Règlement général sur la protection des données

Le RGPD : mise en œuvre pratique en matière de ressources humaines

CNPD
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

14 mai 2018

Luxembourg

Christophe Buschmann

Membre effectif

Agenda

Introduction

Classification des données

Le registre des activités de traitement

La sous-traitance

Le consentement

La durée de conservation

I. Introduction générale

Introduction générale

La balance à trouver

protection des personnes physiques à l'égard du traitement des données à caractère personnel

libre circulation de ces données

- Sécurité
- Transparence
- Contrôle
- Règles claires
- One-stop-shop
- Harmonisation

Caractéristiques clés

"Accountability"

- Nécessite une documentation et attribution de responsabilités
- Presque plus de démarches administratives – contrôle à postériori

Basé sur les risques

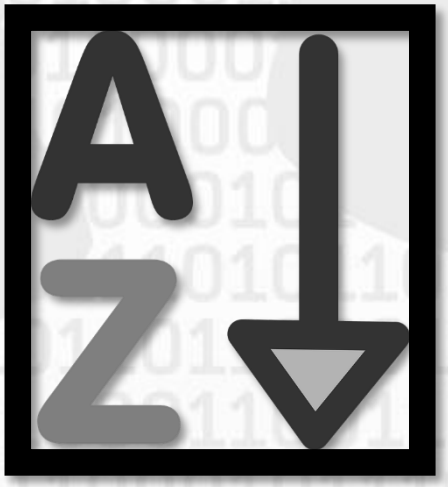
- Exigences incrémentales en fonction du risque (p.ex. Data Breach, Data Privacy Impact Assessments)

Application générale

- Interprétation conjointe avec d'autres règlementations sectorielles le cas échéant
- Application directe

Recommandations

Je suis parfaitement conforme	Je suis dans une démarche mais probablement pas prêt	Je suis concerné mais pas prêt	Je ne suis pas concerné	J'espère ne pas être contrôlé
• Partagez vos expériences • Assurer la continuité et l'évolution • Restez vigilant et sceptiques • Soyez honnêtes sur ce que vous pouvez assurer	• Adoptez une approche basée sur les risques - Evitez d'être bloqué sur des détails au détriment de points plus importants • Ayez courage, soyez transparents – utilisez un langage adapté aux personnes concernées • Faites bon usage de la guidance désormais disponible au niveau EU • Echangez vous avec d'autres • Soyez spécifique pour votre cas – ne restez pas dans l'abstrait juridique • Laissez vous guider par l'esprit du RGPD (transparence, contrôle) et non pas par les sanctions	• Il n'est jamais trop tard pour lancer les démarches – mais vous agissez • Restez positifs et constructifs – la peur ou la renonciation sont des mauvais conseillers • Si vous n'étiez déjà pas conforme avec le régime précèdent – ayez une approche top down – et ne vous concentrez pas sur les subtiles changements – faites un inventaire complet haut niveau que vous déclinez au fur et à mesure	• Assurez vous que c'est vraiment le cas – c'est peu probable – au moins les données de vos salaries sont à gérer • Attention – le RGPD ne se limite pas uniquement aux données dites "sensibles". • Peut être les mesures à mettre en place sont très simples – mais cela ne devrait pas vous empêcher de vérifier la situation	• Cette position n'est pas acceptable – les sanctions qui seront prises dans ce cas le reflèteront • Rendez vous compte que vous allez nuire à vos clients, salaries … et vous même. … et toute la place luxembourgeoise. Une entreprise qui veut assurer sa pérennité ne peut pas adopter cette approche. • En plus de contrôles "aléatoires" la CNPD effectuera des contrôles ciblés lorsque des violations potentielles sont portées à sa connaissance. Ces éléments peuvent venir de clients, d'(anciens) salaries ou des tiers



II. Classification des données

Classification des données

Définition

« 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;

Concernant le périmètre:

- Le RGPD s'applique aux données à caractère personnel – sur base d'un définition large. Ceci inclut les données pseudonymisées. Il y a une différence entre pseudonymisée et anonymisé.
- Le RGPD ne se limite pas aux données personnelles dites "sensibles"
- Le RGPD ne s'applique pas aux données anonymisées (données personnelles qui ont été rendues anonynymes) – guidance par rapport aux techniques d'anonymisation existe. Ceci peut être un piste pour résoudre des problématiques concernant le droit à l'oubli / la suppression.

