



FEDIL

The Voice of Luxembourg's Industry



Comment préparer votre entreprise à l'entrée en vigueur du Règlement Général sur la protection des données (RGPD) ?

15 mars 2017



01

Mot de bienvenue

M. René Winkin, Directeur, FEDIL

Introduction à la problématique et actions de la FEDIL

***Mme Magalie Lysiak, Adviser
FEDIL***

Une réglementation dépassée

- Anciens textes : Directive 95/46/CE qui datait de 1995 et décision cadre de 2008 relative à la protection des données traitées dans le cadre de la coopération policière et judiciaire en matière pénale
- Actualisation et modernisation nécessaire
- Nécessité d'un renforcement des droits dans un monde de plus en plus digitalisé
 - Réseaux sociaux,
 - Captation et transferts de données toujours plus importants,
 - ...

Un besoin d'adaptation

- Avancée importante sur la protection des données
 - Tente à la fois d'améliorer la protection des personnes concernées par le traitement des données,
 - Mais aussi de tenir compte de l'évolution technologique et numérique depuis la directive de 1995.
- Parmi les grandes avancées :
 - Élargissement du champs d'application territorial
 - Renforcement des principes liés au traitement de données à caractère personnel et notamment les données sensibles

Un besoin d'uniformisation

- Adopté sous la forme d'un règlement...
 - Pour pallier aux lacunes de la directive
 - « Level playing field »
- ...qui laisse une importante marge d'appréciation aux Etats membres
 - « Les Etats membres peuvent / peuvent prévoir... »
 - « au titre du droit de l'UE ou du droit d'un Etat membre... »
- De sorte que des mesures de transposition sont rendues nécessaires

Un texte de compromis

- Discussions en cours depuis 2012
- 173 considérants
 - Considérants traditionnels : raisons et justifications du Règlement
 - Considérants « explicatifs »
- Velléités normatives par un contenu additionnel
- Absence de consensus politique

La consécration d'un ensemble de nouveaux droits

- Droit à l'oubli numérique et à l'effacement
- Droit à la limitation du traitement
- Droit à la portabilité des données
- Le rôle accru du responsable du traitement et l'encadrement de la sous-traitance

La FEDIL comme partenaire

- Groupe de travail sur la question
 - Présence de nombreuses sociétés : Post, Encevo, Luxair, Cargolux, Securitas, Adecco, Luxtrust, RTL, etc.
- Réflexion sur les besoins de transposition :
 - Rôle de la CNPD
 - Clarification nécessaire de certaines missions des différentes parties prenantes et interprétations
 - Opportunité d'un avantage concurrentiel pour le Luxembourg

Premières conclusions

- Beaucoup de questions se posent encore et notamment dans l'application concrète de ce nouveau règlement
- Les entreprises sont très attachées aux relations « d'accompagnement » de la CNPD et ne souhaitent pas perdre ceci.
 - Idée d'officiers dédiés aux entreprises
 - Renforcement des moyens de la CNPD nécessaire

Premières conclusions

- Le Luxembourg se veut à la pointe en matière d'économie numérique et il faut que nos mesures de transposition lui permette de conserver un avantage concurrentiel
- La souplesse doit être consacrée : autoévaluation doit être privilégiée pour le responsable de traitement
- La législation en matière de droit du travail et de surveillance sur le lieu de travail doit être revue et permettre un élargissement des possibilités de traitement pour les entreprises (formations filmées, sécurité des salariés, etc.)

La protection des données personnelles: quels enjeux ?

***Me Anthony Favier, Associate
DSM Legal***

I. Notions Fondamentales

II. Règles en la matière

III. Pourquoi un Règlement européen ?

IV. Importance du respect des règles en matière de protection des données pour les PME : conformité légale et valeur économique

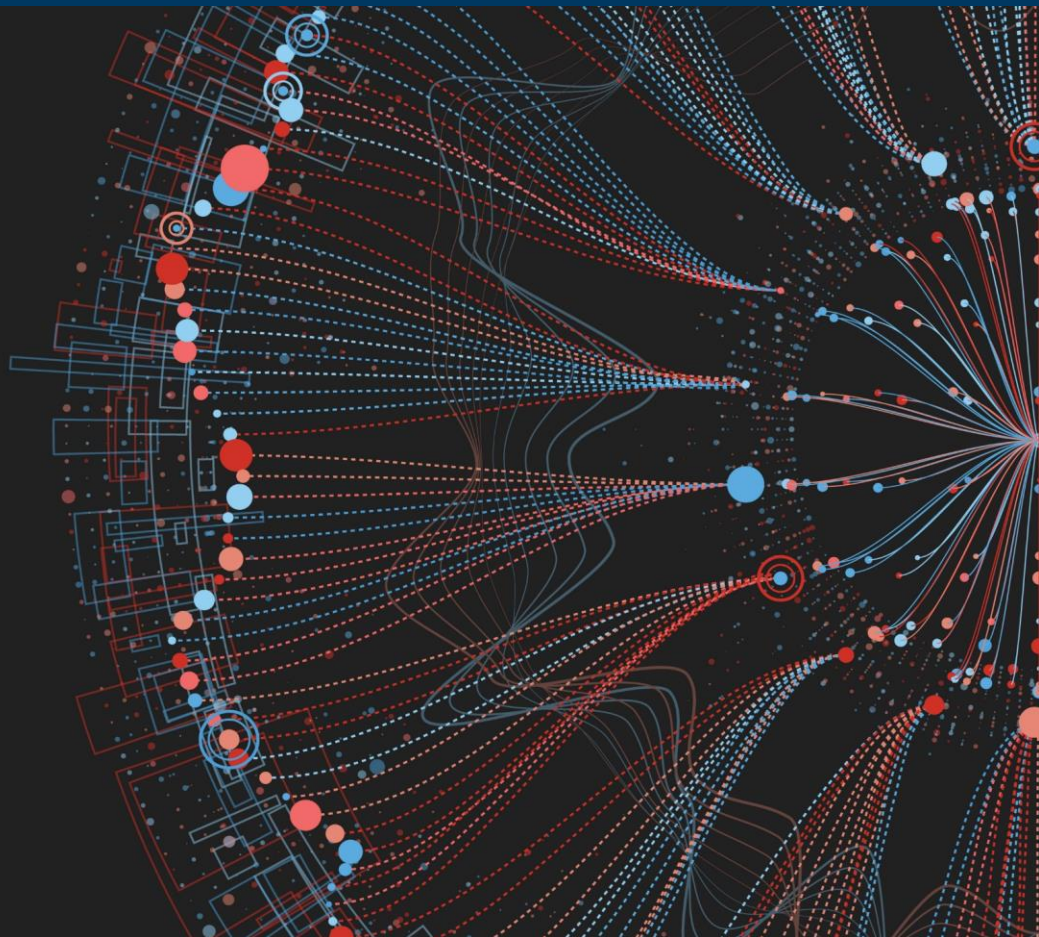
Propos introductifs

- Cadre actuel avec la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (telle que modifiée) – transposition de la Directive 95/46/CE
- Anticiper l'arrivée et l'effet direct du Règlement européen 2016/679 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 (« RGPD »)
- Position des pouvoirs publics à suivre

Propos introductifs

- Données... une mine d'or
- Développement de nouveaux outils d'analyse
- Publicité comportementale
- Tracking : mesure d'audience
- Biométrie : objets connectés (ex: Withings)

ADVANCED ANALYTICS
BIG DATA
AND VISUALIZATION



I. Notions Fondamentales

Directive 95/46/CE

«**données à caractère personnel**»: toute information concernant une personne physique identifiée ou identifiable (personne concernée); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale

Règlement 2016/679

«**données à caractère personnel**», toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, **des données de localisation, un identifiant en ligne**, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale

Notion variable de „donnée personnelle“:

→ Propre aux personnes physiques

→ Conseil d'Etat (France) : personnes morales n'entrent pas dans le champ d'application de la loi (informatique et libertés)

→ Données dites „sensibles“ (régime spécifique)

- Exemple de l'adresse IP :

« la collecte pendant plusieurs années, d'adresses IP qui permettent l'identification des utilisateurs constitue un traitement automatisé de données à caractère personnel contenu dans un fichier lequel doit donner lieu à déclaration à la CNIL ».

