Datagest

LA PROTECTION DES DONNÉES PERSONNELLES UNE OBLIGATION LEGALE

Datagest, une entité de BDO

Datagest en quelques mots

- Entité informatique de BDO à Luxembourg
  - Gestion de l'informatique du groupe
  - Société informatique pour les clients externes
- Nos activités :
  - Éditeur de logiciel :
    - eFiscalease: logiciel de déclaration fiscale
    - PayEase.net: logiciel de calcul de salaire
  - Conseil et assistance informatique
  - Chargé de la protection des données agréé par la CNPD

Datagest

Comment appréhender concrètement l'enjeu de la protection des données personnelles?

1	Notions importantes: définitions, législation et principes fondamentaux
2	Les obligations légales: droits et devoirs des parties prenantes
3	Les évolutions prévisibles: la portée du futur règlement européen
4	Quelques conseils pratiques: des exemples concrets
5	Accompagnement de Datagest pour la protection des données

Datagest

Comment appréhender concrètement l'enjeu de la protection des données personnelles?

1	**Notions importantes: définitions, législation et principes fondamentaux**
2	Les obligations légales: droits et devoirs des parties prenantes
3	Les évolutions prévisibles: la portée du futur règlement européen
4	Quelques conseils pratiques: des exemples concrets
5	Accompagnement de Datagest pour la protection des données

Datagest

Notions importantes

Définitions

- Traitement de données à **caractère personnel** :
  - Toute information **de quelque nature qu'elle soit**
  - Concernant une personne identifiée ou identifiable (uniquement **personne physique**)

- **Fichier** : tout ensemble structuré de données accessible selon des critères déterminés (**fichier informatique ou non**)

- **Responsable du traitement :** celui qui détermine les finalités et les moyens de traitement

Notions importantes

Définitions

- **Sous-traitant :** celui qui traite les données pour le compte d'un responsable
- **Chargé de la protection des données :** désigné par le responsable et agréé par la CNPD
- **CNPD : C**ommission **N**ationale pour la **P**rotection des **D**onnées, autorité nationale de contrôle

Datagest

Notions importantes

Législation en vigueur

- Directive 95/46/CE du Parlement Européen et du Conseil du 24 octobre 1995
- Loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel
- Loi du 30 mai 2005 relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques
- Article L. 261-1 du Code du Travail

Notions importantes

Principes fondamentaux

- La protection de la vie privée constitue un **droit fondamental**
- **Légitimité**: est-ce que la loi autorise le traitement?
- **Finalité**: à déterminer explicitement à l'avance
- **Proportionnalité**: limiter le traitement aux données nécessaires à la finalité
- Durée de **conservation limitée**

Notions importantes

Principes fondamentaux

- **Transparence :** information de la personne concernée des données collectées et de ses droits
- **Sécurité :** assurer l'exactitude et la confidentialité des données
- **Règles spéciales** pour :
  - Catégories particulières de données
  - Surveillance (« normale » et sur le lieu de travail)
  - Transferts des données en-dehors de l'EU

Comment appréhender concrètement l'enjeu de la protection des données personnelles?

1	Notions importantes: définitions, législation et principes fondamentaux
2	**Les obligations légales: droits et devoirs des parties prenantes**
3	Les évolutions prévisibles: la portée du futur règlement européen
4	Quelques conseils pratiques: des exemples concrets
5	Accompagnement de Datagest pour la protection des données

Datagest

Les obligations légales

Droits et devoirs des parties prenantes

- **De la personne concernée :**
  - Être informée des traitements
  - Donner son consentement (explicite pour certains traitements)
  - Accéder à ses données
  - Demander la modification / l'effacement de ses données
  - Droit de s'opposer à un traitement

Les obligations légales

Droits et devoirs des parties prenantes

- **Du responsable de traitement :**

  - Garantir que le traitement est effectué conformément au cadre légal
  - Assurer la sécurité et la confidentialité des données traitées
  - Informer les personnes concernées
  - Veiller aux respect des démarches administratives :
    - Engagement formel de conformité aux autorisations uniques
    - Notification préalable (régime « normal »)
    - Demande d'autorisation préalable pour certains traitements

