Règlement UE 2016/679 du 26 avril 2016

Règlement général sur la protection des données (RGPD)

Organisation et procédures internes à mettre en œuvre par les entreprises - Conseils pratiques

dcl avocats / Luxembourg

INTRODUCTION

Cadre Légal

A compter du 25 mai 2018

- **Application directe** dans tous les Etats européens du **Règlement protection des données**, Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016, plus connu sous les abréviations « **RGPD** » en français et « **GDPR** » en anglais

- **Abrogation** du cadre légal actuel constitué par la **loi modifiée du 2 août 2002** relative à la protection des personnes à l'égard du traitement des données à caractère personnel - Quid des autorisations actuelles ?

- **Au niveau national**, complément du cadre européen fixé par le RGPD par le **projet de loi n° 7184** prévoyant notamment les nouveaux pouvoirs de la **Commission Nationale pour la Protection des Données (la « CNPD »)**

INTRODUCTION

Se mettre en conformité pour le 25 mai 2018

Première étape: répertorier les traitements et gérer les risques

- Nommer le DPO ou personne en charge du projet RGPD
- Répertorier les traitements
- Gérer les risques et le cas échéant établir une/des analyse(s) d'impact
- Compléter le/les registres des traitements

Seconde étape: créer une organisation de la conformité notamment à l'aide de procédures internes

INTRODUCTION

Créer une organisation de la conformité respectant le RGPD

- **Principe de responsabilité** le responsable de traitement et le sous-traitant doivent être en mesure de démontrer à tout moment le respect des principes du RGPD

- **Principe de transparence** le traitement des données personnelles doit être effectué en toute transparence par rapport à la personne concernée ; cette dernière bénéficie d'informations quant au traitement et aux droits d'accès, rectification, limitation, effacement et portabilité concernant ses données personnelles

PLAN

Organisation et procédures internes à mettre en œuvre dans l'entreprise

I. Organisation de la gestion des données personnelles au sein de l'entreprise : sensibiliser le personnel, organiser les procédures RH, maintenir ses registres à jours, gérer les relations avec les sous-traitants, gérer les violations de données

II. Organisation de la gestion des droits des personnes concernées au sein de l'entreprise : gérer l'information des personnes concernées, leur consentement le cas échéant et leurs droits (d'accès, rectification, limitation opposition, effacement, portabilité)

III. Gestion d'un contrôle de la CNPD dans l'entreprise : identifier le cadre légal du contrôle et comment faire face au contrôle

Sensibilisation du personnel

- Désigner un **délégué à la protection des données** (« **DPO** » en anglais) **ou une personne de contact RGPD** au sein de l'entreprise et informer le personnel de l'identité du DPO

- Organiser des **formations régulières** relatives à la protection des données à destination du personnel (département RH)

- **Verrouiller les traitements de données** effectués par les membres du personnel et **assurer la sécurité** des données traitées par le personnel dans le cadre de leurs fonctions

  - exemple de la **charte informatique**

A inclure dans la charte informatique

- **Présenter le DPO / la personne de contact RGPD et sa mission**
- **Encadrer l'utilisation du système informatique de l'entreprise (sur tous appareils) - Encadrer l'utilisation de la boite email professionnelle :** limitation de l'usage privé, cantonnement à un dossier personnel non-partagé, effacement lors du départ de l'employé
- **Restreindre** les enregistrements sur tout appareil informatique et numérique
- **Imposer des règles de sécurité** interdiction des modifications des appareils numériques, interdiction des téléchargements
- **Informer le personnel** concernant les données auxquelles le personnel IT peut accéder dans le cadre de travail d'administration du système
- **Opposabilité de la charte**

I. ORGANISATION DE LA GESTION DES DONNEES PERSONNELLES AU SEIN DE L'ENTREPRISE

Organiser les procédures relatives aux ressources humaines

❑ La procédure de recrutement

- **Base légale du traitement:** consentement / intérêt légitime de l'entreprise
- **Identifier et restreindre** les sources de candidatures
- **Adapter** la procédure en fonction de ces sources
- **Identifier et restreindre** les données collectées auprès des candidats et leur durée de conservation

