Plaidoyer visant à l'adoption rapide d'un acte uniforme OHADA sur la protection des données à caractère personnel

Jean-François HENROTTE
& Coco KAYUDI MISAMU

I. Introduction

La mondialisation du numérique, l'utilisation de l'Internet, l'utilisation de nouvelles technologies et le besoin de communication et de consommation des services … sont des occasions donnant lieu à des traitements de données à caractère personnel.

En effet, plus personne n'échappe à la collecte des données personnelles pour des raisons telles qu'évoquées ci-dessus.

On peut lire dans un rapport intitulé : *Surveillance Giants* récemment publié par une grande organisation de défenses des droits l'homme « Google et Facebook dominent nos vies modernes ; ils ont accumulé un pouvoir inégalé sur la sphère du numérique en collectant et en *monétisant les données personnelles de milliards d'utilisateurs*. Leur contrôle insidieux de nos vies numériques sape le fondement même de la vie privée et c'est l'un des défis majeurs de notre époque en termes de droits humains ».

Nous partageons le point de vue de Kumi Naidoo, secrétaire général d'Amnisty International, lorsqu'il écrit « À l'ère numérique, afin de protéger nos valeurs humaines fondamentales – dignité, autonomie et vie privée – il faut une refonte radicale du fonctionnement des géants de la haute technologie et l'essor d'un Internet qui accorde la priorité aux droits humains ».

La protection de la vie privée doit également être une priorité pour les États parce qu'ils sont également responsables de traitement pour des fins diverses.

On pense par exemple à l'introduction de la dimension électronique dans le Registre du Commerce et du Crédit Mobilier (RCCM) et ses fichiers connexes institués par les articles 34 et suivant de l'acte uniforme révisé portant sur le droit commercial général, adopté le 15 décembre 2010 à Lomé.

Une telle base de données à caractère personnel présente évidemment des dangers pour les commerçants dont les données à caractère personnel sont traitées, dangers auxquels nous pensons, à l'instar de D. Allechi dans sa contribution « L'informatisation du RCCM et la protection des données à caractère personnel », qu'il devrait être obvié par une législation relative à la protection des données.

Enfin, une telle législation, si elle est reconnue par la Commission européenne comme offrant un niveau de protection adéquat, facilite le transfert de données à caractère personnel encadrées par le règlement général sur la protection des données à caractère personnel vers ces pays tiers (voy. infra).

La Convention de l'Union africaine (UA) sur la cybersécurité et la protection des données à caractère personnel – appelée aussi « Convention de Malabo » – a été adoptée à cette fin le 27 juin 2014.

Pour faciliter la mise en œuvre de la Convention, la Commission de l'Union africaine a demandé à l'Internet Society d'élaborer conjointement les lignes directrices du 9 mai 2018 sur la protection de la vie privée et des données à caractère personnel pour l'Afrique.

Elle vise, en vertu de son article 8, à ce que chaque État partie mette en place un cadre juridique ayant pour objet de renforcer les droits fondamentaux et les libertés publiques, notamment la protection des données physiques et de réprimer toute infraction relative à toute atteinte à la vie privée sans préjudice du principe de la liberté de circulation des données à caractère personnel.

> Malgré l'inspiration commune de la directive 95/46, les législations européennes étaient trop diverses et cela nuisait à l'efficacité des entreprises européennes et à la libre circulation des données.

L'échéance des dernières signatures était fixée au 14 mars 2018. Or, force est constater que seuls 14 pays sur les 55 de l'Afrique ont signé cette convention : Bénin, Tchad, Comores, Congo, Ghana, Guinée-Bissau, Mozambique, Mauritanie, Rwanda, Sierra Leone, São Tomé-et-Príncipe, Togo, Tunisie et Zambie.

Et encore, seulement cinq pays – Ghana, Guinée, Ile Maurice, Namibie et Sénégal – l'ont ratifiée pour que celle-ci entre en vigueur sur leur territoire national …

La Convention n'entrera en vigueur 30 jours après le dépôt du 15e instrument de ratification.

On peut donc craindre, avec C. de Laubier dans sa contribution « L'Afrique se met en ordre de bataille contre la cybermalveillance et la cybercriminalité », que cette convention soit un échec.