  → **sanctions administratives, civiles et pénales**

Datagest

Les obligations légales

Droits et devoirs des parties prenantes

- **Du sous-traitant :**

  - Contrat ou acte juridique consigné par écrit
  - Agir sur la seule instruction du responsable du traitement
  - Respecter toutes les obligations de sécurité

  → **éviter d'être requalifié en responsable de traitement**

Les obligations légales

Droits et devoirs des parties prenantes

- **Du chargé de la protection des données** (interne ou externe) **:**
  - **Indépendance** vis-à-vis du responsable
  - Pas de **conflit d'intérêt** avec ses autres missions
  - Obligation de **formation continue**
  - Rôle de **conseiller**
  - Gérer les **formalités requises**
  - Tenir le **registre des traitements** et le transmettre à la CNPD

Comment appréhender concrètement l'enjeu de la protection des données personnelles?

1	Notions importantes: définitions, législation et principes fondamentaux
2	Les obligations légales: droits et devoirs des parties prenantes
3	**Les évolutions prévisibles: la portée du futur règlement européen**
4	Quelques conseils pratiques: des exemples concrets
5	Accompagnement de Datagest pour la protection des données

Datagest

Les évolutions prévisibles: la portée du futur règlement européen

Objectifs

- Harmonisation de la protection des données dans les pays de l'UE
- Renforcement des droits individuels
- Meilleure protection des enfants
- Renforcement du pouvoir des autorités de contrôle (amendes proposées et à valider : jusqu'à 2% du CA mondial ou 1.000.000 €)

Datagest

Les évolutions prévisibles: la portée du futur règlement européen

Nouveaux principes

- One Stop Shop: une autorité de contrôle coordonne les relations avec les responsables et les personnes concernées
- Comité Européen de la Protection des Données
- Applicable dès qu'un résident européen est concerné : peu importe où se trouve le responsable pour certains traitements (vente de produits et de servivces, analyse de comportement)
- "Privacy by Design"

Datagest

Les évolutions prévisibles: la portée du futur règlement européen

Nouveaux principes

- Certification, marques et label en matière de protection des données
- Auto-évaluation des risques pour certains traitements (analyse d'impact)
- Obligation de documenter les traitements
- Obligation de désigner un délégué à la protection des données en fonction de critères à définir (> 250 employés ou activité de surveillance régulière et systématique)
- Obligation de notifier toute violation de données à caractère personnel dans un délai de 24 à 72 heures

Les évolutions prévisibles: la portée du futur règlement européen

Conséquences pratiques

- Simplification de certaines procédures, notamment pour les sociétés multi-nationales
- Personnes concernées mieux informées avec des droits étendus
- Autorités de contrôle avec un véritable pouvoir de sanction
- Responsabilité accrue des responsables du traitement

Les évolutions prévisibles: la portée du futur règlement européen

Conséquences pratiques

- Obligation de prévoir la protection des données dès la conception d'un traitement
- Obligation d'une analyse de risque plus étendue
- Obligation d'une meilleure documentation interne
- Obligation de "s'auto-dénoncer" en cas de violation des données

Comment appréhender concrètement l'enjeu de la protection des données personnelles?

1	Notions importantes: définitions, législation et principes fondamentaux
2	Les obligations légales: droits et devoirs des parties prenantes
3	Les évolutions prévisibles: la portée du futur règlement européen
4	**Quelques conseils pratiques: des exemples concrets**
5	Accompagnement de Datagest pour la protection des données

Datagest

Quelques conseils pratiques: des exemples concrets

Exemple 1 : Programme d'analyse des demandes de carte de crédit

Une entreprise commerciale propose à ses clients des cartes client avec une fonction de crédit.

Pour répondre aux nombreuses demandes, elle a mis en place un système automatisé décidant sur base des informations fournies par le client si une ligne de crédit est accordée.