➢ Exemples pratiques

I. ORGANISATION DE LA GESTION DES DONNEES PERSONNELLES AU SEIN DE L'ENTREPRISE

Exemple de procédures en matière de recrutement

Organiser les procédures relatives aux ressources humaines

❑ Pour les employés existants

- **Base légale du traitement :** exécution du contrat de travail / intérêt légitime de l'entreprise
- **Signature d'un avenant au contrat de travail** incluant les informations à fournir à la personne concernée
- **Signature d'une charte informatique** le cas échéant
- **Information de la délégation du personnel**

Organiser les procédures relatives aux ressources humaines

❑ Organiser le traitement des données lors du départ d'un employé

- **Base légale du traitement :** privilégier l'intérêt légitime de l'entreprise
- **Organiser la copie** sous supervision et moyennant autorisation préalable de l'entreprise des **données stockées à titre personnel et mails personnels stockés** par l'employé dans des dossiers dédiés sur le système de l'entreprise
- Demander à l'employé **d'effacer** ses **données stockées à titre personnel et ses emails personnels** lors de son départ
- Organiser la **restitution des appareils mobiles (téléphone, ordinateur, etc.)** accompagnés des codes d'accès
- Organiser la **signature d'une privacy policy**

Maintenir ses registres à jour

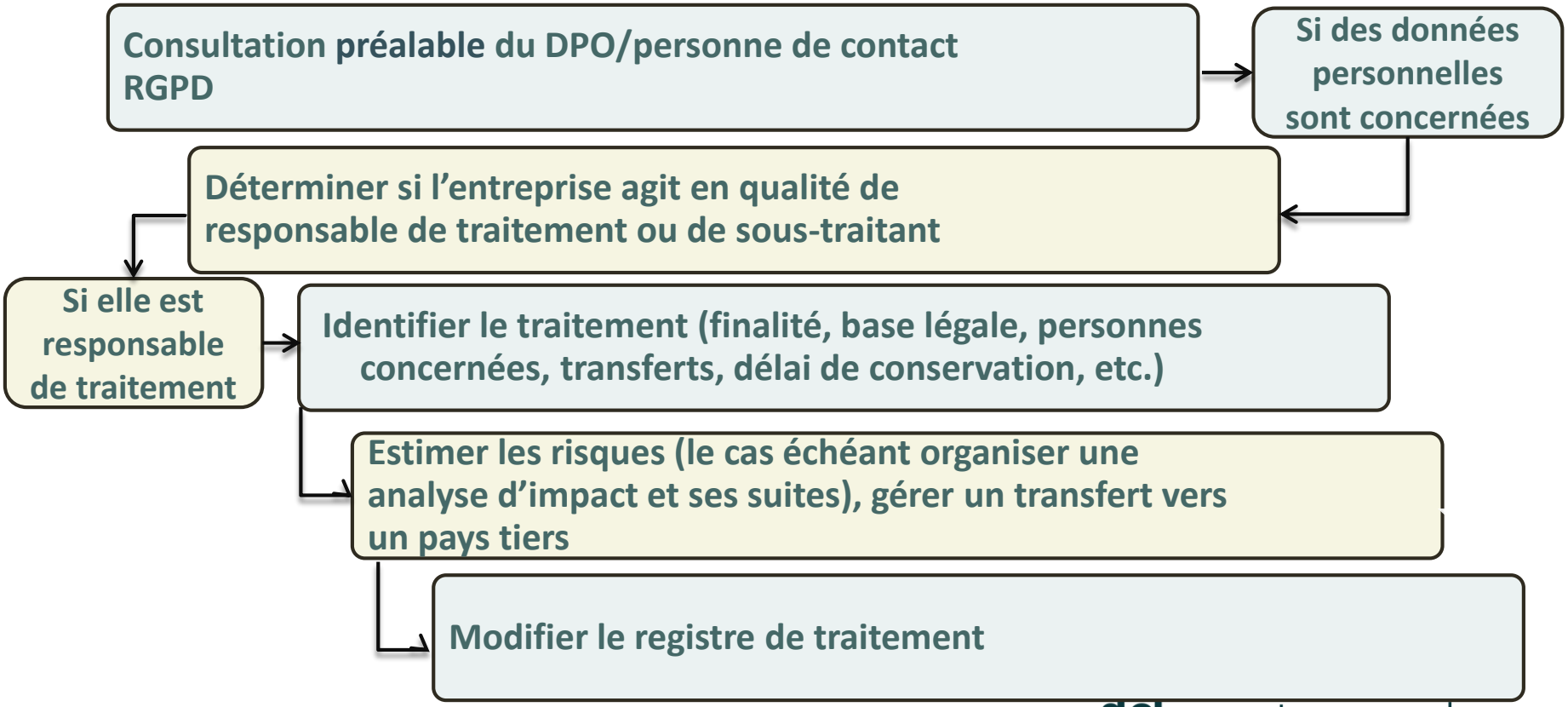
- ❑ L'entreprise doit tenir un **registre des traitements qu'elle effectue en qualité de responsable de traitement** (art. 30 § 1. RGPD) **et un registre des traitements qu'elle effectue en qualité de sous-traitant** (art. 30 § 2. RGPD)