Si l'on examine les législations des États OHADA, tous les États parties ne sont pas dotés d'une telle législation et parmi ceux qui en sont dotés, certaines de leur législation sont obsolètes :

- Le Benin est doté d'une loi 2009-09 du 27 avril 2009 portant protection des données à caractère personnel ;
- Le Burkina Faso est doté d'une loi 010-2004/AN du 20 avril 2004 portant protection des données à caractère personnel ;
- Le Cameroun est doté d'une loi 2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité ;
- Le Congo-Brazzaville a adopté le 30 juillet 2019 une loi portant protection des données à caractère personnel ;
- La Cote d'ivoire est dotée d'une loi 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel ;
- Le Gabon est doté d'une loi 01-2011 du 25 septembre 2011 relative à la protection des données à caractère personnel ;
- La Guinée est dotée d'une loi 2016/037 du 28 juillet 2016 relative à la protection des données à caractère personnel ;
- Le Mali est doté d'une loi 2013-015 du 21 mai 2013 portant protection des données à caractère personnel ;
- Le Niger est doté d'une loi 2017-28 du 3 mai 2017 relative à la protection des données à caractère personnel ;
- Le Sénégal est doté d'une loi 2008-12 du 25 janvier 2008 sur la protection des données à caractère personnel ;
- Le Tchad, notre hôte, est doté d'une loi 007/PR/2015 du 10 février 2015 portant protection des données à caractère personnel ;
- Et enfin, le Togo vient de se doter d'une loi 2019-014 du 29 octobre 2019 relative à la protection des données à caractère personnel.

II. Plaidoyer pour l'adoption d'un acte uniforme OHADA sur la protection des données à caractère personnel et à la libre circulation de ces données

L'Union européenne s'est dotée d'un nouveau règlement général sur la protection des données à caractère personnel (RGPD) pour deux raisons : une uniformisation de la législation au sein de l'Union et une prise en compte des nouvelles technologies et des nouveaux risques pour la protection de la vie privée.

En effet, malgré l'inspiration commune de la directive 95/46, les législations européennes étaient trop diverses et cela nuisait à l'efficacité des entreprises européennes et à la libre circulation des données.

Par ailleurs, si en 1995 on se méfiait des États, il devenait urgent d'encadrer également l'activité des GAFA et leurs nouveaux moyens technologiques.

Du fait de l'hétérogénéité de législations, parfois obsolètes, de ses États parties et que certains de ceux-ci ne disposent même pas de législation sur la protection des données, nous estimons, à l'instar d'autres auteurs comme Mouhamadou Lô, auteur d'un livre sur « La protection des données à caractère personnel en Afrique », qu'il est temps pour l'OHADA de se doter d'un acte uniforme 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, à l'instar du RGPD.

Un tel acte pourrait en outre être reconnu comme offrant un niveau de protection adéquat autorisant le transfert de données à caractère personnel de l'Union européenne vers les États parties de l'OHADA (voy. infra).

À défaut, les entreprises africaines seront en outre victimes si pas du protectionnisme de l'Union européenne, de sa stricte protection des données.

III. La stricte protection des données à caractère personnel au sein de l'Union européenne du RGPD

En effet, les règles encadrant la vie privée et les traitements de données à caractère personnel en vigueur au sein de l'Union européenne sont considérées internationalement comme étant particulièrement protectrices des citoyens, ou contraignantes pour les entreprises, spécialement non européennes, selon le point de vue.

Bien qu'appliqué avec plus ou moins de vigueur selon les États membres et les différentes autorités nationales de protection des données, le RGPD forme un cadre cohérent à l'intérieur des frontières de l'Union.

Toutefois, les flux internationaux de données sont inhérents au monde globalisé dans lequel les citoyens de l'Union se meuvent, singulièrement depuis l'avènement du Cloud, dont les plus grands acteurs ne se situent pas sur le territoire européen.

L'utilisateur d'Internet ne sait pas toujours si le site web qu'il va visiter et auquel il va fournir des données est établi ou non sur le territoire de l'Espace économique européen (EEE).

L'utilisateur d'Internet ne sait pas toujours si le site web qu'il va visiter et auquel il va fournir des données est établi ou non sur le territoire de l'Espace Economique Européen (le RGPD est en vigueur en Islande, Norvège et Liechtenstein).

Des données à caractère personnel peuvent donc être traitées dans d'autres pays du globe n'offrant pas un niveau de protection de la vie privée équivalent, voire aucune protection.

La portée des droits conférés par le règlement serait dérisoire si les internautes européens bénéficiaient d'une protection précaire face aux entreprises étrangères qui exercent des activités dans l'EEE.