C.Cass (France) 03-11-2016 pourvoi n°15-22595

Directive 95/46/CE	Règlement 2016/679
<p>«traitement de données à caractère personnel» (traitement): toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.</p>	<p>«traitement», toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données <u>ou des ensembles de données à caractère personnel</u>, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.</p>

Responsable du traitement (Data Controller)	Sous-Traitant (Data Processor)
<p>La personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel. Lorsque les finalités et les moyens du traitement sont déterminés par ou en vertu des dispositions légales, le responsable du traitement est déterminé par ou en vertu des critères spécifiques conformément aux dispositions légales</p>	<p>La personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données pour le compte du responsable du traitement</p>

→ **Notions Responsable de traitement/sous-traitant**

→ **Relation contractuelle: rôles respectifs (enjeux/responsabilités) à définir.**

→ **Le nouveau Règlement met les responsables de traitement et les sous-traitants sur un pied d'égalité en matière d'obligations (ex: obligation de tenue des registres).**

→ **En pratique, le responsable de traitement peut perdre la main sur le traitement effectué sur les données qu'il transmet au sous-traitant.**

II. Règles en la matière

Sept principes clés à respecter :

- Principe de finalité : les données à caractère personnel ne peuvent être recueillies et traitées que pour un usage déterminé et légitime.
- Principe de proportionnalité : seules doivent être enregistrées les informations pertinentes et nécessaires pour leur finalité.
- Principe de pertinence : les données personnelles doivent être adéquates, pertinentes et non excessives au regard des objectifs poursuivis.

Sept principes clés à respecter :

- Principe de durée limitée de conservation des données : Les informations ne peuvent être conservées de façon indéfinie dans les fichiers informatiques. Une durée de conservation doit être établie en fonction de la finalité de chaque fichier.
- Principe de sécurité et de confidentialité des données : mesures à prendre par le responsable de traitement (et le sous-traitant) pour garantir la confidentialité des données et éviter leur divulgation.

Sept principes clés à respecter :

Principe de transparence (information) : le responsable du traitement de données personnelles doit avertir/informer les sujets du traitement dès la collecte des données et en cas de transmission de ces données à des tiers.

Principe du respect du droit des sujets du traitement : chaque sujet bénéficie d'un droit d'accès, de rectification ou d'opposition au traitement de ses données personnelles (+ droit à l'oubli, portabilité).

Obligations (loi du 2 août 2002) :

→ Exemptions : ex: traitements RH, gestion paie, comptabilité, etc.

→ Formalités auprès de la CNPD :

- Notification préalable
- Autorisation préalable

Autorisations préalables : des données ou transferts plus „sensibles“

→ Traitement à des fins de surveillance :

- Vidéosurveillance (enregistrement)
- Surveillance (monitoring) de salariés

→ Interconnexion de données : mise en relation automatisée d'informations provenant de fichiers ou de traitements qui étaient au préalable distincts

→ Transfert de données vers un pays tiers (cf n'assurant pas un niveau de protection adéquat)



Projet de loi n°7049 (« smooth transition » vers le RGPD) :

→ simple notification à la CNPD pour :

- Traitement à des fins de surveillance (enregistrement) ;
- Interconnexion de données ;
- Transfert vers des pays tiers n'assurant pas un niveau de protection suffisant si outils contractuels de protection (ex : clauses contractuelles types).

Le RGPD vient „alléger“ lesdites formalités déclaratives en favorisant une compliance en amont (tenue de registres): logique de conformité.

→ Désengorger les autorités nationales de protection des données.

Quelques chiffres :

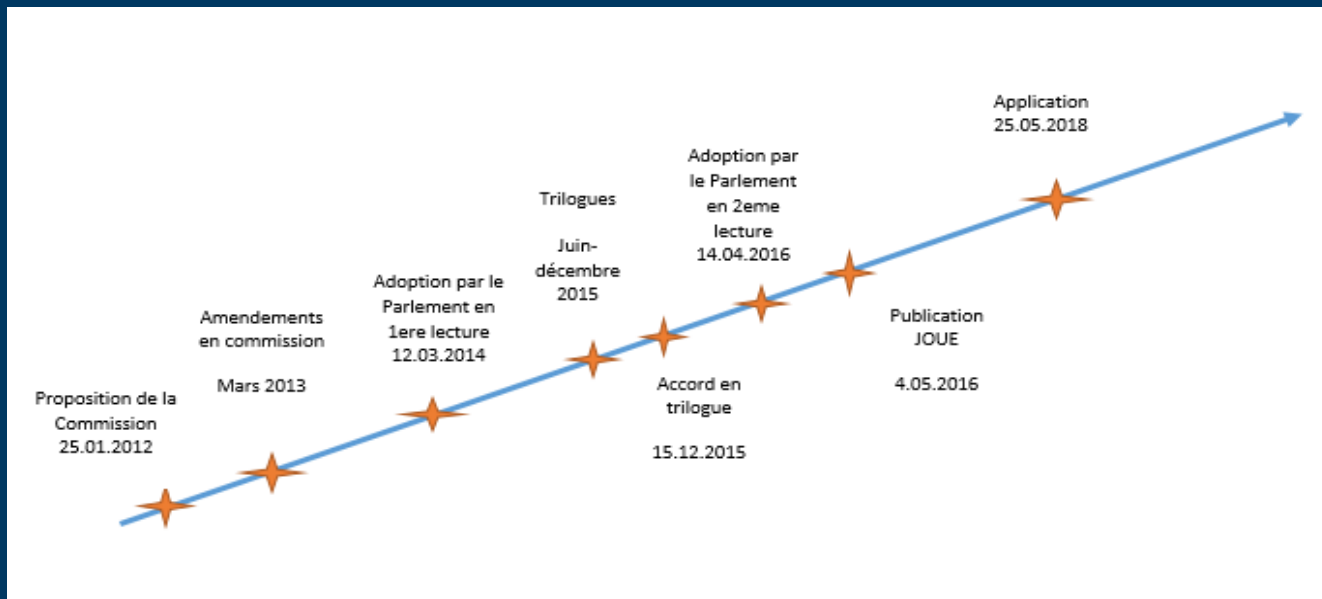
- Rapport annuel 2015 de la CNPD : 705 notifications ordinaires (soit +25% par rapport à 2014).
- 969 demandes d'autorisations préalables.

III. Pourquoi un Règlement européen ?

- Directive 95/45/CE → nécessité de lois de transposition nationales.
- Fragmentation de la mise en œuvre de la protection des données dans l'Union, une insécurité juridique.
- Nécessité d'une application cohérente et homogène des règles de protection des libertés.

- **Besoin d'un cadre juridique plus solide en matière de protection des données (cf « Digital Single Market »).**
- **Les opérateurs étrangers doivent être soumis aux mêmes règles du jeu que les opérateurs européens (“level playing field”).**
- **Consécration de nouveaux droits : ex: droit à l'oubli, portabilité des données, ...**

- Règlement 2016/679 sera donc d'effet direct dans tous les Etats Membres dès le 25 mai 2018.



