Recommandation n° 02/2017 du 12 avril 2017

Objet: Recommandation à l'égard des sociétés clientes d'Atos Worldline/EquensWorldine émettrices de cartes de paiement établies en Belgique (CO-AR-2017-003)

La Commission de la protection de la vie privée ;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après LVP), en particulier l'article 30 ;

Vu le rapport de Monsieur Ivan Vandermeersch

Émet, le 12 avril 2017, la recommandation suivante:

I. Descriptif des faits

1. Dans le cadre de leurs activités en tant qu'émetteur de cartes de paiement, la majorité des institutions bancaires établies en Belgique ont confié la prestation de certains services de sous-traitance à Atos Worldline[1]/Equens[2] (ci-après « Atos Worldline/EquensWorldline »). Atos Worldline/EquensWorldline fournit dans ce cadre le système informatique pour l'émission des cartes de paiement, le traitement des autorisations de transactions financières et également d'autres services, tels la mise à disposition de centres d'appels pour le « Card Stop » (blocage de cartes de paiement) et les traitements y associés, ainsi que le traitement technique des plaintes relatives aux transactions bancaires (par exemple, lorsqu'un utilisateur conteste le fait d'avoir effectué une certaine transaction). Ces services de sous-traitance sont prestés par Atos Worldline/EquensWorldline pour le compte de la majorité des banques établies en Belgique depuis le rachat de la société Banksys en 2006.

2. En 2013, Atos Worldine a confié la prestation de certains services (mise en place d'une sous-traitance ultérieure) à des sociétés du groupe Atos en dehors de l'Union Européenne (ci-après « UE »). Ces services sont mutualisés, ce qui implique qu'ils sont également prestés pour l'ensemble des sociétés émettrices de cartes de paiement établies en Belgique qui sont clientes d'Atos Worldline/EquensWorldline et la date de début des transferts internationaux est identique pour toutes.

3. Sur la base des informations obtenues par la Commission, voici une description des services qui ont fait l'objet d'une sous-traitance ultérieure en dehors de l'UE :

- **Au Maroc :**
    - A la société ITS Nearshore Center Maroc SARL (depuis janvier 2013)
        - **Services concernés**

- Service Card Stop[3] : Gestion des appels téléphoniques pour Card Stop, traitements à des fins d'identification des cartes concernées et d'authentification de leur détenteur, blocage des cartes de paiement et rapportage (reporting) pour permettre la résolution ultérieure des problèmes liés aux cartes bloquées.
- Back office des ATM (Automated Teller Machine) pour les incidents lors de transactions bancaires.

[1] Jusqu'au mois d'octobre 2016, il s'agissait plus précisément des sociétés Atos Worldline S.A./N.V. (BE 0418.547.872, Bruxelles) et Atos Worldline (B 378 901 946, Bezons, France).

[2] A partir du mois d'octobre 2016, il s'agit des succursales belge (BE 0535.900.650, Bruxelles) et françaises (819 173 782 00031, Bezons, France) de la société de droit néerlandais Equens SE (30220519, Utrecht).

[3] Par exemple, pour ce qui concerne un des client d'Atos Worldline/Equens, 40% des appels y sont gérés, à savoir approximativement 70 000 appels en 2015.

- **Données transférées**

- Dans le cadre des prestations « Card Stop » il s'agit des données relatives aux cartes et à leurs détenteurs personnes physiques[4] et les données relatives aux transactions[5].
- Dans le cadre du service lié au back office des ATM : ceci concerne les données relatives aux numéros de cartes.

- **En Inde :**
  - A la société Worldline India private Ltd (depuis juin 2013):
    - **Services concernés**

- Dispute Handling[6] : gestion opérationnelle des contestations de transactions par les clients (par ex. en cas de double paiement). Les appels sont gérés en Belgique mais le suivi des traitements a lieu en Inde.
- Fraud Database : traitement des contestations en cas de risque de fraude.
    - **Données transférées**
- Dans le cadre de ces prestations : les données relatives aux cartes et à leurs détenteurs personnes physiques[7] et les données relatives aux transactions[8].

  - A la société Atos India pvt Ltd (depuis mars 2015) (Certaines différences existent entre les informations fournies par Atos et un de ses clients émetteur de cartes de paiement)
    - **Services concernés**

Selon l'information communiquée par un client d'Atos Worldline sur la base des informations communiquées par EquensWorldline:

- Service de support de tests de programmes informatiques (en environnement de tests).
- Service de support de seconde ligne pour des applicatifs Linux principalement pour la résolution des incidents (par ex. application gérant le montant maximum de découvert autorisé, personnalisation des cartes).