- ❑ Il est également conseillé de tenir à jour **une liste de ses sous-traitants**

- ✓ **Prévoir une procédure applicable à tout nouveau traitement ou toute modification d'un traitement existant**

I. ORGANISATION DE LA GESTION DES DONNEES PERSONNELLES AU SEIN DE L'ENTREPRISE

Exemple d'un nouveau traitement pour lequel l'entreprise agit comme responsable de traitement



Gérer les relations avec les sous-traitants

- Vérifier les **conditions de sécurité** (techniques et organisationnelles), **sous-traitance en cascade, transfert vers un pays tiers,** etc. Procédure relative à la sélection des sous-traitants

- Tenir un **registre des sous-traitants** contenant les coordonnées des DPO/personnes de contact et les références aux contrats de sous-traitance

- Insérer au minimum les **clauses types** dans les contrats de sous-traitance (art. 28 RGPD – liste sites régulateurs européens) – exemple de contrat de sous-traitance publié par l'ICO (UK), accessible depuis le site de la CNPD

Gérer les violations de données

- **Notification** de la CNPD dans les **72 heures**, en cas de **violation de données susceptibles d'engendrer des risques** pour les droits et libertés des personnes
- **Contenu de la notification** prévu à l'article 33 RGPD

a. Nature de la violation, catégorie et nombre de personnes concernées et nombre d'enregistrement concernés
b. Nom et coordonnées du DPO ou personne de contact auprès de laquelle des informations supplémentaires peuvent être obtenues
c. Description des conséquences probables de la violation
d. Description des mesures prises par le responsable de traitement

- **Modèle de courrier de communication à la personne concernée**

March 26, 2018

10632
DOROTHEE CIOLINO
9 VANUE JP PESCATORE
LUXEMBOURG 2324 LUXEMBOURG

Subject: Notice of Data Breach

Dear Dorothee Ciolino,

I am writing to inform you of a data security incident that may have affected your payment card information. At I we take the privacy and security of your information very seriously and regret any concern that this incident may cause you. That is why we are contacting you and informing you about steps that can be taken to protect your information.

What Happened? On February 25, 2018 ca learned of a potential data security incident involving the unauthorized installation of malware on our e-commerce web platform. As soon as we discovered the incident, we took immediate steps to secure this information and contacted the appropriate law enforcement agencies. We also launched an investigation and retained a leading forensics firm to determine what happened and whether customer payment card information had been accessed or acquired without authorization. This letter serves to inform you of the incident and to share with you steps that you can take to protect your information.

What Information Was Involved? We believe that the malware could have comprised payment card information belonging to customers who utilized our web platform to purchase products from February 22, 2017 to March 5, 2018. The affected payment card information may have included names, card numbers, expiration dates, and security codes.

What Are We Doing? As soon as M ca discovered the incident, we took the steps described above. We also reported the incident to the Federal Bureau of Investigation ("FBI") and we are working with both the FBI and the United States Secret Service to hold the perpetrators accountable. In addition, we reported the matter to the payment card brands in order to protect your payment card information and prevent fraudulent activity. We are also providing you with information about steps that you can take to protect your personal information. Finally, we take the security of all information in our systems very seriously and have taken steps to enhance the security of I customer information and our e-commerce web platform in order to prevent similar incidents from occurring in the future.

What You Can Do: You can follow the recommendations on the following page to protect your personal information. We recommend that you review your current and past credit and debit card account statements for discrepancies or unusual activity. If you see anything that you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, you should call the bank that issued the credit or debit card immediately.