Le RGPD :

- renforce les droits des citoyens et leur donne plus de maîtrise sur leurs données personnelles,
- allège les formalités préalables pour les organismes qui traitent des données (entreprises, administrations, etc.),
- implique une coopération renforcée entre les autorités de protection européennes.

Quelques objectifs poursuivis par le RGPD :

→ Un cadre juridique unifié pour l'ensemble de l'UE :

Le Règlement s'applique dès lors que le responsable de traitement ou le sous-traitant est établi sur le territoire de l'Union européenne ou que le responsable de traitement ou le sous-traitant met en œuvre des traitements visant à fournir des biens et des services aux résidents européens ou à les « cibler ».

→ Uniformisation de la concurrence avec les opérateurs hors - UE

→ Guichet unique (one-stop-shop) : les entreprises seront en contact avec un « guichet unique », à savoir l'autorité de protection des données de l'État membre où se trouve leur « établissement principal », désignée comme l'autorité « chef de file ».

→ Mécanisme devra être soumis à l'épreuve de l'usage

→ Un renforcement des droits des personnes :

- **Consentement renforcé :** la charge de la preuve du consentement incombe au responsable de traitement.
- **Le droit à la portabilité des données :** ce nouveau droit permet à une personne de récupérer les données qu'elle a fournies sous une forme aisément réutilisable.
- **La protection des données dès la conception et par défaut (privacy by design/privacy by default)**

→ Des responsabilités partagées :

- Le sous-traitant est tenu de respecter des obligations spécifiques en matière de sécurité, de confidentialité et en matière d' « accountability » (procédures internes).
- Il a notamment une obligation de conseil auprès du responsables de traitement pour la conformité à certaines obligations sur règlement (études d'impact, failles, sécurité, destruction des données, contribution aux audits)

IV. Importance du respect des règles en matière de protection des données pour les PME : conformité légale et valeur économique

- Sanctions actuelles (loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel)

→ Un traitement de données effectué en violation des dispositions de la loi est puni d'une peine d'emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 EUR ou d'une de ces peines seulement.

→ Sanctions disciplinaires de la CNPD : ex :

- verrouiller, effacer ou détruire des données faisant l'objet d'un traitement contraire aux dispositions de la loi ou de ses règlements d'exécution;
- interdire temporairement ou définitivement un traitement contraire aux dispositions de la loi ou à ses règlements d'exécution.

- Apports du Règlement :

→ sanctions encadrées, graduées et renforcées

→ les responsables de traitement et les sous-traitants peuvent faire l'objet de sanctions administratives importantes en cas de méconnaissance des dispositions du règlement

Les autorités de protection peuvent notamment :

- Prononcer un avertissement ;
- Mettre en demeure l'entreprise ;
- Limiter temporairement ou définitivement un traitement ;
- Suspendre les flux de données ;
- Ordonner de satisfaire aux demandes d'exercice des droits des personnes ;
- Ordonner la rectification, la limitation ou l'effacement des données.

- Amendes administratives imposées par le Règlement :
 - Jusqu'à 20 millions d'euros, ou, dans le cas d'une entreprise, de 2% jusqu'à 4% du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu.
 - pour les traitements transnationaux, la sanction sera conjointement adoptée entre l'ensemble des autorités concernées, donc potentiellement pour le territoire de toute l'Union européenne.
 - dans ce cas, une seule et même décision de sanction décidée par plusieurs autorités de protection sera infligée à l'entreprise.

Valorisation des données:

- Les données (notamment les fichiers clients) ont une valeur
- Actif du fonds de commerce
- Licéité du fichier est fondamentale pour pouvoir le vendre

- Exemple : liquidation judiciaire Virgin Megastore

Base de données des clients “Fidélités” de Virgin : 1,6 millions de clients

→ Vendu à la FNAC pour 54,000 EUR

→ 3 centimes par client !!

- L'arrêt de la Cour de Cassation française du 25 juin 2013 (n° 12-17.037) – caractère illicite d'un fichier

En espèce, il s'agissait d'une acquisition d'un fonds de commerce de vente de vins aux particuliers qui comprenait un fichier clients informatisé.

L'acquéreur constate que ledit fichier n'a pas été déclaré à la CNIL par le vendeur et demande l'annulation de la vente du fichier pour défaut de déclaration. La Cour de Cassation lui donne gain de cause et prononce la nullité de la vente.

→ Nécessité d'un fichier “dans le commerce”

Valoriser le Big Data

DATAVEYES

Exemple d'application:

<http://dataviz.intersport-rent.fr/>

→ Données de fréquentation par station de sport d'hiver et par période

Sexe

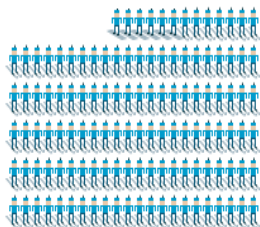
Âge

Niveau

Équipement

Région

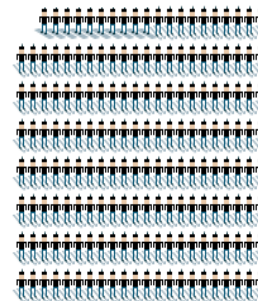
Pays



25% DÉBUTANT



41% INTERMÉDIAIRE

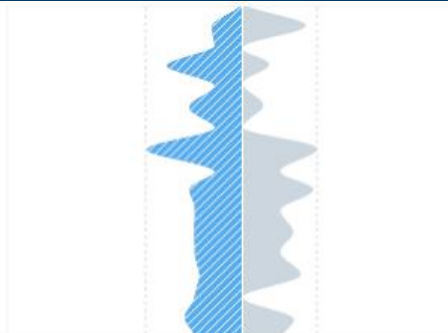


35% BON



GENERATIVE IDENTITY

Dataveyes



WORLDCUP 2014

Twitter France



TWEETS #GOT SEASON 4

Orange Cinéma Séries (OCS)



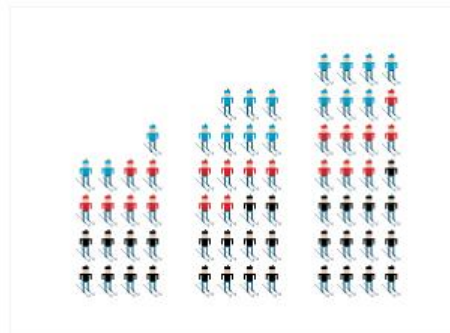
DATATRIP

Lab Dataveyes



BUZZ #CÉSAR 2014

Canal Plus



WHO ARE YOU GOING TO SKI ...