Selon l'information communiquée par Atos Worldline N.V./S.A.:

- Service de support technique pour l'installation de programmes informatiques (en environnement de production).

[4] Numéro de carte, nom et prénoms du détenteur, date de naissance, numéro de compte lié à la carte, type de carte et date d'expiration.

[5] Montant, date et heure, ATM, localisation et commerce concerné.

[6] Pour ce qui concerne un client d'Atos Worldline / Equens, 10% des dossiers y sont gérés, à savoir 1000 dossiers pour 2015.

[7] Numéro de carte, nom et prénoms du détenteur, date de naissance, numéro de compte lié à la carte, à l'exclusion du code PIN.

[8] Montant, date et heure, ATM, localisation et commerce concerné.

- **Données transférées**

Selon l'information communiquée par un client d'Atos Worldline :

- Pour les tests informatiques : seulement en environnement de test, n'ayant jamais accès aux données de production et donc avec un accès limité aux données des clients des responsables de traitement
- Service de support : données relatives à des transactions bancaires[9].

4. La Commission dispose d'un modèle de courrier que la société Atos Worldline N.V./S.A. aurait envoyé[10] le 28 septembre 2012 à certaines sociétés émettrices de cartes de paiement établies en Belgique pour les informer de leur intention de transférer les appels francophones relatifs au service Card stop (et Card holders Care calls) à une entité Atos au Maroc. La Commission prend acte des informations communiquées par Atos Worldline/EquensWorldline mais dès lors que cet envoi est contesté par certains clients d'Atos et que la Commission ne dispose pas des preuves de ces envois, l'existence de cette information n'est pas, aux yeux de la Commission, certaine. Par ailleurs, le contenu de cette information préalable n'est que partiel car il ne couvre qu'une partie des services prestés au Maroc et aucun service presté en Inde.

5. Un des clients d'Atos Worldline/EquensWorldline dit avoir pris connaissance des activités de sous-traitances ultérieures en Inde et au Maroc de manière fortuite lors d'une revue contractuelle du contrat de sous-traitance en été 2015. Peu après, la société Atos Worldline N.V./S.A. a réalisé un rapport interne portant sur tous les contrats de services conclus avec les sociétés émettrices de cartes de paiement établies en Belgique.

6. Suite à ce rapport, la société Worldline Belgium[11] a envoyé un courrier entre les mois d'octobre 2015 et d'avril 2016 à différentes sociétés émettrices de cartes de paiement établies en Belgique pour les informer des activités de sous-traitances ultérieures, notamment en Inde et au Maroc et pour obtenir leurs autorisations. Selon les informations dont la Commission dispose, ce courrier n'aurait pas été envoyé à l'ensemble des clients concernés.

7. En réponse à ce courrier, différentes sociétés émettrices de cartes de paiement établies en Belgique ont octroyé leur autorisation. Les premières autorisations datent du mois d'octobre 2015, les dernières du mois d'octobre 2016. Selon les informations dont la Commission dispose, plusieurs sociétés n'ont pas encore octroyé leur autorisation bien que les services en Inde et au Maroc soient prestés pour leur compte.

---

[9] Numéro de carte, montant, date, heure, ATM, localisation et commerce concerné.

[10] La Commission ne dispose pas des copies des courriers envoyés et donc des destinataires.

[11] Qui a la même adresse qu'Atos Worldline N.V./S.A.

8. La Commission a interrogé les sociétés Atos Worldline N.V./S.A. et EquensWorldline sur l'encadrement juridique des transferts internationaux de données.