Classification des données

Explications complémentaires

Concernant les mesures de sécurité et notamment la confidentialité

- Les mesures de sécurité s'appliquent à toutes les données à caractère personnel – les mesures devront être proportionnel au risque engagé pour les personnes concernées. Ceci fait le lien avec les données dites « sensibles ».
- L'obligation de confidentialité s'applique à toutes les données à caractère personnel aussi bien pour le responsable de traitement que pour ses potentiels sous-traitants.

Concernant une classification des données:

- Difficulté de classifier une donnée sans tenir compte du contexte / de l'utilisation qui en est faite (ou qui peut en être faite). P.ex. différence entre le nom qui figure sur une liste de distribution marketing d'un club de sport ou sur une liste de patients pour des séances de dialyse.
- Le RGPD prévoit des règles qui s'appliquent à tous le traitement de données à caractère personnel – ainsi que des règles plus strictes plus spécifiques dans certains cas / pour certain types des données. (p.ex. obligation de réaliser une DPIA (art.35),…)
- Certains traitements (faisant recours à des données dites « sensibles ») sont encadrés par des disposition non pas repris dans le RGPD mais plutôt dans les lois nationales (p.ex. données relative aux condamnations pénales et aux infractions (art.10), traitement du numéro d'identification national (art. 87), traitement des données dans le cadre des relations de travail (art.88),…)

Classification des données

Exemple illustratif

Les données qui ne sont pas à caractère personnel ne sont pas dans le périmètre du RGPD

Donnée (Chiffre d'affaire, Catalogue des services, Nombre d'employés, Données anonymisées,…)

Donnée à caractère personnel (Nom, prénom, adresse…)

Catégories particulières:

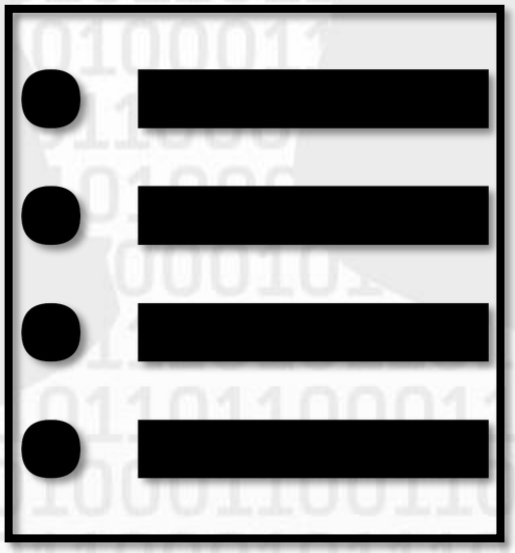
- **Donnée génétique** (Analyse du génome)
- **Donnée biométrique** (Empreinte, signature IRIS, reconnaissance faciale…)
- **Donnée concernant la santé** (Certificat médicaux, visites médicales…)
- **Donnée qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, concernant la vie sexuelle ou l'orientation sexuelle** (Appartenance syndicat, …)

Donnée relative aux condamnations pénales et aux infractions (extrait du casier, …)

Le principe de l'interdiction de traitement s'applique – sauf si une des conditions reprise dans l'article 9 (2) s'applique)

Le traitement me peut être effectué que sous le contrôle de l'autorité publique ou si le traitement est autorisé par le droit de l'Union ou par le droit d'un 'État membre qui prévoit des garanties appropriées pour les droits et libertés des personnes concernées

Les principes générales du RGPD s'appliquent - la licéité du traitement doit être basé sur une des conditions de l'article 6



III. Le registre des activités de traitement et les RH

Le registre des activités de traitement

Définition

RGPD: Registre qui, pour chaque activité de traitement, comporte notamment les informations suivantes:

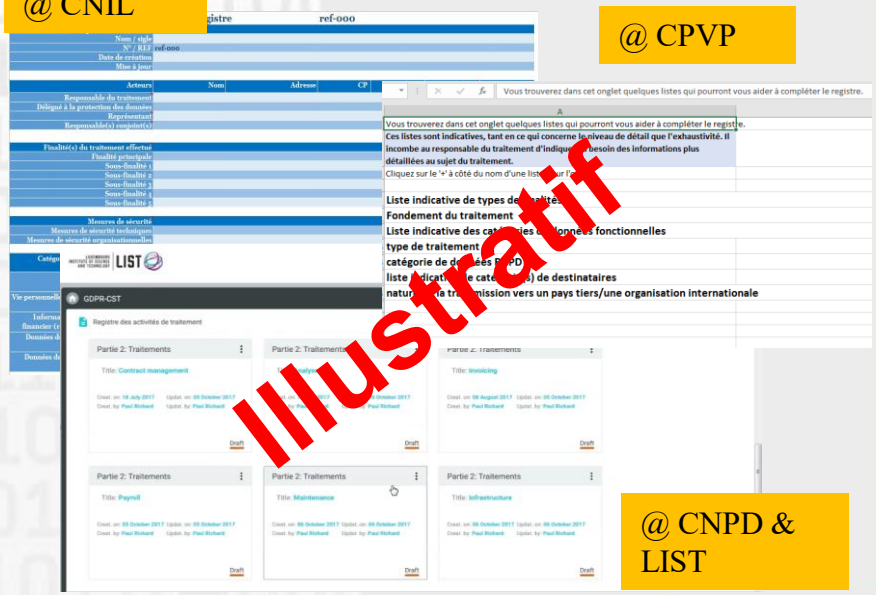
a) le nom et les coordonnées du responsable du traitement (…)
b) les finalités du traitement;
c) une description des catégories de personnes concernées et des catégories de données à caractère personnel;
d) les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées (…)
e) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale(…)
f) dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données;
g) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles (…)

Concernant l'approche

- Rôle du registre dans le "programme" de conformité
- Approche "top-down" vs. approche "bottom-up" (avantages et inconvénients)
- Niveau de granularité
- Documentation (spécifique ou intégrée)
- Importance de la finalité – et de la base de légitimité
- Le regsitre public géré par la CNPD
- Position du WP29 (du 19/04/2018) par rapport à l'obligation ou pas d'avoir un register – et l'impact sur les données RH
- Recommandation n°06/2017 du 14 juin 2017 de la CPVP

@ CNIL

@ CPVP



@ CNPD & LIST

Le registre des activités de traitement

Particularités et exemples dans le domaine des RH

Relation de subordination générale (i.e. consentement)	Balance entre activité professionnelle et vie privée	Contexte en plein changement (digitalisation, travail à domicile,…)

Classification et exemples illustratifs

Traitements administratifs

- Exemples: Contractualisation-recrutement, déclaration entrée sortie, imposition, congés, salaires, maladies,…
- En règle général basé sur des obligation légales (code de travail) ou l'exécution d'un contrat.

Traitements opérationnels

- Exemples: Gestion des horaires / plans de travail, évaluations, travail sur projets (offres),…
- Souvent basé sur obligation légale, exécution d'un contrat OU intérêt légitime

Traitements "nice to have"

- Exemples: Fête de Saint Nicolas, Réseau d'anciens, Convenait, …
- En règle général basé sur le consentement (si possible)

Le registre des activités de traitement

Cadre général pour le recrutement

Finalité

Identifier et embaucher une personne

Base de légitimité

Précontractuel / intérêt légitime

Personnes concernées

Potentiels recrutés

Données traitées

Données d' indentification, qualifications, …

Suppression

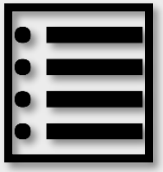
Rejet +x sauf pour le/les candidats retenus (finalités compatibles)

Exemple de risques pour les potentiels recrutés

Perte de confidentialité candidature – employeur actuel – opportunités ratés

Perte de confidentialité de la décision de refus – perte d'opportunité auprès d'autres employeurs

Décision sur données incomplètes/fausses – perte d'opportunité / discrimination



Le recrutement

Quelques points d'attention

- **Bien informer le candidat** – si possible avant qu'il envoie la candidature. Pour les candidature spontanée, prévoir dans la mesure du possible des information sur le site internet
- Informer le candidat sur toutes **les sources d'information que vous utilisez** - aussi sur d'éventuelles recherches basé sur des données dans le domaine public (réseaux sociaux,…) – ne pas faire de recherches à l'insu des personnes. Ne pas exiger l'accès aux comptes media sociaux
- Si vous voulez garder des CV pour une **campagne de recrutement ultérieure** – demander le consentement
- Informer le candidat sur ces droits – il a notamment **le droit d'accès à son dossier** de candidature y inclus les éventuelles notes pris sur lui.
- **Contacter les entreprises pour vérification des expériences** de manière licite (p.ex. en demandant l'autorisation au candidat)
- **Sécuriser l'accès aux dossier de recrutement** en interne – et ne les transmettez pas à une autre société
- Ne pas collecter des **données pas nécessaires – ou illégaux** (discrimination)
- **Pour les chasseurs de tête** – pour chaque transmission d'un dossier qui contient des données personnelles – vérifier la légitimité, et le cas échéant demander l'autorisation.