Intersport



Anthony FAVIER

Associate / Avocat à la Cour

afavier@dsm.legal

Merci de votre attention

DSM Avocats à la Cour

55-57 rue de Merl, L-2146 Luxembourg B.P. 2648 | L-1026 Luxembourg

Téléphone : +352 262 562 1

E-mail : contact@dsm.legal

Site web : www.dsmlegal.com

L'impact du RGPD sur l'organisation interne de l'entreprise

***Me Vincent Wellens, Partner
NautaDutilh Avocats***

1. Sensibiliser au sein de l'entreprise

☐ responsabilités accrues

- plus de pouvoirs pour les autorités
- plusieurs autorités susceptibles d'être impliquées dans des affaires transfrontalières
- amendes administratives allant jusqu'à 4% du CA
- responsabilité pénale
- responsabilité solidaire dans les procédures civiles avec d'autres responsables et sous-traitants
- actions collectives
- risque à la réputation
- Cass. fr. (2013): transaction portant sur un fichier illicite = entachée de nullité

☐ vie privée au programme du comité

- ☐ former les employés importants et tout autre personnel clé (effort à l'échelle de la société)
- ☐ réunions spéciales pour CRM, HR, IT, etc.
- ☐ inclure les commentaires du business
- ☐ contact-clé dans chaque secteur d'activité
- ☐ protection des données à inclure dans toutes les politiques de l'entreprise

2. Organiser une bonne gestion (1)

- ☐ des « mesures organisationnelles » adéquates
- ☐ pour les responsables du traitement et pour les sous-traitants
- ☐ budget suffisant
- ☐ ressources internes suffisantes
- ☐ équipe pour la conformité au RGPD:
 - représentants pour toutes les parties prenantes concernées et inclure les postes existants tels que CDA, CIO, (C)ISO
 - plan de conformité au RGPD
 - analyse des lacunes
 - combler les lacunes – consensus commercial!
 - conformité permanente (DPIAs, enregistrement de traitement, ...)
- ☐ rapport régulier à / participation de (tout!) le comité
- ☐ audits réguliers

2. Organiser une bonne gestion (2)

☐ DPD !

- obligatoire lorsque :
 - (i) les activités principales consistent en des opérations de traitement nécessitant une surveillance systématique et à grande échelle
 - (ii) traitement à grande échelle de données sensibles
- missions :
 - (i) information et conseil
 - (ii) surveillance de la conformité
 - (iii) points de contacts des autorités
- DPD pour un seul groupe est possible
- signaler directement au niveau le plus élevé de la hiérarchie
- pas de conflits d'intérêts
- pas d'instructions hiérarchiques

☐ désigner un DPD le plus tôt possible

☐ garantie d'impartialité

- DPD peut être externe

☐ (in)compatibilités avec d'autres fonctions au sein de l'entreprise

- DPD + chargé de conformité = ok
- DPD + CISO, CIO, etc. = pas ok

3. Tracer toutes les données personnelles (1)

- ❑ nouveau principe de responsabilité en matière de qualité des données
- ❑ registres des activités de traitement
 - aucune obligation pour les organisations < 250 personnes à moins qu'il y ait un traitement
 - ✓ susceptible de porter atteinte aux droits et libertés des personnes concernées,
 - ✓ pas occasionnel, ou
 - ✓ comprend des données sensibles
- ❑ pas suffisant d'être conforme, la conformité doit être prouvée
- ❑ audit des données existantes pour l'analyse des lacunes
- ❑ RGPD : obligation de garder les relevés d'opérations de traitement
- ❑ utiliser pour l'audit pré-RGPD le même format que celui requis par le RGPD

3. Tracer toutes les données personnelles (2)

- les registres doivent comprendre

- ✓ coordonnées du responsable du traitement (incl. DPD)
- ✓ catégories de données
- ✓ finalités du traitement
- ✓ catégories de personnes concernées
- ✓ catégories de destinataires
- ✓ informations sur les transferts de données vers un pays hors de l'UE/EEA
- ✓ délais d'effacement
- ✓ description générale des mesures de sécurité

- ✓ déterminer si l'entreprise
 - responsable du traitement (déterminant les finalités et moyens) ou
 - sous-traitant (agissant au nom du responsable du traitement)
- ✓ notion large de "données personnelles"
 - "toute information se rapportant à (= à propos) et personne physique identifiée ou identifiable"
 - données tel qu'un nom, une adresse électronique, une adresse physique, des numéros de téléphone, ...
 - mais aussi des exemples moins évidents adresses IP (surtout en cas de profilage), données liées aux fonctions d'administrateur / directeur
- ✓ définition claire des finalités !
 - éviter les incompatibilités
- ✓ idée claire des durées de conservation !
- ✓ identifier également la base de la licéité du traitement

4. Adapter les informations aux personnes concernées (1)

❑ droit fondamental : le droit à l'information

❑ informations

- concises,
- transparentes,
- intelligibles,
- facilement accessibles,
- en utilisant un langage simple et clair

❑ par écrit ou tout autre moyen, y compris par voie électronique

❑ indications pratiques et utiles de l'autorité britannique

The image shows two forms side-by-side, illustrating good and bad practices for data collection. The left form is a good example, while the right form is a bad example.

Left Form (Good Practice):

- Marked with a green checkmark.
- Fields: Date of Birth, Occupation, Address, Post Code.
- Section: **How information about you will be used**
- Text: "We may share your information with credit reference agencies and other companies for use in credit decisions, for fraud prevention and to pursue debtors."
- Text: "We would like to send you information about our own products and services, by post, telephone, email and SMS. If you agree to being contacted in this way, please tick the relevant boxes."
- Options: ☐ Post, ☐ Email, ☐ Phone, ☐ SMS, ☐ Automated phone call.
- Text: "We would also like to share your information with other selected garden products retailers so that they may send you information about their products and services by post. If you agree your information being shared in this way, please tick the box."
- Text: "If you need any further information please write to us at 10 Street Name, Town Name, County Name AB123CD."
- Fields: Customer signature, Date.

Right Form (Bad Practice):

- Marked with a red X.
- Fields: Date of Birth, Occupation, Address, Post Code.
- Section: **LEGAL DECLARATION**
- Text: "X Limited is a company incorporated in England and is a member of the X Retail Group ('the Group'). The Group ('we/us') also includes 'Y' Limited and Z Limited and their associated companies from time to time. The personal identifiable information you provide will be processed in accordance with the Data Protection Acts 1984 and 1998 and other applicable laws. We will use your information so that we can process your order. This includes administering any accounts, processing your bank/credit card details in order to obtain payment, arranging delivery of any goods purchased, and the prevention and detection of fraud. We can hand over your information to anyone to whom we transfer our rights and duties under our agreement with you or if we have a duty to do so and the law allows us to do it. We will use your information for market research and the marketing of our products and services. This may include contacting you by post, telephone, email or SMS unless you indicate you do not want to be contacted in any of these ways by calling us on 0800 23 45 67. We will use your information to search the files of credit reference agencies who will record that search. This information may be used by other lenders in making credit decisions about you, members of your household and those with whom you may be financially linked. Information held about you by the credit reference agencies may already be linked to records relating to people with whom you are financially linked. For the purposes of credit searching, you may be treated as financially linked and you will be assessed with reference to any associated records. We will share our information with other companies, for the purposes of market research and the marketing of their products and services, unless you indicate that you wish to be excluded from such uses by contacting us on 0800 23 45 67. By signing this form you consent to the information you provide being processed for the above purposes."
- Fields: Customer Signature, Date.

Annotations on the Right Form:

- Confusing and legalistic language. Closely spaced text, small italic font in light grey.
- Unnecessary – means little to the public.
- Specific opt-in consent is required for some e-marketing and is good practice for all direct marketing.
- Confusing language.
- No details of what type of companies.
- Bad practice to seek one consent for several types of processing.

4. Adapter les informations aux personnes concernées (2)

❑ la déclaration « vie privée » doit inclure:

- identité et coordonnées du responsable du traitement (et DPD)
- finalités du traitement
- catégories de destinataires
- fondement juridique du traitement
- transfert vers pays tiers
- durée de conservation
- droit de porter plainte au DPA
- origine des données
- existence des droits des personnes concernées
- accès, correction, effacement, objection

❑ vérifier la cohérence avec le registre et vice versa

❑ l'extension substantielle des informations à fournir

❑ exigence d'être concis et transparent

❑ layered approach



> How will we use the information about you?

How will we use the information about you?

Process your order, manage your account, personalise your use of the website and post offers of other products and services we offer to you (if you agree).