9. Atos Worldline/EquensWorldline a fait référence aux règles d'entreprise contraignantes de son groupe (ci-après, « BCR sous-traitant ») dont la procédure de revue européenne a été finalisée fin septembre 2014. La Commission, étant membre de l'engagement informel de reconnaissance mutuelle entre autorités de protection des données, n'a pas remis en cause le contenu des engagements pris dans les BCR lors de la procédure de coopération européenne. Cette procédure vise à assurer une harmonisation de l'évaluation du niveau de protection offert par une politique de protection des données intra-groupe (BCR). En conformité avec les législations nationales, les BCR dont la procédure européenne est finalisée doivent faire l'objet d'une autorisation nationale afin de pouvoir être utilisé comme outil de transfert. Certaines conditions additionnelles peuvent être imposées par l'autorité nationale compétence, comme par exemple, l'obligation de mettre en œuvre les obligations de transparence et d'accessibilité des BCR pour les personnes concernées ou d'apporter les preuves relatives à l'engagement juridique des entreprises concernées. Pour ces BCR, Atos Belgium N.V./S.A. a pris contact avec la Commission le 7 mars 2016 pour introduire une demande d'avis de la Commission en vue d'obtenir une autorisation par Arrêté royal. Le protocole d'accord entre le SPF Justice et la Commission établissant la procédure d'autorisation pour les BCR sous-traitants n'a été conclu que le 3 octobre 2016 et donc aucune autorisation par Arrêté royal de BCR sous-traitants ne pouvait être donnée en Belgique avant cette date. Le secrétariat de la Commission a posé des questions et demandé des documents relatifs à ces BCR à Atos Belgium N.V./S.A. Certaines informations sont encore manquantes. Par conséquent, les BCR sous-traitant d'Atos n'ont pas encore fait l'objet d'un avis de la Commission, ni d'une autorisation par Arrêté royal.

10. Par ailleurs, à la connaissance de la Commission, un seul client d'Atos Worldline/EquensWorldline a conclu des clauses contractuelles types directement avec les sociétés indiennes et marocaine (suite à l'intervention de la Commission).

11. Le secrétariat a auditionné Atos Worldline N.V./S.A./EquensWorldline le 13 janvier 2017 et il l'a entendu, à sa requête, le 9 février 2017. Le secrétariat a également participé en tant qu'observateur à une inspection menée par la CNIL le 6 février 2017 au siège du groupe Atos à Bezons (Atos SE).

12. Ces sociétés ainsi que les sociétés visées par la présente recommandation ont été invitées à communiquer leur point de vue sur cette recommandation par écrit. Les sociétés visées par la présente recommandation ont également été entendues.

II. Analyse juridique

A. L'obligation de mettre en place des mesures de sécurité (Art. 16§4 LVP) et lorsque un traitement est confié à un sous-traitant, de veiller au respect de ces mesures, notamment par la stipulation de mentions contractuelles (Art. 16§1.2 LVP)

13. En vertu de l'article 16§4 de la LVP, « *Afin de garantir la sécurité des données à caractère personnel, le responsable du traitement (…) ainsi que le sous-traitant doivent prendre les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel contre (…) la modification, l'accès et tout autre traitement non autorisé de données à caractère personnel. Ces mesures doivent assurer un niveau de protection adéquat, compte tenu, d'une part, de l'état de la technique en la matière et des frais qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels.* »

14. En vertu de l'article 16§1.2, « *Lorsque le traitement est confié à un sous-traitant, le responsable du traitement ou, le cas échéant, son représentant en Belgique, doit veiller au respect de ces mesures*[12] *notamment par la stipulation de mentions contractuelles* »

15. La relation entre Atos Worldline/EquensWorldline et les institutions financières émettrices de cartes de paiement est encadrée par des contrats de sous-traitance périodiquement renouvelés. La Commission a pris connaissance des conditions contractuelles pour la sous-traitance ultérieure d'une trentaine d'institutions financières émettrices de cartes de paiement établies en Belgique.

16. Les contrats de sous-traitance définissent généralement d'une part, les entreprises autorisées à avoir accès aux données, et d'autre part, les mesures techniques et organisationnelles relatives à la gestion et au contrôle des accès aux données personnelles.

17. Pour ce qui concerne les entreprises autorisées à avoir accès aux données, l'ensemble des contrats qui ont été analysés requièrent un consentement spécifique et préalable lorsque la société Atos Worldline/EquensWorldline envisage de faire de la sous-traitance ultérieure en intra-groupe et en dehors de l'Union européenne. Cette exigence implique nécessairement des mesures de transparence préalable. Certains des contrats analysés spécifient que l'information doit être donnée au moins trois mois à l'avance. La Commission estime que le niveau de protection apporté par ces contrats est généralement élevé.

[12] Les mesures de sécurité technique et d'organisation relatives aux traitements, voir la référence à l'Art. 16§1.1 de la LVP.

18. Cependant, comme indiqué au point 4 de cette recommandation, les mesures d'informations préalables n'ont été que partiellement réalisées par Atos Worldline/EquensWorldline.

19. Comme décrit aux point 6 et 7 de cette recommandation, des mesures de transparence complémentaires ainsi que des démarches pour obtenir l'autorisation de certains responsables de traitement ont été apportées à la fin de l'année 2015. Plusieurs autorisations ont été délivrées entre la fin 2015 et le mois de septembre 2016. Certaines autorisations n'ont cependant pas encore été octroyées.