For More Information: Further information about how to protect your personal information appears on the following page. If you have questions please call 1-800-338-3679, Monday through Saturday, 8 a.m. – 8 p.m. CT, excluding major holidays.

Thank you for your loyalty to M a and your patience through this incident. We take your trust in us and this matter very seriously. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Chief Financial Officer

Gérer les violations de données

- **Registre des violations** à compléter par l'entreprise (art. 33 § 5 RGPD) comprenant les faits concernant la violation, ses effets et les mesures prises pour y remédier

- La procédure de gestion des violations de données devra naturellement prévoir la mise à jour de ce registre en cas de nouvelle violation

Exemple de registre des violations

(art. 33 §5 GDPR Date of the last entry of the record of data breach:

Processor								
Name	Corporate form	Business	RCS number	Address	Data Protection Officer	Since	Deputy	Since

XX - Record of data breach								
Date of the data breach /identified period of the data breach	Kind of		Description of the personal data breach	Consequence of the breach (2)	Technical or organizational measures taken/or to take to remedy to the breach (1)	Notification to the CNPD (as the case may be)		Date of information to the data subject (as the case may be) (4)
	Data Subject	Personal data				Date of the notification to the CNPD (as the case may be) (3)	Answer from the CNPD (if any) (5)	

(1) to be fulfiled based on the information provided by the IT Department or the relevant department
(2) state the number or at least the possible number of persons affected by the breach and describe the potential consequences
(3) as from 25 May check the CNPD website in order to verify whether a notification form is available online. Keep a pdf copy of the filled form.
(4) keep a pdf copy of the notification message to the data subject
(5) keep the questions and answers provided by all parties

Gestion de l'information des personnes concernées

La liste des **informations à fournir à la personne concernée** figure aux articles 13 et 14 du RGPD

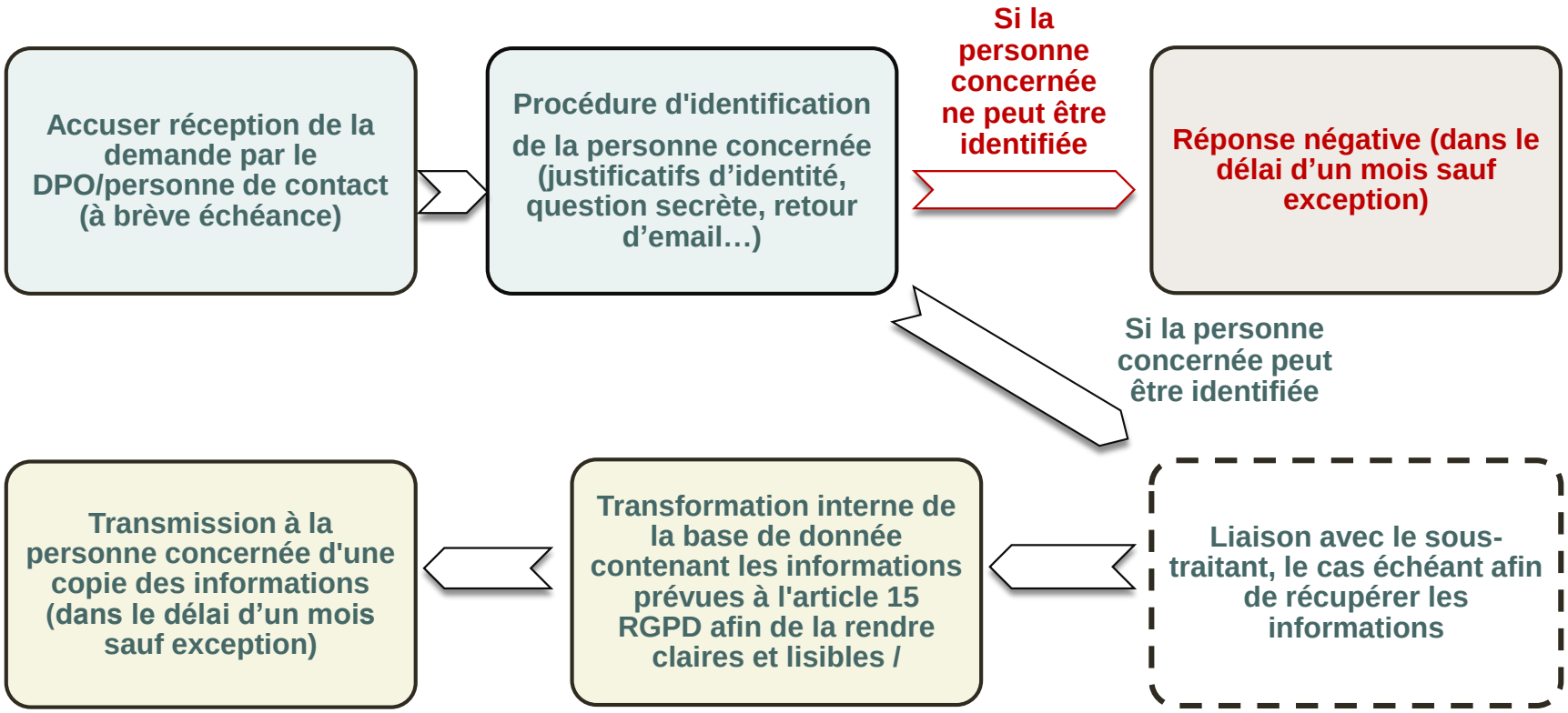
Délai de communication: au moment où les données sont collectées (pour les données collectées auprès des personnes concernées)