May be shared with – members of our group of companies (if you agree). Won't be shared – for marketing purposes outside of our group. [Please follow this link for further information.](#)

5. Adapter le langage de consentement

- ☐ doit être :
 - libre
 - spécifique
 - éclairé et
 - univoque (acte positif!)
- ☐ consentement explicite pour certains types de traitements de données
 - données sensibles (origine ethnique, opinions politiques, religion, données biométriques, santé, ...)
 - profilage (si fondé sur le consentement)
- ☐ consentement des parents pour les mineurs (> 13-16)
- ☐ la charge de la preuve incombe au responsable du traitement
- ☐ analyser et lister les situations pour lesquelles le consentement est requis et de quelle manière
- ☐ attention particulière portée aux traitements sensibles et profilage
- ☐ analyser formulaires de consentement et conditions générales :
 - consentement spécifique : pas de langage unique de consentement
 - vérifier toute la chaîne si l'entreprise n'obtient pas les données de la personne même
- ☐ procédé d'identification des mineurs
- ☐ collecte / archivage des formulaires de consentement sur un support durable !

6. Processus permettant l'exercice des droits des personnes concernées

- | | |
|--|--|
| <ul style="list-style-type: none">❑ droit à :<ul style="list-style-type: none">▪ information (cf. point 5.)▪ accès▪ rectification▪ effacement (droit à l'oubli)<ul style="list-style-type: none">✓ exceptions, telles que la conservation légale▪ restriction▪ portabilité des données !▪ opposition<ul style="list-style-type: none">✓ situation particulière de la personne✓ marketing / profilage▪ ne pas se soumettre à la prise de décision automatisée (profilage) | <ul style="list-style-type: none">❑ ressources suffisantes pour répondre en temps utile et sans frais❑ définir clairement dans quelles situations quels droits peuvent être exercés❑ informations claires permettant à la personne concernée de faire valoir ses droits❑ assurer l'accessibilité des données❑ conserver les données dans un format structuré, couramment utilisé et lisible par une machine❑ veille réglementaire<ul style="list-style-type: none">▪ certaines limitations ne sont pas encore fixées par la loi |
|--|--|

7. Analyse préalable d'impact avant tout nouveau projet

☐ analyse d'impact :

- en cas de risque élevé probable (ex : nouvelles technologies)
- avant le traitement
- liste d'activités nécessitant une analyse d'impact
 - ✓ ex : profilage, surveillance systématique des espaces publics (distributeurs automatiques de billets, etc.), ...
 - ✓ à compléter par l'autorité nationale
- consultation préalable avec l'autorité nationale si l'évaluation révèle un risque élevé

☐ « mini » analyse d'impact pour évaluer si l'impact est probablement élevé ou non

☐ étape obligatoire avant chaque lancement de projet

☐ allouer suffisamment de temps au calendrier du projet pour une analyse d'impact (plus une éventuelle consultation avec l'autorité)

8. Intégrer la protection des données à tous les stades des projets

- ❑ privacy by design:
 - lors de la détermination des moyens de traitement et au moment du traitement
 - mise en œuvre de mesures pour se conformer aux principes de protection des données (ex : la minimisation des données)
 - selon l'état de la technique, le coût, la nature, la portée du traitement
- ❑ privacy by default:
 - mesures garantissant que, par défaut, seules sont traitées les données personnelles nécessaires pour chaque finalité
- ❑ important au moment de choisir les fournisseurs de solutions !
- ❑ mise en œuvre de mesures adaptées sur la base d'audits
- ❑ procédé d'effacement automatique lorsque la durée de conservation expire
- ❑ mesures à rajouter dans les registres de données ?

9. Mettre en place des mesures de sécurité appropriées (1)

- ❑ mesures techniques et organisationnelles appropriées
 - pseudonymisation et cryptage des données
 - confidentialité, intégrité, mise à disposition et résistance permanente des services / systèmes de traitement
 - restauration de la mise à disposition en cas d'incident
 - tester et évaluer régulièrement l'efficacité des mesures
- ❑ codes de conduite/certification
- ❑ des mesures insuffisantes peuvent avoir d'autres conséquences, par exemple :
 - perte de secrets commerciaux
 - risque pour la réputation
- ❑ suffisamment de ressources pour élaborer et prouver la robustesse de la sécurité
- ❑ documenter les mesures de sécurité, tests et manquements
- ❑ s'aligner aux normes existantes comme les normes ISO 27k
- ❑ respecter les codes de conduite

9. Mettre en place des mesures de sécurité appropriées (2)

☐ notification de violation des données :

- à l'autorité : sans retard abusif et lorsque faisable <72h
 - ✓ à moins que la violation des données à caractère personnel ne soit susceptible d'entraîner un risque
- à la personne concernée : sans retard abusif
 - ✓ à moins que la violation des données à caractère personnel ne soit susceptible d'entraîner un risque
 - ✓ Exceptions en cas d'effort disproportionné ou de mise en œuvre de mesures de sécurité appropriées

☐ mettre en œuvre des procédures et solutions de détection, déclaration et enquêtes en matière de violation

☐ prévoir le signalement de violation des données par des fournisseurs externes

☐ prévoir un plan en cas d'incidents relatif à la violation des données

- déterminer à l'avance quel type de violation doit être notifié
- rédiger à l'avance des documents standard

10. Analyser tous les contrats pertinents impliquant un traitement des données personnelles

- ❑ nouvelles obligations et principe général de responsabilité
 - ❑ présomption de responsabilité conjointe responsable / sous-traitant
 - ❑ dispositions obligatoires dans les contrats de sous-traitance
- ❑ analyser les contrats afin de :
 - refléter les nouvelles obligations du responsable de traitement
 - inclure les nouvelles obligations du sous-traitant
 - inclure les dispositions obligatoires
 - définir précisément les rôles et les responsabilités en matière de traitement des données

Un nouveau rôle pour le sous-traitant ou le prestataire collecteur de données

***Me Héloïse Bock, Partner
Arendt & Medernach***

Acteurs concernés (1/2)



- Champ d'application matériel :

Personnes physiques, personnes morales de droit privé ou public traitant des données personnelles

Activité indifférente (finance, informatique, industrie, santé, etc.)

Taille indifférente (sous réserve de certaines exceptions pour les PME)

Acteurs concernés (2/2)



- Champ d'application territorial:

- Responsables du traitement (RT) / Sous-traitants (ST) établis dans l'UE
- RT/ST établis hors UE