Le registre des activités de traitement

Cadre général pour la gestion courante des RH

Catégories de finalités		
Gestion administrative (…)	Gestion opérationnelle (…)	Gestion de services « additionnels » (…)

↓

Base de légitimité (usuelles)			
Exécution du contrat	Obligation légale	Intérêt légitime	Consentement (dans certain cas)

↓

Transferts type			
Fiduciaire	Intragroupe	Administrations	Clients ou autres sociétés

↓

Données traitées (usuelles)		
Données d'identification, certificats maladie, données financières…	Qualifications, évaluations,…	Données de contact, autres…

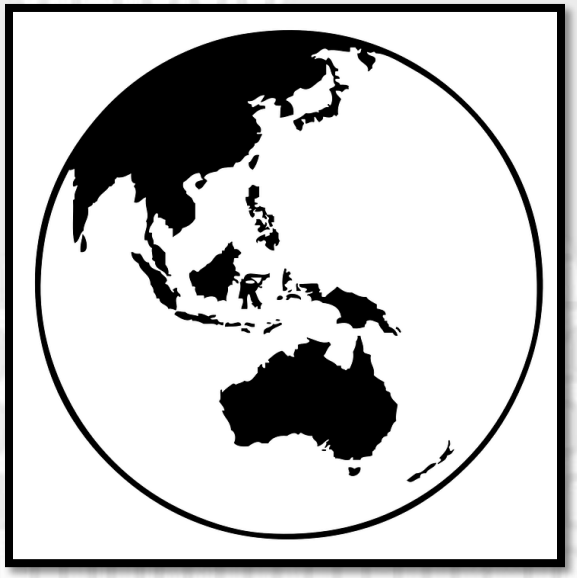
↓

Suppression		
Fin de contrat (+x?)	Durée légale (Code de travail, code de commerce,..)	Autres dispositions (avec consentement)

La gestion courante des RH

Quelques points d'attention

- Attention à la **limitation des finalités** – ne pas utiliser les données collectés pour une finalité pour une autre finalité (incompatible)
- Limiter l'accès aux données pour **éviter tout potentiel détournement de finalité**.
- **Organiser le quotidien au travail** de manière à accorder le droit à la vie privée aux salariés (communication, réunion, ….)
- **Effort supplémentaire concernant la transparence** et le droit à l'information (i.e. vue la multitude des traitements pour lesquels l'employeur sera amené à traiter les données)
- **Mesures supplémentaires pour gérer les données « de santé »** ou autres données « dites sensibles » - gestion des absence pour cause de maladie (application du principe de minimisation),…
- **Sécurisation des données lors de transferts** – notamment en cas d'envoi de grandes quantités (p.ex. fiduciaire)
- Vérifiez si des **exigences spécifiques nationales** s'appliquent (p.ex. surveillance sur le lieux de travail, droit à l'image, casier judiciaire, numéro d'identification national…)
- Vérifiez la présence **d'obligation légales (nationales) sectorielles** – cela facilitera l'identification de bases de légitimité
- Lorsque vous voulez garder les **données de salariés qui ont quittée l'entreprise** ou qui sont partis en retraite – prévoir un base de légitimité appropriée (p.ex. consentement)



IV. La sous-traitance

La sous-traitance

Quelques points d'attention

Les règles générales du GDPR en ce qui concerne la sous-traitance s'appliquent – article 28. Les principales sont:

- Disposer d'un contrat conforme à l'article 28 (3)
- Gérer la potentielle sous-traitance en cascade
- Assurer la transparence envers les salariés (droit d'information)
- Identifier un base de légitimité – dans de nombreux cas c'est l'intérêt légitime – ceci nécessite de documenter la proportionnalité