20. Considérant ce qui précède, la Commission estime que l'obligation contractuelle relative à l'information et à l'autorisation préalable des responsables de traitement qui incombe à Atos Worldline/EquensWorldline n'a pas été pleinement respectée.

21. En outre, certains contrats exigent également, en cas de sous-traitance ultérieure, le report des obligations du sous-traitant initial sur le sous-traitant ultérieur. L'exigence de reporter les obligations relatives à la protection des données personnelles devra par ailleurs être systématique lors de l'entrée en application du Règlement européen de la protection des données 2016/679/UE[13]. Aucun élément en la possession de la Commission ne permet d'établir que Atos Worldline/EquensWorldline ait rempli cette obligation en s'assurant que les sociétés marocaine et indiennes, lorsqu'elles agissent en tant que sous-traitant ultérieur, aient accepté les mêmes obligations contractuelles relatives à la protection des données à caractère personnel que celles qui avaient été prévues dans le contrat de sous-traitance initial. Cette obligation contractuelle n'est donc *a priori* toujours pas remplie.

22. Cependant, suite à l'intervention de la Commission une des sociétés clientes d'Atos Worldline/EquensWorldline a signé directement des clauses contractuelles types avec les sociétés indiennes et marocaines, ce qui implique que ces sociétés sont devenues à son égard des sous-traitants directs du point de vue de la protection des données à caractère personnel (et non plus des sous-traitants ultérieurs). Dans une telle hypothèse, le report des obligations n'est plus strictement requis et c'est au responsable de traitement d'évaluer si la protection offerte par les clauses types est suffisante pour le cas d'espèce.

23. Pour ce qui concerne un client particulier émetteur de cartes de paiement d'Atos Worldline/EquensWorldline, la Commission a pu consulter l'entièreté du contrat de sous-traitance, en ce compris les dispositions contractuelles relatives à la gestion de la sécurité.

[13] Article 28.4.

24. En vertu de ce contrat, les données sont traitées dans des applications d'Atos Worldline, il y a une obligation pour Atos Worldline de faire une analyse des accès (« Audit Logging[14] »). Il est prévu que les journaux d'audit (« audit trail ») soient accessibles en ligne pendant une durée minimum d'un an. Ils sont ensuite archivés sur bande (« archived on tape ») pour 1100 jours (3 ans).

25. Lorsque les données sont traitées dans des applications client, les accès font l'objet d'une matrice de contrôle d'accès (« access control matrix »).

26. Les dispositions contractuelles des différentes sociétés clientes d'Atos Worldline/EquensWorldline émettrices de cartes de paiement établies en Belgique ainsi que leurs mesures organisationnelles et techniques ne leur ont pas permis de détecter l'accès non autorisé par les sociétés indiennes et marocaine. La Commission estime inacceptable que ces entreprises, responsables de traitement, n'aient pas été en mesure de savoir où ont été traitées les données personnelles dont elles ont la responsabilité juridique et cela durant près de deux années, de 2013 à 2015. Ce constat est d'autant plus accablant compte tenu de la nature des données concernées (données financières) et de la confidentialité particulière qui y est attachée.

27. Il est essentiel que les sociétés émettrices de cartes de paiement établies en Belgique clientes d'Atos Worldline/EquensWorldline assurent que des mesures organisationnelles et techniques soient mis en place afin de leur permettre de garder un contrôle sur les lieux où leurs données sont traitées (en ce compris transférées et accédées) et par qui elles sont traitées. Le choix des mesures revient au responsable de traitement, il pourrait s'agir par exemple d'une obligation de reporting régulier des logging d'accès ou inventaire régulier des accès comportant les informations sur les lieux et les entreprises accédant aux données, et le contrôle de ces informations par le biais d'audit régulier spécifique ou ponctuel lorsqu'une anomalie est détectée.

28. La Commission est aussi particulièrement interpellée par le fait que la prise de connaissance des accès non autorisés aux données personnelles n'ait, selon les informations obtenues par la Commission, pas conduit à une investigation de ces entreprises afin de vérifier les risques particuliers liés à cet accès non autorisé.

29. La Commission estime que, pour respecter les articles 16§1.2 et 16§4 de la LVP, les responsables de traitement doivent mettre en place des mesures organisationnelles et techniques permettant de constater les accès non autorisés lorsque les données sont confiées à leur sous-traitant ; veiller au respect des mesures techniques et organisationnelles mises en place par leur sous-traitant et mettre en œuvre les mesures d'investigation lors du constat d'un accès non autorisé.