La technologie et la globalisation induisent une multitude de transferts de données transfrontières. Le responsable du traitement, soumis au règlement, peut transférer les données à caractère personnel vers

des tiers ou faire appel à des sous-traitants étrangers. Le RGPD autorise ces flux, mais les règles sont différentes lorsque les données sont transférées au sein de ou en dehors de l'Union européenne.

IV. Les transferts de données à des responsables de traitement ou à des sous-traitants établis en-dehors de l'Union européenne

Grâce au RGPD, les États membres appliquent le même niveau de protection lors du traitement de données à caractère personnel.

Un transfert **au sein de** l'Union européenne est par conséquent autorisé et régi de la même manière qu'un transfert au sein d'un même État et doit donc respecter les principes généraux de la réglementation (respect notamment des principes de légitimité, compatibilité de la communication avec le traitement d'origine, information des personnes concernées).

Les choses sont différentes si le responsable de traitement souhaite exporter des données à caractère personnel **hors de** l'Union européenne.

L'article 44 du RGPD dispose qu' : « un transfert, vers un pays tiers ou à une organisation internationale, de données à caractère personnel qui font ou sont destinées à faire l'objet d'un traitement après ce transfert ne peut avoir lieu que si, sous réserve des autres dispositions du présent règlement, les conditions définies dans le présent chapitre sont respectées par le responsable du traitement et le sous-traitant, y compris pour les transferts ultérieurs de données à caractère personnel au départ du pays tiers ou de l'organisation internationale vers un autre pays tiers ou à une autre organisation internationale. Toutes les dispositions du présent chapitre sont appliquées de manière à ce que le niveau de protection des personnes physiques garanti par le présent règlement ne soit pas compromis. »

Ni la directive antérieure 95/46, ni le règlement ne définissent cette notion de «transfert». Le transfert de données suppose un déplacement effectif de données à l'étranger, quel que soit le support utilisé, dans le but de faire l'objet d'un traitement. Rendre accessible des données sur un serveur informatique à partir de l'étranger ne constituerait par contre pas un transfert selon une frange de la doctrine[1] se basant sur une interprétation de l'arrêt *Lindqvist* de la Cour de Justice. Cette interprétation est toutefois critiquée par une autre partie de la doctrine[2].

En suivant ces derniers auteurs, il convient effectivement de tenir compte du caractère limité de la question préjudicielle ayant amené la Cour de Justice à se prononcer en partie sur la notion de transfert dans l'arrêt *Lindqvist*.

Une manière de réconcilier les positions tout en tenant compte du libellé du RGPD est de considérer que le transfert de données visé par le RGPD suppose, à la fois, un déplacement effectif de donnée et un objectif de traitement dans un pays tiers.

Il est à noter que le transfert de données constitue en tant que tel un traitement de données et qu'il doit donc respecter, outre les règles encadrant le transfert, l'ensemble des règles afférentes aux traitements de données en général.

L'article 44 du RGPD pose comme principe l'interdiction des transferts de données vers des pays n'offrant pas un niveau de protection adéquat.

Différents régimes permettent d'aboutir à ce niveau de protection adéquat, à différentes conditions. Des États non européens peuvent avoir mis en place un niveau de protection suffisant, leur permettant d'être reconnus.

Les transferts vers un État tiers ou une organisation internationale peuvent se faire si la Commission européenne a constaté, par voie de décision qu'un État tiers, un territoire ou un secteur spécifique de cet État tiers ou l'organisation internationale concernée présente un niveau de protection adéquat.

En effet, l'article 45 du règlement autorise la Commission européenne à décider qu'un État tiers (voire un territoire ou un secteur spécifique – comme le secteur privé ou un secteur économique particulier[3] – de cet État tiers) ou qu'une organisation internationale présente un niveau suffisant de protection des données, de telle sorte qu'aucune autorisation spécifique ne sera nécessaire pour transférer des données vers ces entités.

Le règlement formalise et étend les critères déjà examinés *in concreto* par la Commission ou les Autorités nationales pour déterminer si un état offre un niveau de protection adéquat (ou si des BCR sont valables au regard du droit européen). De manière générale à travers l'ensemble du RGPD, les procédures à suivre sont également détaillées afin de dégager des solutions cohérentes, par référence soit à la procédure de concertation contenue dans le règlement, soit à la procédure d'examen contenue dans le règlement 182/2011 du Parlement Européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission. En l'occurrence, en vertu de l'article 93.2, la procédure prévoit un avis préalable du Comité Européen de la Protection des Données (CEPD) et renvoie, pour les modalités pratiques de l'examen à la procédure décrite à l'article 5 du règlement 182/2011.