Forme de la communication: libre

- Clauses dans les contrats clients – acceptation spéciale
- Privacy policy à signer
- Disclaimer au bas des emails lors d'un premier contact

II. ORGANISATION DE LA GESTION DES DROITS DES PERSONNES CONCERNEES AU SEIN DE L'ENTREPRISE

Droit d'accès de la personne concernée (art. 15 RGPD)



Gestion des droits des personnes concernées

❑ **Droit de rectification (art. 16 RGPD) droit de limitation (art. 18) :**
cf. procédure demande d'accès

❑ **Droit à l'effacement (art. 17 RGPD)**

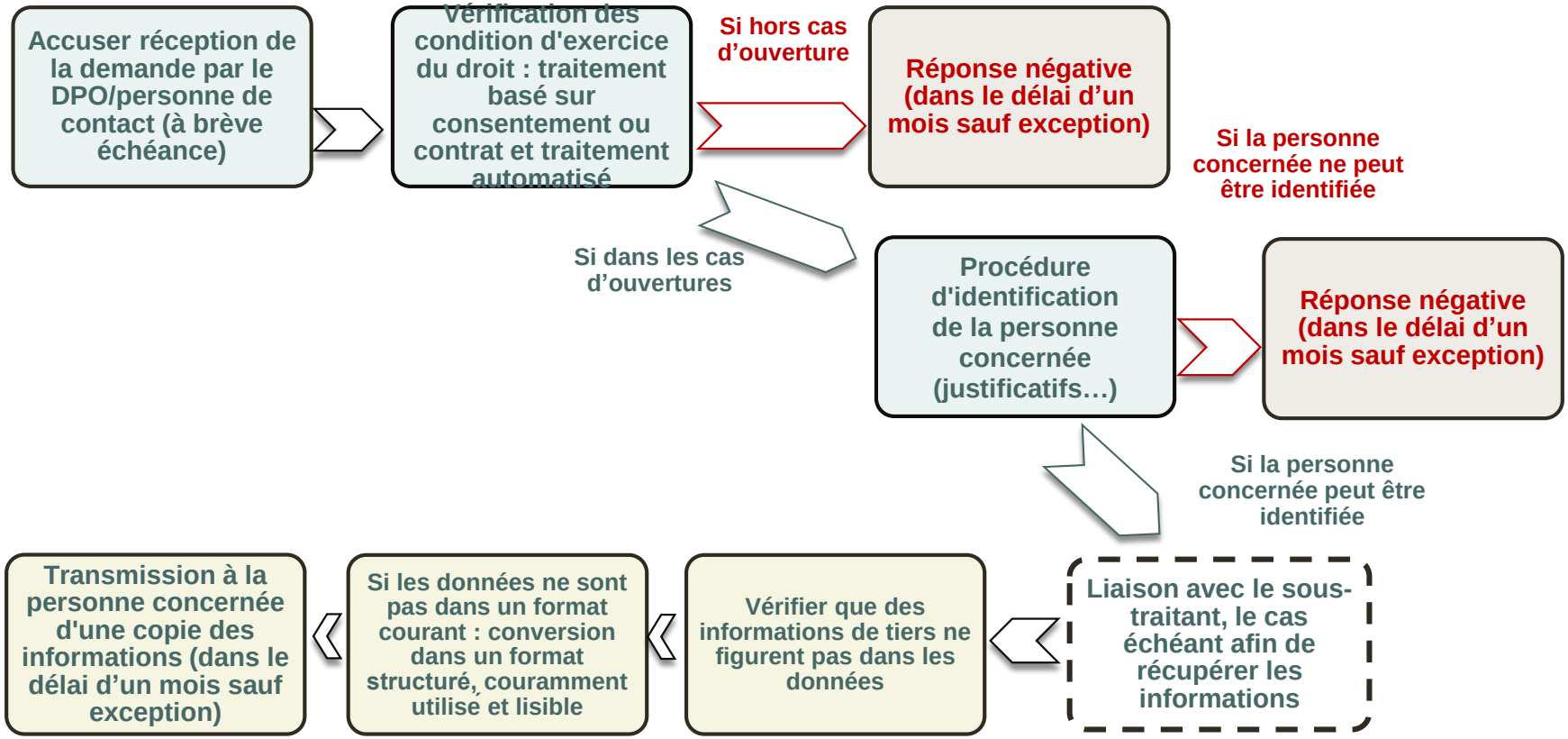
- Existe uniquement pour des **motifs limités**
- Prévoir les moyens de **vérifier l'existence du motif invoqué** par la personne concernée