[14] Les éléments des loggings : identité des utilisateurs finaux ; description de l'action entreprise ; action réussie ou non ; moment de l'action ; depuis où (appareil utilisé (ex. IP, nom de l'appareil, Internet Browser) ; et le canal de communication utilisé.

B. L'obligation de choisir un sous-traitant qui apporte des garanties suffisantes (Art. 16§1.1 LVP)

30. L'article 16§1.1° de la LVP impose à tout responsable de traitement de choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité techniques et d'organisation relatives aux traitements.

31. Selon les informations mises à la disposition de la Commission, il semblerait que les autorisations permettant la sous-traitance en Inde et au Maroc ont été octroyées sans qu'un exercice de « due diligence » n'ait été conduit à l'égard de ces sociétés.

32. Selon les propos d'un des clients, la simple appartenant au groupe Atos apportait les garanties suffisantes.

33. Cependant, la Commission tient à signaler que l'appartenance à un groupe n'implique pas nécessairement l'assurance que les garanties apportées par certaines entités soient automatiquement offertes par les autres. En effet, au sein d'un groupe, les entités peuvent avoir des personnalités juridiques distinctes et offrir des niveaux de garantie différents.

34. L'article 1.2.3 de politique intra-groupe d'Atos qui fixe les garanties en matière de protection des données (« Atos Binding Corporate Rules ») stipule que cette politique aura des effets juridiquement contraignants entre les entités d'Atos lorsque celles-ci auront signé un accord Intra-groupe[15]. Il est à noter que si la société Atos India Private Limited a signé cet accord le 29 février 2016, la société ITS Nearshore Center Maroc SARL ne vient que très récemment de le signer[16] et la société Worldline India private Ltd ne l'a toujours pas signé. Ceci démontre une différence de garanties juridiques au sein du groupe Atos.

35. Un des moyens de s'assurer qu'un sous-traitant ultérieur offre des garanties suffisantes consiste à reporter les obligations contractuelles relatives à la protection des données à caractère personnel applicables au sous-traitant initial. En outre, compte tenu de la sensibilité et confidentialité particulière des données traitées, un examen de « due diligence » des sous-traitants (et des sous-traitants ultérieurs) est recommandable afin de vérifier leur aptitude à respecter les mesures organisationnelles, techniques et contractuelles normalement imposées à tout sous-traitant. Aucun élément en la possession de la Commission n'a permis d'établir que les sociétés marocaine

[15] Art. 1.2.3: "These BCR are part of the Intra Group Agreement which make all Group policies legally binding amongst all Atos entities which enter into the Intra Group Agreement and which are listed in Appendix 2."

[16] La version signée du contrat n'étant pas datée, le caractère récent du moment de la signature a été communiqué lors de déclarations orales des représentants d'Atos le 6/2/2017.

et indiennes, lorsqu'elles agissent en tant que sous-traitant ultérieur, ont pris un engagement contractuel de respecter des obligations contractuelles identiques ou similaires à celles qui sont imposées à Atos Worldline/EquensWorldline dans les contrats de sous-traitance conclus avec ses clients, et cela afin d'assurer la continuité de la protection contractuelle.

36. La Commission estime pourtant que pour respecter l'article 16§1.1 de la LVP, les responsables de traitement visés par la présente recommandation doivent veiller au respect de ces conditions qui permettent de choisir un sous-traitant apportant des garanties suffisantes.

C. L'obligation de respecter les règles en matière de transferts internationaux de données à caractère personnel (Art. 21 et 22 LVP)

37. Afin d'assurer le respect des règles en matière de transferts internationaux de données à caractère personnel, un des clients d'Atos Worldline/EquensWorldline a signé des clauses contractuelles type avec les sociétés marocaine et indiennes en septembre 2016 (voir le point 10 de la recommandation). La Commission tient à signaler que l'encadrement des transferts internationaux doit avoir lieu préalablement au début des transferts (2013).

38. La société Atos Worldline/EquensWorldline a indiqué à la Commission que les transferts vers les sociétés filiales en Inde et au Maroc étaient encadrées juridiquement par les « BCR sous-traitant » (voir le point 9 de cette recommandation). Le Groupe de l'article 29 reconnait la possibilité pour des responsables de traitement d'apporter des garanties suffisantes par la conclusion d'un contrat de service rendant obligatoires des BCR sous-traitant[17].