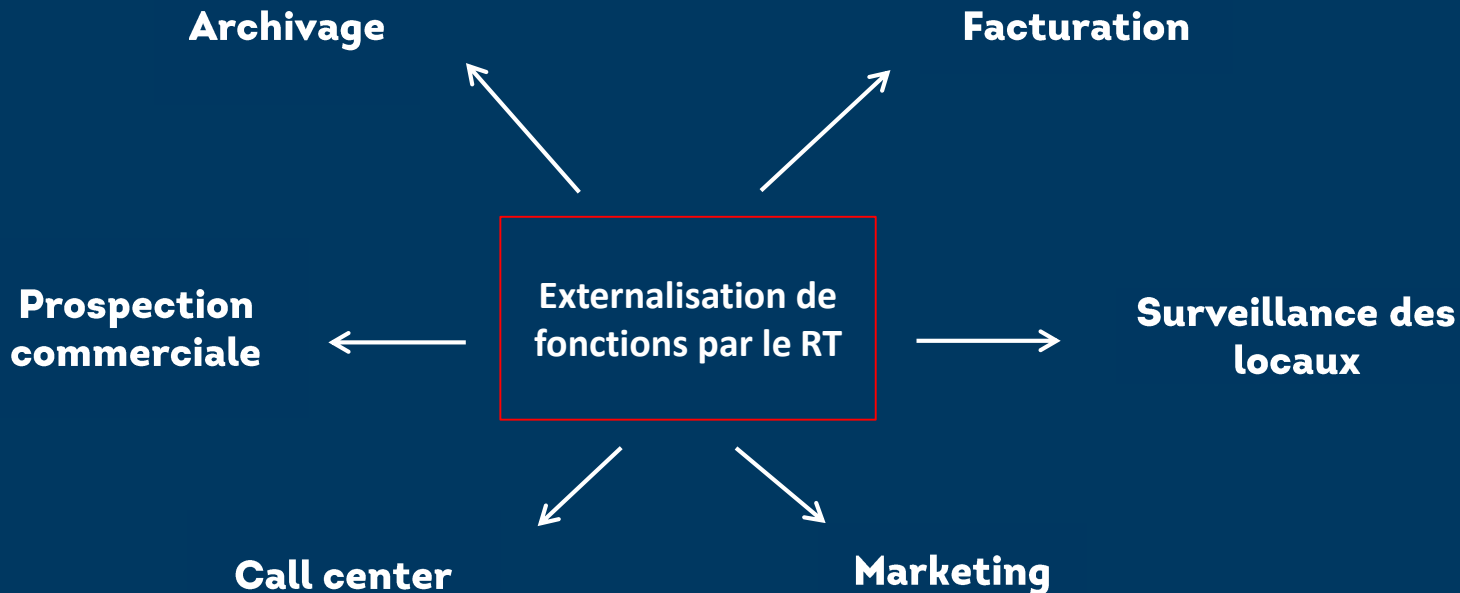
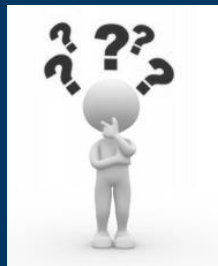
Offre de biens ou de services à des personnes établies dans l'UE (ex. e-commerce)
Suivi du comportement de ces personnes dans l'UE (ex. profilage sur Internet)

Identification des rôles (1/2)

- **Définitions inchangées dans le GDPR (article 4):**
 - Responsable de traitement : La personne qui seule ou conjointement avec d'autres détermine les finalités et les moyens du traitement
- => Consécration du concept de responsables conjoints de traitement (RC) (article 26 GDPR)
- Sous-traitant : La personne qui traite des données pour le compte du RT
- **Rôle primordial de la distinction (allocation de responsabilité)**



Identification des rôles (2/2)



Rôle actuel du sous-traitant (1/2)

- Article 22 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel:
 - Obligation du RT de mettre en œuvre toutes les mesures techniques et l'organisation appropriées pour assurer la protection des données qu'il traite contre la destruction, la perte, l'altération, la diffusion ou l'accès non autorisés
 - Il incombe au ST de veiller au respect de ces mesures

Rôle actuel du sous-traitant (2/2)

- **Choix du ST : garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements à effectuer**
- **Contrat écrit entre le RT et le ST prévoyant au minimum que :**
 - **Le ST n'agit que sur la seule instruction du RT, et que**
 - **Les obligations de sécurité du traitement incombant de par la loi au RT incombent également au ST**

Relation ST/RT (GDPR) (1/4)

- **Importance du choix du ST (article 28 GDPR et considérant 81) :**
 - connaissances spécialisées
 - fiabilité
 - ressources suffisantes
- **Contrat de sous-traitance obligatoire entre RT / ST :**
 - contrat particulier
 - clauses contractuelles types



Relation ST/RT (GDPR) (2/4)

- « Sous-sous traitance » :

- autorisation écrite préalable du RT, spécifique ou générale
- contrat identique entre le ST et le SST

Aucune exonération du ST quant au respect de ses obligations

Relation ST/RT (GDPR) (3/4)

- **Contrat de sous-traitance : contenu renforcé (article 28 GDPR)**
 - Objet, durée, nature, finalité du traitement, type de données traitées, catégories de personnes concernées, obligations et droits du RT
 - Obligation du ST de ne traiter les données que sur instructions documentées du RT!



Relation ST/RT (GDPR) (4/4)

- **Contrat de sous-traitance: contenu renforcé (article 28 GDPR)**
 - Obligation de coopérer avec le RT
 - Sort des données au terme du contrat
 - Obligation de sécurité et de confidentialité du personnel
 - Conditions de la sous-sous traitance



Nouvelles obligations impactant l'organisation interne du ST (1/4)

Désignation obligatoire d'un représentant dans l'UE (article 27 GDPR)

➤ Quand?

ST pas établi dans l'UE

Activités de traitement liées à l'offre de biens ou services à des personnes situées dans l'UE, ou au suivi de leur comportement dans l'UE

➤ Exceptions (2)

Nouvelles obligations impactant l'organisation interne du ST (2/4)

Désignation obligatoire d'un représentant dans l'UE (article 27 GDPR)

➤ Rôle

Personne de contact des autorités de contrôle et des personnes concernées en lieu et place ou en plus du ST

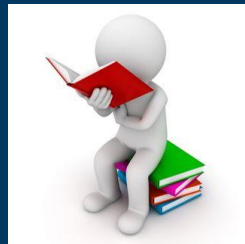
Tenue du registre des activités de traitement

Aucune exonération du ST quant au respect de ses obligations

Nouvelles obligations impactant l'organisation interne du ST (3/4)

Tenue d'un registre des activités de traitement de données effectuées pour le compte du RT (article 30 GDPR)

Exception limitée pour les entreprises de moins de 250 employés,
sauf exceptions légales



Nouvelles obligations impactant l'organisation interne du ST (4/4)

Désignation d'un délégué à la protection des données (article 37 GDPR)

- Désignation obligatoire dans certains cas listés par le GDPR
 - Rôle :
 - Veille à la conformité au GDPR, conseille le ST en ce sens
 - Point de contact pour l'autorité de contrôle / la personne concernée
- Aucune exonération du ST quant au respect de ses obligations**



Nouvelles obligations de coopération (1/3)

- **Obligation directe de coopération avec l'autorité de contrôle (article 31 GDPR)**
- **Obligation d'assister le RT :**
 - **Assiste le RT pour les analyses d'impact (article 38 GDPR)**
 - **Notifie le RT des violations de données dans les meilleurs délais (article 33 GDPR)**

Pas d'obligation légale de notifier les personnes concernées et autorités de contrôle compétente(s)



Nouvelles obligations de coopération (2/3)

Obligation généralisée de notification (articles 33 et 34 du GDPR)

- A l'autorité de contrôle (RT) :
 - Exception : pas de risque pour les droits de la personne concernée
 - Notification dans les meilleurs délais et si possible dans les 72h



Nouvelles obligations de coopération (3/3)

Obligation généralisée de notification (articles 33 et 34 du GDPR)

- **Aux personnes concernées (RT) :**
 - Si risque élevé pour les droits et libertés individuelles ou que l'autorité de contrôle l'exige, sauf exceptions (ex : données chiffrées)
 - Notification dans les meilleurs délais
- **Le RT supporte le coût de la notification**

Une responsabilité accrue du ST (1/2)

- **Recours juridictionnel direct contre le ST (article 79 GDPR)**
- **Droit à réparation (article 82 GDPR) :**
 - **Responsabilité du RT du fait de « *sa participation au traitement* » pour la totalité du dommage causé par le traitement**



Une responsabilité accrue du ST (2/2)

➤ Responsabilité du ST dans 2 cas :

Non-respect de ses propres obligations découlant du GDPR

Agissement en dehors des instructions (licites) du RT ou contrairement à celles-ci

MAIS

Responsabilité solidaire organisée par le GDPR entre le RT et ST



Des sanctions renforcées sous le GDPR (1/2)

- Nouveau pouvoir de sanctions financières pour les autorités de contrôle :
 - 4% C.A. mondial ou 20 MIO € pour certaines violations :
 - ☐ Principes de base
 - ☐ Droits des personnes concernées
 - ☐ Transferts pays tiers
 - 2% C.A. mondial ou 10 MIO € pour autres violations



Des sanctions renforcées sous le GDPR (2/2)

- **Maintien des sanctions administratives** existantes (ex. interdiction du traitement, ordre d'effacement des données, etc.)
- **Sanction propre au ST** (article 28 GDPR): **requalification en RT** lorsqu'il détermine les finalités et les moyens du traitement.