  Exemple: retrait du consentement de l'ex employé de l'entreprise – chercher autre fondement juridique au traitement (intérêt de limiter l'utilisation du consentement)

- Prévoir la procédure de notification des destinataires des données prévue à l'article 19 RGPD

II. ORGANISATION DE LA GESTION DES DROITS DES PERSONNES CONCERNEES AU SEIN DE L'ENTREPRISE

Droit à la portabilité des données (art. 20 RGPD)



Identifier le cadre légal du contrôle

La CNPD dispose d'un **pouvoir de contrôle** du respect des règles prévues par le RGPD (art. 57 RGPD) s'exerçant notamment par:

- Contrôle sur place
- Enquête sur dossier
- Audit approfondi

III. GESTION D'UN CONTRÔLE DE LA CNPD DANS L'ENTREPRISE

FAIRE FACE AU CONTRÔLE : GUIDE DU CONTROLÉ

- **Informer et former le personnel** concernant la possibilité d'un contrôle par la CNPD
- **Canaliser le flux d'informations :** présenter (physiquement) le DPO ou personne de contact s'il n'y a pas de DPO et vérifier l'identité des agents de la CNPD (contrôle sur place ou enquête sur dossier)
- Disposer d'une **procédure interne** en cas de contrôle inopiné ou annoncé
- Limite aux informations auxquelles la CNPD peut accéder – **secret professionnel**
- Prendre **connaissance et vérifier tous les points du procès-verbal ou rapport** dressé après le contrôle
- Faire part de ses **commentaires**, demander des **éclaircissements** et respecter les **délais** imposés par la CNPD dans ses recommandations
- Si la décision de la CNPD à l'issue du contrôle comporte une **sanction** se conformer à celle-ci ou le cas échéant respecter le **délai de recours** indiqué sur la décision

EN CONCLUSION

Au regard du fonctionnement interne de l'entreprise : 2 piliers

- **Le DPO ou la personne en charge de la protection des données personnelles – centralise toutes les demandes relatives à la gestion des données personnelles et assure le principe de *privacy by design* et d'*accountability***

- **Le registre des traitements – document synthétique mais exhaustif de la gestion de la protection de données**

POUR TOUTE QUESTION

Dorothée CIOLINO
Avocat aux Barreaux de Paris et de Luxembourg
ciolino@dclavocats.com

DCL Avocats S.à r.l.
9, Avenue Jean-Pierre Pescatore
L-2324 Luxembourg
Tél. + 352 26 00 11 1
Fax +352 27 12 51 81
www.dclavocats.com