39. Cependant, la Commission estime que pour ce qui concerne les transferts internationaux émanant du territoire belge, les BCR sous-traitant du groupe Atos ne peuvent actuellement être considérés comme un encadrement juridique suffisant en conformité avec l'article 22§1, dernier alinéa. En effet, la Commission considère que plusieurs conditions ne sont pas remplies en l'espèce.

40. Pour que les BCR sous-traitants du groupe Atos puissent rencontrer les exigences de l'article 22§1, dernier alinéa de la LVP, il faut :

- que la procédure de revue européenne ait été finalisée, ce qui est le cas en l'espèce (voir le point 9 de la recommandation);

[17] Working document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, 6 Juin 2012 (WP195).

- que les filiales belges du groupe ayant mis en place des BCR sous-traitant aient fait l'objet d'une autorisation par Arrêté royal, ce qui n'est pas le cas en l'espèce (voir le point 9 de la recommandation) ;

- que le contrat de service entre Atos et ses clients (les sociétés émettrices de cartes de paiement établies en Belgique) rendent obligatoire l'application des BCR sous-traitant à leur cadre contractuel, ce qui, selon l'analyse des contrats reçus par la Commission (voir le point 15 de cette recommandation), n'est pas le cas en l'espèce et donc entraîne ipso facto la non-application des BCR sous-traitant à leur égard ;

Depuis 2016, les modèles de clauses contractuelles du groupe Atos[18] prévoient une référence aux BCR sous-traitant sans toutefois prévoir un engagement explicite de les respecter et de les appliquer pour le contrat de service particulier. En vertu des BCR sous-traitant d'Atos[19] et des exigences du Groupe de l'article 29[20], cet engagement est pourtant nécessaire pour une application des BCR sous-traitant à l'égard de leurs clients. Les modèles internes de clauses contractuelles du groupe Atos ne sont donc pas conformes à leurs propres BCR.

- que les entreprises exportatrices (les sociétés belges d'Atos Worldline/EquensWorldline) démontrent s'être engagées formellement à respecter les BCR sous-traitant, par la signature de l'accord intragroupe, ce qui n'est pas le cas en l'espèce ;

Le groupe Atos considère que l'adoption des BCR sous-traitant par le conseil de direction du groupe Atos qui aurait eu lieu au cours du premier semestre 2015, suffit pour les rendre obligatoires. Cependant, la Commission estime que l'adoption des BCR sous-traitant par le conseil de direction d'un groupe n'implique pas automatiquement une obligation juridique opposable aux tiers dans le chef de ses filiales belges. Il est à noter finalement que l'analyse du groupe Atos est contradictoire avec les exigences de ses propres BCR sous-traitant dès lors que ces derniers requièrent que ses filiales signent l'accord intragroupe afin que les BCR sous-traitant soient rendus obligatoires[21]. La Commission conclut par conséquent que l'engagement formel des entreprises exportatrices n'est pas démontré.

---

[18] Standard data protection clauses to be inserted in sales contracts.

[19] Art. 1.2.5 Where Atos acts as a Data Processor, Atos commits in the Service Level Agreement that binds Atos and its Customer, to respect these BCR.

[20] Working document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, 6 Juin 2012 (WP195), Point II (Commitments to be taken in the Service Level Agreement.

[21] Article 1.2.3. de la version 1.4 des BCR sous-traitant du groupe Atos: "These BCR are part of the Intra Group Agreement which make all Group policies legally binding amongst all Atos entities which enter into the Intra Group Agreement and which are listed in Appendix 2", https://atos.net/content/dam/global/documents/atos-binding-corporate-rules.pdf .

- que les entreprises importatrices démontrent s'être formellement engagées à respecter les BCR sous-traitant par la signature de l'accord intragroupe, ce qui n'est pas le cas en l'espèce ;

La société Atos India pvt Ltd a signé cet accord le 29 février 2016 et la société ITS Nearshore Center Maroc SARL aurait très récemment également signé l'accord[22]. A l'heure actuelle, la société Worldline India private Ltd n'a toujours pas signé cet accord. Par conséquent, cette condition n'est que partiellement remplie (une des sociétés n'étant pas encore partie au contrat). Par ailleurs, la signature de l'accord intragroupe ne peut avoir d'effet qu'à partir de sa date de signature.

41. Au vu de ce qui précède, la Commission estime que les articles 21 et 22 de la LVP qui régissent les flux internationaux de données ont été violés (jusqu'au moment de la conclusion de clauses contractuelles types). Tant ces responsables de traitement qu'Atos Worldline/EquensWorldline ont la responsabilité juridique de la violation de ces articles,.