Conclusion

- Le ST se limite, sous l'empire des textes actuels, à participer à la sécurité des données traitées
- Le nouveau système s'oriente vers une **approche plus globale de la conformité**, où chaque acteur est responsabilisé
- Au vu des sanctions financières très importantes posées par le GDPR, il est important d'anticiper son entrée en vigueur et de **revoir sans plus tarder les contrats de sous-traitance en cours ainsi que les mesures organisationnelles et techniques en place dans l'entreprise**

Merci pour votre attention!

Questions?

Héloïse Bock

Avocat à la Cour

Conseiller d'Etat

+352 40 78 78 321

heloise.bock@arendt.com

La protection des données dans un contexte transfrontalier

***Me Catherine Di Lorenzo, Counsel
Allen and Overy***

Focus sur les transferts de données personnelles vers un prestataire situé hors de l'Union européenne

Transferts de données personnelles (1/3)

- ❖ Le transfert de données personnelles (« Données ») qui font ou sont destinées à faire l'objet d'un traitement après ce transfert sont possibles dans certaines conditions.
- ❖ Le transfert ne recouvre pas seulement le transfert physique mais également le fait de données accès à distance à des Données.

Transferts de données personnelles (2/3)

- ❖ L'accès à des Données depuis un pays tiers à celui dans lequel les Données sont stockées est un transfert de Données.

Ex: lorsque vous appelez un call center situé au Maroc, afin de régler un problème d'accès à une application, les salariés du call center vont avoir accès à distance à vos Données Personnelles qui sont situées sur votre ordinateur: cela constitue un transfert de Données.

- ❖ Le transfert de Données personnelle au sein de l'UE est libre.

Transferts de données personnelles (3/3)

- ❖ Le transfert de Données personnelles hors de l'UE est strictement encadré → nécessité de démontrer que les Données transférées bénéficieront du même niveau de protection dans le pays hors UE vers lequel elles sont envoyées que si elles étaient restées uniquement au sein de l'UE.
- ❖ Les pays offrant un niveau de protection adéquat sont les suivants :
 - ❖ Les pays de l'EEE (membres UE + Islande, Norvège, Liechtenstein)
 - ❖ Autres pays offrant un niveau de protection adéquat : Andorre, Argentine, Canada (organisations commerciales), Iles Feroé, Guernsey, Israel, Ile de Man, Jersey, Nouvelle-Zélande, Suisse, Uruguay, sociétés US sous le « Privacy Shield »

Comment encadrer les transferts de données personnelles hors de l'UE? (1/4)

- ❖ Il existe plusieurs moyens permettant d'effectuer un transfert de Données hors UE en toute légalité:
 - ❖ Transfert vers un pays reconnu comme étant adéquat
OU
 - ❖ Privacy Shield (pour certains destinataires aux États-Unis d'Amérique)
OU
 - ❖ Clauses contractuelles types
OU
 - ❖ Code de conduite approuvé + engagement d'appliquer les garanties appropriées

Comment encadrer les transferts de données personnelles hors de l'UE? (2/4)

OU

- ❖ **Certification** approuvé + engagement d'appliquer les garanties appropriées

OU

- ❖ **Binding Corporate Rules (BCR)** : Politique Groupe approuvée par les 28 autorités européennes de protection des données - les transferts entre les entités d'un groupe ayant adopté des BCR sont libres
 - ❖ Groupe d'entreprises : une entreprise qui exerce le contrôle et les entreprises qu'elle contrôle
 - ❖ Etablissement principal : lieu de l'administration centrale dans l'UE ou de l'établissement ayant pris les décisions quant aux finalités et aux moyens du traitement de données à caractère personnel

Comment encadrer les transferts de données personnelles hors de l'UE? (3/4)

❖ Autres exceptions pour les transferts hors UE

- ❖ Consentement explicite de la personne concernée.
- ❖ Le transfert est nécessaire à l'exécution d'un contrat ou à la mise en œuvre de mesures précontractuelles.
- ❖ Le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu dans l'intérêt de la personne concernée.
- ❖ Le transfert est nécessaire pour des motifs importants d'intérêt public.
- ❖ Le transfert est nécessaire à la constatation, à l'exercice ou à la défense de droits en justice.

Comment encadrer les transferts de données personnelles hors de l'UE? (4/4)

- ❖ Le transfert est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'autres personnes, et la personne concernée se trouve dans l'incapacité de donner son consentement.
- ❖ Le transfert a lieu au départ d'un registre qui, conformément au droit de l'Union ou au droit d'un État membre, est destiné à fournir des informations au public.
- ❖ Le transfert ne revêt pas de caractère répétitif, ne touche qu'un nombre limité de personnes concernées, est nécessaire aux fins des intérêts légitimes impérieux du responsable du traitement sur lesquels ne prévalent pas les intérêts ou les droits et libertés de la personne concernée (+ garanties appropriées, information de l'autorité de contrôle du transfert et de la personne concernée).

Le consentement : la solution facile? (1/2)

- ❖ Doit être donné de façon libre, spécifique, éclairée (expression univoque de l'accord de la personne concernée soit par une déclaration écrite soit par un acte positif clair)
 - ❖ Consentement doit être clair, par ex. déclaration écrite (électronique : cases à cocher, paramètres techniques) ou orale ou comportement univoque compte tenu du contexte
 - ❖ Pas de consentement en cas de silence, de cases cochées par défaut ou d'inactivité
 - ❖ Droit pour la personne concernée de retirer facilement le consentement à tout moment (aussi facilement qu'il a été donné)
- ❖ Charge de la preuve revient au responsable du traitement

Le consentement : la solution facile? (2/2)

- ❖ Lorsque le traitement a plusieurs finalités, demande de consentement présentée pour chaque question sous une forme qui la distingue clairement des autres questions
- ❖ N'est pas valable si déséquilibre significatif entre la position de la personne concernée et celle du responsable du traitement

Concrètement :

Dans la majorité des cas, le consentement n'est pas la bonne option.

Solution privilégiée: les clauses contractuelles types

- ❖ Le sous-traitant agit pour le compte de ses clients responsables de traitement: il convient donc d'utiliser les Clauses contractuelles types adoptées par une décision de la Commission européenne adoptée en février 2010.
- ❖ Ces clauses visent à s'assurer que l'importateur de données garantissent le même niveau de protection aux données que si celles-ci étaient restées au Luxembourg.
- ❖ Qui doit les signer?
 - ❖ L'Exportateur est défini comme le responsable de traitement qui transfère les données à l'importateur de données
 - ❖ L'Importateur de données est défini comme le sous-traitant établi dans un pays tiers qui accepte de recevoir de l'exportateur de données des données à caractère personnel

Concrètement :

le contrat doit être signé entre le client et le sous-traitant situé hors UE.