Dans son processus d'évaluation, la Commission devra particulièrement tenir compte des éléments listés à l'article 45, plus nombreux et plus précis que ceux contenus dans la directive 95/46.

La décision devrait préciser sa portée territoriale et, si possible, identifier l'Autorité indépendante de Protection des données.

Un document de travail wp254$^{rev.}$01 du Groupe de travail de l'article 29, désormais CEPD, établit les critères de référence pour l'adéquation.

Une intéressante nouveauté par rapport à la situation actuelle réside dans l'obligation pour la Commission de surveiller le déroulement effectif des transferts réalisés sur base de cette décision et de vérifier que l'État tiers ou l'organisation internationale concernée présente **toujours** un niveau de protection adéquat. À défaut, la Commission peut entrer en discussion avec l'État tiers ou l'organisation en vue de trouver une solution et amender ou suspendre la décision, sans possibilité de rétroaction toutefois. La Commission peut également décider, suivant le considérant 106, qu'un État tiers ne présente pas de niveau de

protection adéquat et interdire les transferts vers ces États tiers, sous réserve de l'application des articles 46 à 49.

La modification ou la suspension de la décision doit également respecter la procédure décrite à l'article 5 du règlement 182/2011.

Outre les trois membres de l'Espace Économique Européen que sont la Norvège, le Liechtenstein et l'Islande, au jour de la rédaction des présentes, les pays suivants sont considérés par la Commission comme présentant un niveau de protection adéquat : la Suisse, le Canada (pour les traitements soumis à la loi canadienne «Personal Information Protection and Electronic Documentation Act» et pour les données relatives aux passagers aériens), Andorre, l'Argentine, les États-Unis (si le destinataire des données aux États-Unis a adhéré aux « principes du bouclier de sécurité», ou «Privacy Shield» ainsi que pour les données relatives aux passagers aériens), Guernesey, l'île de Man, les îles Féroé, Jersey, l'Australie (pour les données relatives aux passagers aériens), Israël, la Nouvelle-Zélande, l'Uruguay et le Japon.

Dans les limites éventuellement édictées par la Commission et dans les limites du champ d'application du RGPD, des données à caractère personnel peuvent donc être transmises vers ces pays à des fins de traitement, moyennant uniquement le respect de l'ensemble des règles encadrant la protection des données dans l'État membre de départ.

Aucun pays africain n'est reconnu comme offrant un niveau de protection adéquat.

En l'absence de décision d'adéquation, le transfert ne peut donc se faire vers un *État* africain que moyennant des garanties appropriées offertes par le responsable du traitement ou par le sous-traitant, garanties coulées dans un instrument juridique contraignant, par exemple des clauses contractuelles, des règles d'entreprise contraignantes ou des codes de conduite ou mécanisme de certification. Le règlement prévoit enfin un certain nombre d'exceptions (le consentement de la personne concernée, le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat ou à la constatation, à l'exercice ou à la défense de droits en justice[4] …).

V. Conclusions

La collecte des données à caractère personnel est soit subie (à l'utilisation des services) soit obligatoire (imposé par l'État pour des besoins d'identification de la personne ou des de sécurité nationale). Dans les deux cas, personne concernée se voit contraint par une machine puissante contre laquelle elle n'a d'autre choix que de subir.

Il revient donc aux États de garantir la protection des données de types divers, collectées à différents niveaux. Il est sidérant de voir les collecteurs de ces données les vendre à l'insu et/ou contre le gré des personnes concernées (usagers de services).

L'intervention des États devrait garantir un traitement transparent des données à caractère personnel exclusivement pour les finalités pour lesquelles elles sont collectées. Il est impérieux que les États, particulièrement africains, se dotent d'une loi pour encadrer les traitements de données à caractère personnel. Il faut également prévoir la création d'autorités de protection des données chargées d'assurer le contrôle et sanctionner les abus et tout manquement à la loi.

En plein essor de la quatrième révolution, celle du numérique, les États africains devraient prendre leur destin en main afin d'éviter de subir le même sort que lors des trois dernières révolutions notamment agricole et industrielle.