D. L'obligation générale de veiller au respect à la licéité du traitement de données (Art. 4§2 et 4§1.1 LVP)

42. En vertu des articles 4§2 et 4§1.1 de la LVP, il incombe au responsable du traitement d'assurer que les données soient traitées licitement.

43. Compte tenu des éléments mis à sa disposition (voir sous le titre II.A de la présente recommandation), la Commission constate que les contrats de sous-traitance n'ont pas été pleinement respectés. Les violations contractuelles ont entrainé également une violation de la LVP (ex. non-respect des instructions par le sous-traitant, non-respect des règles en matière de transferts internationaux de données).

44. Selon les informations dont dispose la Commission, après avoir eu connaissance des transferts en Inde et au Maroc et donc du non-respect de leur contrat, les sociétés clientes d'Atos Worldline/equensWorldline émettrices de cartes de paiement établies en Belgique n'ont pris aucune mesure opérationnelle concernant ces activités réalisées le temps d'assurer un encadrement contractuellement (comme la demande de rapatriement au sein de l'UE de ces activités dans les plus brefs délais).

45. Par ailleurs, à la connaissance de la Commission, aucune mesure visant à dénoncer la violation contractuelle n'a été prise (avant l'intervention de la Commission) par les sociétés clientes d'Atos

[22] Selon les déclarations faites lors de l'inspection de la société Atos SE le 6 février 2017, la Commission disposant d'un contrat signé mais non daté.

Worldline/equensWorldline émettrices de cartes de paiement établies en Belgique à l'égard d'Atos Worldline/EquensWorldline

46. Pour assurer la licéité du traitement des données, les sociétés clientes d'Atos Worldline/equensWorldline émettrices de cartes de paiement établies en Belgique, en tant que responsable de traitement, auraient dû prendre des mesures préventives visant à assurer le respect du contrat et, après la prise de connaissance des violations contractuelles, auraient dû prendre des mesures promptes et efficaces afin de s'assurer qu'elles prennent fin au plus vite.

III. Recommandations

1. La Commission recommande aux sociétés émettrices de cartes de paiement établies en Belgique clients d'Atos Worldline/EquensWorldline de renforcer ses mesures organisationnelles et techniques visant à protéger les données personnelles et à assurer le respect des contrats de sous-traitance

47. Des mesures organisationnelles et techniques doivent être mises en place par les sociétés émettrices de cartes de paiement établies en Belgique clients d'Atos Worldline/EquensWorldline permettant d'assurer et de contrôler que les données personnelles confiées par ses consommateurs soient uniquement accédées par des personnes autorisées (mesures préventives). Il s'agit notamment la mise en place de loggins d'accès par ces sociétés pour les traitements réalisés au sein de leur groupe et de l'imposition par le biais de contrats de mécanismes analogues à leurs sous-traitants pour les traitements que ces derniers réalisent pour le compte de ces sociétés. La Commission a constaté l'existence de telles dispositions dans certains contrats visant à assurer que les traces d'accès aux données (logging) soient conservées et accessibles. Cependant, l'existence de ces garanties contractuelles doivent être complétées par des mesures visant à vérifier leur respect en pratique. Le choix des mesures revient au responsable de traitement, il pourrait s'agir par exemple d'une obligation de reporting régulier des logging d'accès ou inventaire régulier des accès comportant les informations sur les lieux et les entreprises accédant aux données, et le contrôle de ces informations par le biais d'audit régulier spécifique ou ponctuel lorsqu'une anomalie est détectée. Selon les informations à la disposition de la Commission, les mesures contractuelles, d'audit et de certifications existantes n'ont pas permis aux sociétés de cartes de paiement de prendre conscience que des données personnelles étaient transférées en Inde et au Maroc. Il convient par conséquent de renforcer ces mesures pour permettre un contrôle plus efficace. L'essentiel étant de permettre aux responsables de traitement de pouvoir garder un contrôle sur les lieux où leurs données sont traitées (en ce compris transférées et accédées) et par qui elles sont traitées.Les sociétés émettrices de cartes de paiement établies en Belgique doivent s'assurer d'avoir les habilitations contractuelles pour pouvoir

vérifier ces mesures chez leurs sous-traitants et cela même si ceux-ci ne sont pas établis sur le territoire belge.

48. Des mesures organisationnelles et techniques doivent être mises en œuvre par les sociétés émettrices de cartes de paiement établies en Belgique clients d'Atos Worldline/EquensWorldline lors du constat d'un accès non autorisé (mesures réactives). Les personnes en charge de la sécurité des données et de la conformité juridique au sein de ces sociétés doivent investiguer les risques particuliers liés à cet accès non autorisé et conseiller sur les mesures à prendre.