Encadrement juridique du transfert de données



- Les transferts au sein de l'UE sont libres.
- Seul le contrat de prestation de service est nécessaire.

Encadrement juridique du transfert de données



- Les transferts hors de l'Union européenne mais vers des pays assurant un niveau de protection adéquat sont libres.
- Seul le contrat de prestation de service est nécessaire.

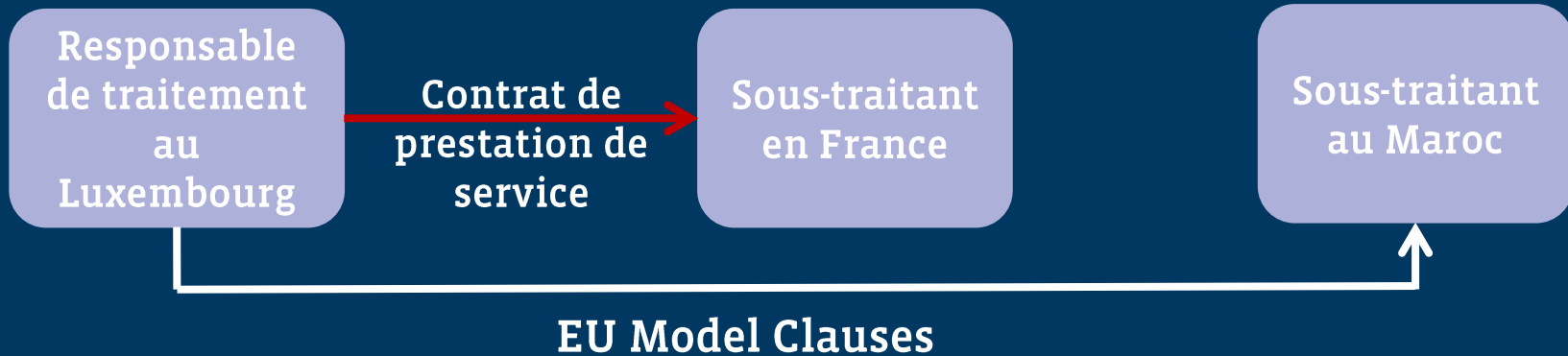
Encadrement juridique du transfert de données



- Les transferts hors de l'Union européenne vers un pays n'assurant pas un niveau de protection adéquat doivent être encadrés.
- Il convient de signer les clauses contractuelles types en plus du contrat de prestation de service.

Encadrement juridique du transfert de données

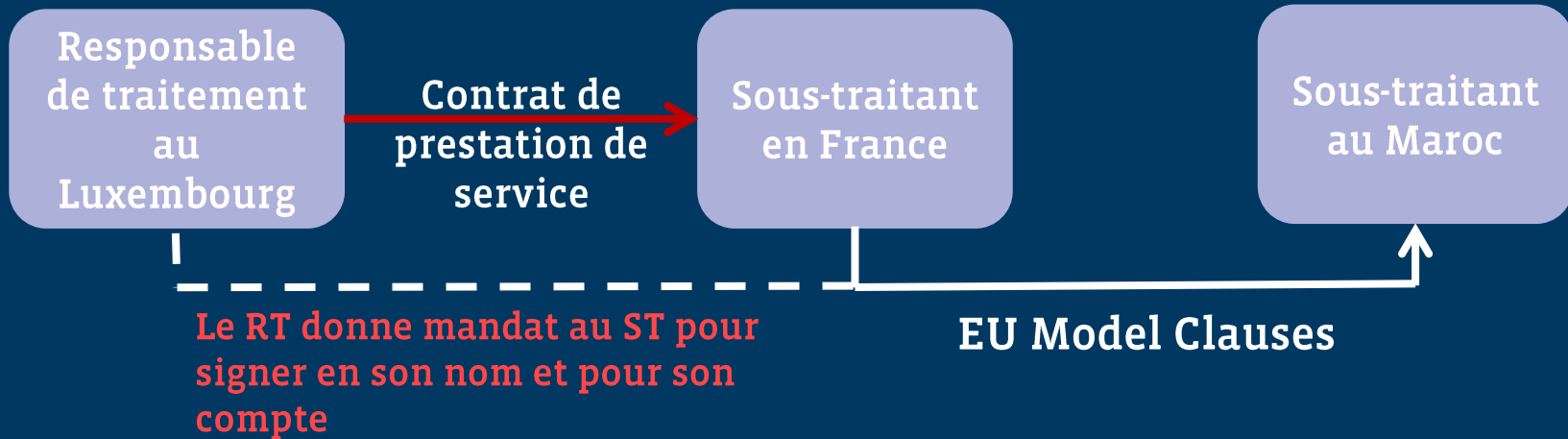
Option 1



➔ Les transferts hors de l'Union européenne vers un pays n'assurant pas un niveau de protection adéquat doivent être encadrés par le responsable de traitement or, en l'espèce c'est le sous-traitant qui transfère les données hors de l'Union européenne.

Encadrement juridique du transfert de données

Option 2



→ Les transferts hors de l'Union européenne vers un pays n'assurant pas un niveau de protection adéquat doivent être encadrés par le responsable de traitement or, en l'espèce c'est le sous-traitant qui transfère les données hors de l'Union européenne.

Les sanctions

- ❖ Le non-respect des dispositions liées au transfert considéré comme violation majeure.
- ❖ Sanction la plus lourde : amendes administratives jusqu'à 4% du chiffre d'affaires annuel mondial total.



Questions?

These are presentation slides only. The information within these slides does not constitute definitive advice and should not be used as the basis for giving definitive advice without checking the primary sources.

Allen & Overy means Allen & Overy LLP and/or its affiliated undertakings. The term partner is used to refer to a member of Allen & Overy LLP or an employee or consultant with equivalent standing and qualifications or an individual with equivalent status in one of Allen & Overy LLP's affiliated undertakings.

FEDIL

07

Intervention

Mme Tine Larsen, Présidente

CNPD

Questions/Réponses

Mme Magalie Lysiak, Adviser, FEDIL

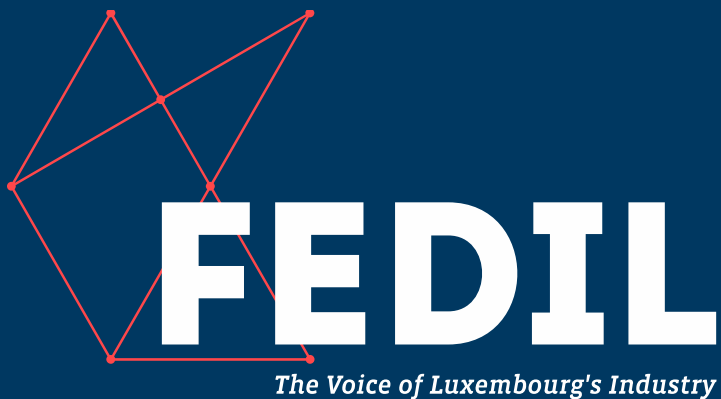
Me Anthony Favier, Associate, DSM Legal

Me Vincent Wellens, Partner NautaDutilh Avocats

Me Héloïse Bock, Partner Arendt & Medernach

Me Catherine Di Lorenzo, Counsel Allen and Overy

Mme Tine Larsen, Présidente, CNPD



**MERCI POUR
VOTRE
ATTENTION!**

*7, rue Alcide de Gasperi
Luxembourg-Kirchberg
Boîte postale 1304
L-1013 Luxembourg*

*fedil@fedil.lu
tel: +352 43 53 66-1
fax: +352 43 23 28
www.fedil.lu*