Nous plaidons donc pour l'adoption rapide par l'OHADA d'un acte uniforme 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.

L'acte uniforme relatif à la protection des données à caractère personnel que nous appelons de nos vœux pourra, outre la protection moderne des personnes concernées elles-mêmes, à terme, être reconnu par la Commission européenne comme offrant un niveau de protection adéquat et permettre donc de mêmes transferts aisés.

Dans l'intervalle, mais également pour les responsables du traitement établis dans les autres États tiers, les responsables de traitement peuvent utiliser une des options offertes par le RGPD : par exemple des règles d'entreprise contraignantes, des clauses contractuelles types ou particulières, passer par le mécanisme de la certification ou l'adhésion à un code de conduite. Le règlement prévoit enfin un certain nombre d'exceptions que les entreprises, et leurs conseils, pourront exploiter.

Une chose est sûre : le RGPD est exigeant, mais n'est qu'un cadre. Il autorise encore les traitements de données à caractère personnel dans l'Union européenne et dans le reste du monde.

L'article 44 du RGPD pose comme principe l'interdiction des transferts de données vers des pays n'offrant pas un niveau de protection adéquat.

Il convient néanmoins que les responsables du traitement situés dans les États tiers maîtrisent, avec leurs conseils, le RGPD. Ce sera bientôt la clef obligatoire pour continuer à traiter avec des entreprises européennes.

Jean-François HENROTTE
Avocat aux barreaux de Liège et de Bruxelles
Directeur de la Stratégie Digitale de l'UIA
Lexing
Liège, Belgique
jf.henrotte@lexing.be

Coco KAYUDI MISAMU
Bâtonnier du barreau de Kinshasa-Matete
Etude Bâtonnier Kayudi
Kinshasa, R.D. Congo
ckayudi@gmail.com

1. V. notamment l'avis prudent de B. DOCQUIR, «*Le droit de la vie privée*», Bruxelles, Larcier, 2008, p. 244.

2. V. notamment C. DE TERWAGNE (ed.), «*Vie privée et données à caractère personnel*», Bruxelles, Politiea, 2014, chapitre 4.2/2.

3. Considérant 104.

4. Que ce soit dans une procédure judiciaire, dans une procédure administrative ou toute procédure à l'amiable, y compris les procédures devant les organismes de réglementation, considérant 111.

Juriste International : editorial policy

The aim of Juriste International *is to offer a forum for discussion and information on issues of interest to practising lawyers throughout the world.*
Juriste International *will not avoid difficult or controversial issues. A journal which covered only the safe or easy issues, or which only published articles expressing the consensus view or the opinions of the majority, would not be worth reading.*
The views expressed in articles in Juriste International *are the views of the authors. Publication in* Juriste International *does not imply that either the UIA or* Juriste International *shares or supports those views.*
Publication or dissemination of advertising or promotional material does not indicate endorsement or support of any product, service, person or organisation by the UIA or Juriste International.

Juriste International : politique éditoriale

L'objectif du Juriste International *est d'offrir un forum de débats et d'informations sur des sujets qui intéressent les juristes en exercice dans le monde entier.*
Le Juriste International *n'esquivera pas les questions délicates ou controversées. Une publication qui ne viserait que des sujets faciles et sans risques ou qui ne publierait que des articles exprimant des opinions unanimes ou majoritaires ne vaudrait pas la peine d'être lue.*
Les opinions exprimées dans le Juriste International *ne reflètent que celles de leurs auteurs. La publication dans le* Juriste International *n'implique ni que l'UIA ni que le* Juriste International *partagent ou soutiennent ces opinions.*
La publication ou la dissémination de matériel publicitaire ou promotionnel par le Juriste International *n'indique en aucun cas l'approbation des produits, services, personnes ou organisations par l'UIA ou par le* Juriste International.

Juriste International : política editorial

El objetivo de Juriste International *es el de ofrecer un fórum de debate e información sobre temas que interesan a los juristas en ejercicio en el mundo entero.*
Juriste International *no eludirá las cuestiones delicadas o controvertidas. No valdría la pena leer una publicación que trate únicamente sobre temas fáciles y sin riesgo, o que publique tan sólo artículos que expresen opiniones unánimes o mayoritarias.*
Las opiniones expresadas en Juriste International *son sólo el reflejo del punto de vista de sus autores. Su publicación en* Juriste International *no implica que la UIA o* Juriste International *comparta o apoye dichas opiniones.*
La publicación o distribución de material publicitario o promocional en Juriste International *no indica en ningún caso la aprobación de los productos, servicios, personas u organizaciones por parte de la UIA o de* Juriste International.