49. Ces mesures doivent être promptes et efficaces afin de mettre fin le plus rapidement possible à la violation du contrat, ce qui peut impliquer, en fonction d'une analyse au cas par cas, de requérir du sous-traitant la suspension des traitements réalisés par le sous-traitant le temps d'assurer la mise en place d'un encadrement contractuel, ou si cela n'est pas possible, le rapatriement de ces activités sur le territoire européen dans les plus brefs délais. En outre, le responsable peut interpeller son sous-traitant pour violation contractuelle (en ce compris par une poursuite judiciaire si nécessaire).

2. La Commission recommande aux sociétés émettrices de cartes de paiement établies en Belgique clients d'Atos Worldline/EquensWorldline de mettre en place des procédures pour garantir que ses sous-traitants apportent des garanties suffisantes

50. Les sociétés émettrices de cartes de paiement établies en Belgique clients d'Atos Worldline/EquensWorldline doivent, avant de confier leurs données à un sous-traitant (en ce compris à un sous-traitant ultérieur), mettre en place des procédures leur permettant d'assurer que celui-ci apporte des garanties suffisantes en matière de protection des données.

51. Parmi ces garanties, l'article 16 de la loi prévoit actuellement l'obligation de conclure un contrat de sous-traitance. A cet égard, les sociétés émettrices de cartes de paiement établies en Belgique clients d'Atos Worldline/EquensWorldline envisagent de signer (ou ont déjà récemment signé) un contrat de sous-traitance directement avec les sous-traitants ultérieurs (clauses contractuelles types 2010/87/UE). Par ailleurs, dès l'entrée en application du règlement général de la protection des données, lorsque le responsable de traitement aura autorisé la sous-traitance ultérieure, ses sous-traitants initiaux auront une obligation juridique directe d'imposer aux sous-traitants ultérieurs les mêmes obligations contractuelles relatives à la protection des données à caractère personnel que celles qui leur sont imposées. Outre des mesures contractuelles, des mesures de vérification doivent être mises en place par le responsable de traitement pour s'assurer que ces conditions sont respectées en pratique.

52. Compte tenu de la sensibilité et confidentialité particulière des données traitées dans le secteur visé par la présente recommandation, il convient également de réaliser un examen de « due diligence » des sous-traitants (et des sous-traitants ultérieurs) afin de vérifier leur aptitude à respecter les mesures organisationnelles, techniques et contractuelles normalement imposées à tout sous-traitant. L'examen doit se faire au niveau de l'entreprise concernée et pas uniquement à l'égard du groupe auquel elle appartient.

3. La Commission recommande aux sociétés émettrices de cartes de paiement établies en Belgique clients d'Atos Worldline/EquensWorldline de mettre en place des procédures pour respecter les règles en matière de transferts internationaux de données à caractère personnel

53. Des procédures permettant d'assurer que les articles 21 et 22 de la LVP sont respectés doivent être mises en place par les sociétés émettrices de cartes de paiement établies en Belgique clients d'Atos Worldline/EquensWorldline. . La Commission considère qu'une mesure utile à cet égard serait la mise en place d'un registre interne des transferts internationaux de données personnelles (tant au sein du groupe qu'en dehors du groupe). Cette mesure deviendra obligatoire dès l'entrée en vigueur du Règlement européen à la protection des données le 25 mai 2018 . Ces sociétés devraient également mettre en place des mesures pour que des garanties appropriées, telles des clauses contractuelles types, soient mises en place avant le début de tout transfert régulier et impliquant un nombre important de données personnelles (en ce compris lorsqu'ils sont réalisés par leurs sous-traitants). Ceci implique une information et formation adéquate de leur personnel.

54. Outre le cas du §10 de la présente recommandation, la Commission a pris connaissance de l'initiative récente de equensWorldline de proposer à ses clients belges de signer, via mandat, des clauses contractuelles types 2010/87/UE pour l'encadrement juridique des transferts internationaux effectués par equensWorldline. Cette solution ne pourra avoir d'effet que si l'ensemble des clients bénéficiant de ces services à l'étranger ont accepté de signer ces contrats (et donc accepté l'intervention de ces sociétés pour la prestation de leurs services) et n'aura d'effet qu'à compter de la date de leur signature.

L'Administrateur f.f., Le Président,

(sé) An Machtens (sé) Willem Debeuckelaere