwaltsgerichtshof Berlin (Cour des avocats du barreau de Berlin), arrêt du 14.11.2019 – I AGH 6/18 – point 14, juris). Aucun élément ne permettrait de conclure que l'obligation d'un chiffrement de bout en bout correspondrait à l'état de la technique et qu'il devrait donc être utilisé par le Conseil fédéral de l'ordre des avocats (Anwaltsgerichtshof Berlin, arrêt du 14 novembre 2019 – I AGH 6/18 – point 83, juris). Il n'existe d'ailleurs aucune prescription dans le sens d'un tel chiffrement de bout en bout (BGH, arrêt du 22.03.2021 – AnwZ [Brfg] 2/20 –, BGHZ 229, 172-213, point 88). Pour ce qui est en tout cas du Land de Hesse, les messages transmis entre l'intermédiaire, la HZD, et la juridiction concernée – et donc également le Verwaltungsgericht Wiesbaden (tribunal administratif de Wiesbaden) – ne sont pas chiffrés.

32 Mais cela importe peu en l'espèce, car la procédure correspond à une procédure de courrier électronique. En ce qui concerne le service de messagerie électronique sur internet Gmail, la Cour a jugé qu'il ne s'agissait pas d'un service de communications [électroniques], car ce service ne comporte pas un accès à Internet, [de sorte qu'il] ne consiste pas entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques et ne constitue donc pas un « service de communications électroniques » (arrêt du 13 juin 2019, Google, C-193/18, EU:C:2019:498). La boîte postale électronique judiciaire et administrative (EGVP) n'est donc pas un service relevant de la directive 2002/58/CE [du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), JO L 201 du 31 juillet 2002, p. 37)] (article 2, paragraphe 4, du RGPD). Il s'ensuit que le RGPD s'applique, avec pour conséquence que l'EGVP et les procédures qui y sont associées doivent être consignées dans un registre des activités de traitement et que les responsabilités respectives doivent faire l'objet d'un accord en tant que procédure impliquant une pluralité de responsables du traitement, conformément à l'article 26 du RGPD. Ces deux éléments font en l'espèce défaut, ce qui conduit à douter de la licéité du transfert de données.

33 La boîte postale électronique judiciaire et administrative (EGVP) constitue une procédure de l'administration de la justice, qui relève du deuxième pouvoir, à savoir le pouvoir exécutif, et de la partie défenderesse, qui fait également partie du pouvoir exécutif. La juridiction de céans est donc convaincue qu'il incombe à la défenderesse de veiller à ce que la procédure électronique de transfert des données des mémoires et des dossiers soit conforme au RGPD.

34 Pour la juridiction de céans, la question se pose donc de savoir, dans le cadre de l'activité juridictionnelle, comment procéder avec les données fournies par le système de l'EGVP via la boîte postale des autorités publiques (BeBPo) lorsque la procédure de l'EGVP et le traitement des données associé à cette procédure ne sont pas en tant que tels conformes au RGPD.

35 La juridiction de céans doit à tout le moins tenir compte du RGPD et s'y conformer dans le cadre de son activité juridictionnelle. Dans son arrêt du 9 juillet 2020, Land Hessen (C-272/19, EU:C:2020:535, points 42 et s.), la Cour a expressément précisé à cet égard que l'indépendance du juge national s'entend uniquement de l'indépendance personnelle (point 49) et n'inclut pas l'institution judiciaire dans son ensemble. Par conséquent, l'activité juridictionnelle se déroule uniquement dans le cadre de l'indépendance personnelle.

36 La juridiction de céans n'a donc aucune influence sur la licéité du traitement des données par l'administration de la justice, car elle s'exerce hors de l'« activité juridictionnelle », au niveau du pouvoir exécutif. La juridiction de céans doit toutefois tenir compte du droit européen et s'y conformer. Si les parties à la procédure ne respectent pas le droit de l'Union, l'utilisation des données en justice

devrait probablement être exclue, car dans le cas contraire, la juridiction participerait à un traitement illicite des données. En l'espèce, le fait que la défenderesse, au vu des éléments échangés jusqu'à présent, viole sans doute (sciemment) les dispositions du droit européen vient encore aggraver la situation.

37 Nous ne sommes pas non plus dans un cas de figure qui justifierait l'utilisation de ces données en justice sur le fondement de l'article 17, paragraphe 3, sous e), du RGPD aux fins de la constatation, l'exercice ou la défense de droits en justice par la partie défenderesse. Les données sont certes utilisées par la défenderesse pour respecter une obligation légale qui requiert le traitement, prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis, ou pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement, voir l'article 17, paragraphe 3, sous b), du RGPD. Mais cela reviendrait en même temps à légaliser durablement une pratique contraire à la législation sur la protection des données.

38 Les questions posées sont donc particulièrement importantes lorsqu'il s'agit de mettre en œuvre le RGPD dans le cadre d'une procédure juridictionnelle. L'objectif énoncé à l'article 1er, paragraphe 2, du RGPD, à savoir la [protection] des libertés et droits fondamentaux des personnes physiques, et en particulier leur droit à la protection des données à caractère personnel, serait compromis.

39 À cet égard, à tout le moins en cas de réponse négative à la question 1, il devrait être nécessaire de s'en remettre à la décision de la personne concernée – en l'occurrence le requérant – ou plutôt d'obtenir son consentement exprès à l'utilisation de ses données dans le cadre d'une procédure juridictionnelle, bien qu'elles aient fait l'objet d'un traitement formellement illicite.

40 Cependant, cela aurait également pour conséquence qu'en cas de refus, les données traitées par la défenderesse, qu'elle présente sous la forme du dossier administratif électronique « MARIS », ne pourraient pas être traitées (utilisées) par le tribunal. Cela aurait alors pour conséquence que la décision n'aurait aucune base tant qu'il ne serait pas remédié au manquement aux obligations en matière de documentation. La décision initiale de la défenderesse devrait systématiquement être annulée. Aucune décision sur le statut de réfugié dont se prévaut la personne concernée ne serait possible tant qu'il ne serait pas remédié au manquement aux obligations en matière de documentation.

[omissis]