JURISTE INTERNATIONAL

UIA PUBLICATION / PUBLICATION DE L'UIA / PUBLICACIÓN DE LA UIA

Publication Director / Directeur de la Publication / Director de la Publicación
President Jerome ROTH

Union Internationale des Avocats (UIA)
20, rue Drouot,
75009 Paris (France)
Tel. +33 1 44 88 55 66 - Fax. + 33 1 44 88 55 77
E-mail : uiacentre@uianet.org
Site Web : www.uianet.org
ISSN : 0758-2471

EDITORIAL TEAM / ÉQUIPE DE REDACTION / EQUIPO DE REDACCIÓN

Nicole VAN CROMBRUGGHE,
Chief Editor / Rédacteur en Chef / Redactor Jefe

Barbara GISLASON,
Deputy Chief Editor / Rédacteur en Chef Adjoint / Redactor Jefe Adjunto

Section Directors / Directeurs de rubriques / Directores de sección

UIA News / Actualités de l'UIA / Novedades de la UIA
Paolo LOMBARDI

Human Rights and Protection of Lawyers / Droits de l'Homme et de la Défense / Derechos Humanos y de la Defensa
Romina BOSSA ABIVEN ⇨ Nadine DOSSOU ⇨ Gustavo SALAS RODRIGUEZ

The Legal Profession / La Profession d'Avocat / La Abogacía
⇨ Pierluca DEGNI ⇨ Aboubacar FALL ⇨ Mary-Daphné FISHELSON

Legal Practice / Pratique du Droit / Ejercicio de la Abogacía
Marc GALLARDO MESEGUER ⇨ Christoph ÖRTEL ⇨ Steven RICHMAN

Young Lawyers representative / Représentant Jeunes Avocats / Representante Jóvenes Abogados
Thomas RUDKIN

Editorial Assistant / Secrétaire de Rédaction / Secretaria de Redacción
Marie-Pierre RICHARD

ADVERTISING SALES AGENCY/ RÉGIE PUBLICITAIRE / AGENCIA DE MEDIOS

SEEPP - Régis LAURENT
7, rue du Général Clergerie - 75116 Paris - France - Tél. : +33 1 47 27 50 05
seepp@wanadoo.fr

Typesetting and printing / Composition et impression / Composición e impresión
Evoluprint - Parc Industriel Euronord - 10 rue du Parc
CS 85001 Bruguières - 31151 Fenouillet Cedex

Circulation - Distribution / Tirage - Distribution / Tirada - Distribución
3 000 exemplaires / copies / ejemplares

Photos credit / Crédit photos / Crédito fotos
Cover: © Shutterstock / Page 1: © Shutterstock - Rawpixel.com /
Page 2 (Upper): © Shutterstock - Ivelin Radkov; (Lower): © Shutterstock - Purple Anvil /
Page 6: © UIA / page 14: © UIA / Pages 11 et 13: © Pixabay - Mohamed Hassaan /
Page 16: © Shutterstock / Page 15: © UIA /
Page 22 (Upper): © Shutterstock - Photographee.eu; (Lower): © Shutterstock - Edward Crawford /
Page 23: © Shutterstock - Doom.ko / Page 24-25: © UIA /
Page 28 (Upper): © Shutterstock - HQuality; (Lower): © Shutterstock: SariArLawKa2 /
Page 30: © Shutterstock / Page 36: © Shutterstock - GaudiLab /
Page 38 (Upper): © Shutterstock - santima.studio, (Lower: © Shutterstock - Jiw Ingka /
Page 40: © Shutterstock - TarikVision / Page 53: © Shutterstock - Bakhtiar Zein / Page 54 : Shutterstock /
Page 58: © Shutterstock - Yevhen Vitte / Page 63: © Shutterstock - Olivier Le Moal /
Page 64 : © ShutterstockPage 65: © Shutterstock - PhuShutter / Page 67: © Shutterstock - Bakhtiar Zein /
Page 68: © Shutterstock –Viktoria Kurpas / Page 73, 74 & 75 : © Shutterstock

your legal, tax and
business services firm
in Luxembourg

arendt

legal, tax and regulatory change

we are with you all the way

arendt.com