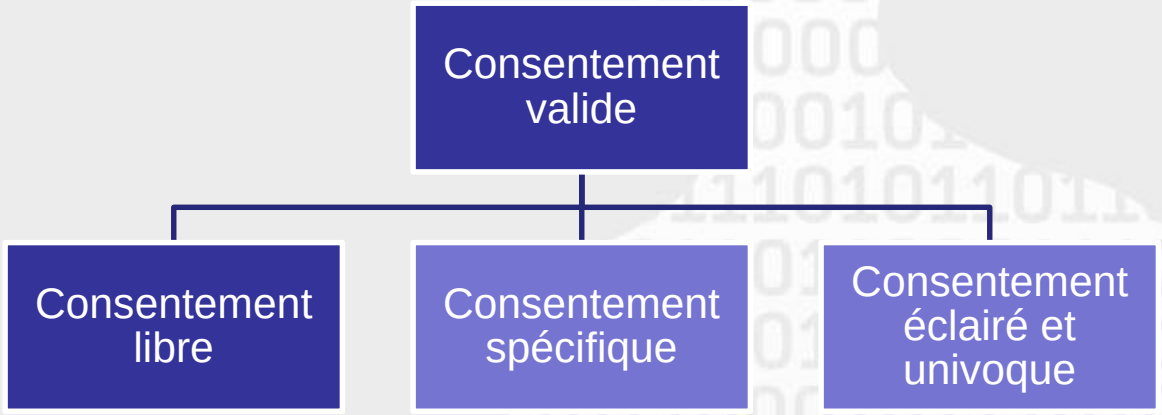
Quelques points d'attention particuliers:

- Assurer la **confidentialité des données tout au long de la chaine** de sous-traitance (et que les personnes ayant accès en sont tenus)
- La **sous-traitance est souvent accompagné de transferts** – ces transferts devront être encadrés notamment lorsqu'elles se font hors UE.
- En cas de **« sous-traitance » intra-groupe** – vérifier s'il s'agit d'une sous-traitance (exécution exclusivement sur base de vos instructions) ou si éventuellement la maison mère devient responsable (conjoint) pour certains traitements qu'elle effectue – et si dans ce cas le transfert est légitime.
- Si vous utilisez des **services dans le nuage** – vérifier la présence d'éventuels transferts hors UE – et si c'est le cas vérifier comment ces transferts sont encadrés (BCR; Privacy Shield, Clauses contractuelles standard,…)

V. Le Consentement

Le Consentement

Particularités dans la gestion RH



Rappel des autres bases de licéité (art.5):
- Exécution d'un contrat
- Obligation légale
- Intérêts vitaux
- Mission d'intérêt public
- Intérêt légitime

Points d'attention concernant le consentement dans la relation employeur – employé:
- **Le caractère « libre »** du consentement est difficile à prouver
- Il est important de choisir la base de légitimité la plus appropriée – non pas celle qui parait la plus simple à satisfaire
- Le consentement dans la relation de travail **n'est pas exclue** comme base de licéité
- **Retrait** - Il doit être aussi simple de retirer que de donner son consentement
- Droit d'obtenir du responsable du traitement **l'effacement (dans les meilleurs délais)** des données la concernant si retrait du consentement et s'il n'existe pas d'autre fondement juridique au traitement.
- **Ne pas demander le consentement si c'est pas la base appropriée**

VI. La durée de conservation

La durée de conservation

La durée de conservation limitée fait partie des principes relatifs au traitement des données à caractère personnel – Article 5 (e):

RGPD: Les données à caractère personnel doivent être conservées sous une forme permettant l'identification des personnes concernées pendant **une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées**….(limitation de la conservation)

Points d'attention:

- La durée de rétention est donc déterminée par rapport à la finalité – et non pas de manière « absolue » exclusivement par rapport à la donnée elle-même.
- Les données anonymisées ne rentrent plus dans le périmètre du RGPD.
- Si la finalité du traitement a été atteinte il y a apriori une obligation de les supprimer – sauf si le responsable de traitement doit les garder (sur base d'une obligation légale par exemple), A ce moment ce « nouveau » traitement justifie le stockage et la durée de rétention est fixé par ce traitement.

La durée de conservation

Exemple illustratif

Données détenues par le responsable de traitement sur une personne X

Gestion de carrière	Organisation Saint Nicolas	Gestion salaire	Gestion Réseau d'anciens
• Evaluation année xxx • Evaluation année yyy • …	• Un fils qui a 5 ans • …	• Heures de travail 2014 • Heures de travail 2015	• Coordonnées de contact
3 ans après la promotion	Le lendemain de la fête	Voir obligation légale	Tant que X ne retire pas son consentement

On constate donc qu'il n y a pas de durée de rétention unique pour les données concernant une personne donnée

Commission nationale pour la protection des données

Merci pour votre attention!