Quelques conseils pratiques: des exemples concrets

Exemple 1 : Programme d'analyse des demandes de carte de crédit

➔ Art. 31. (a) de la loi de 2002: à condition que la demande de conclusion ou d'exécution du contrat […] ait été satisfaite ou que des mesures appropriées, telle que la possibilité de faire valoir son point de vue, garantissent la sauvegarde de son intérêt légitime

Quelques conseils pratiques: des exemples concrets

Exemple 2 : Externalisation du calcul des salaires à une fiduciaire

Le calcul des salaires n'est pas effectué en interne par le département RH, mais est externalisé auprès d'une fiduciaire.

Quelques conseils pratiques: des exemples concrets

Exemple 2 : Externalisation du calcul des salaires à une fiduciaire

❑L'employeur reste le responsable du traitement

❑La fiduciaire devient sous-traitant

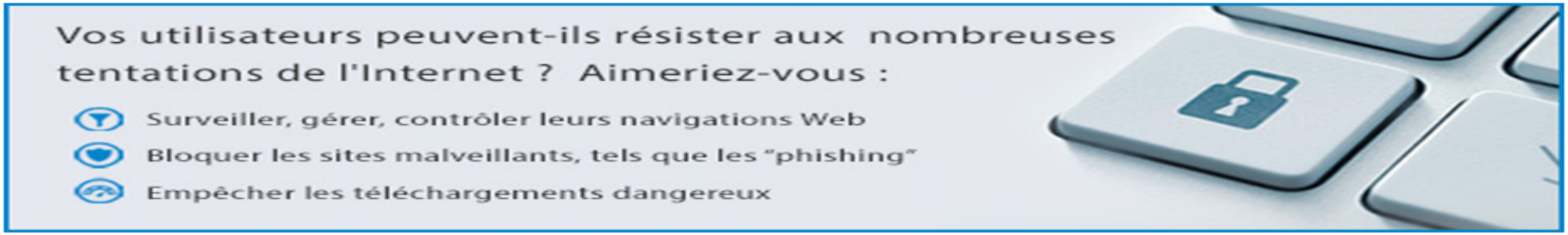
➔Contrat obligatoire mentionnant que :

- Le sous-traitant n'agit que sur la seule instruction du responsable de traitement
- Les obligations de sécurité du responsable de traitement lui incombent également

Datagest

Quelques conseils pratiques: des exemples concrets

Exemple 3 : Publicité pour un contrôle de l'activité WEB



Bonjour Mr XXX,

Les statistiques d'utilisation de l'Internet ne sont pas enthousiasmantes : 40% du temps passé sur Internet serait non-professionnel. Quelques exemples courants : les réseaux sociaux, les web-emails, les vidéos sur Youtube, etc...

Aimeriez-vous améliorer la productivité des membres de votre entreprise, distraits par l'Internet ? Si oui, nous vous recommandons **XYZ Module**.

Module vous révèle les activités principales de vos utilisateurs sur Internet. Grâce à cela, vous pouvez empêcher l'accès vers des sites indésirables, malicieux ou des URL type « Phishing ». Vous pouvez aussi limiter l'accès aux sites perturbateurs de la bande passante. Vous sécurisez en outre votre réseau en scannant les fichiers que téléchargent les utilisateurs.

Ce logiciel XYZ Module, à installer sur un serveur Windows, est vite amorti vu l'impact qu'il a sur la productivité de vos utilisateurs. Vous aimeriez une solution semblable sans recours à un serveur Windows local ? Elle s'appelle « **Module B** », elle existe sur un « serveur virtuel sur le Web », serveur prêt à vous recevoir via un Browser Internet.

Pour chacune de ces solutions, n'hésitez pas à nous contacter.

Bien à vous, YYY

Une question ? Contactez-nous …

.

Datagest

Quelques conseils pratiques: des exemples concrets

Exemple 3 : Publicité pour un contrôle de l'activité WEB

- Surveillance sur le lieu de travail
- Exigence d'une autorisation préalable
- Uniquement possible dans certaines limites
- Le consentement des salariés est exclu

Datagest

Quelques conseils pratiques: des exemples concrets

Exemple 4 : Utilisation de la vidéosurveillance autorisée pour éviter les vols dans un magasin pour démontrer que le salarié fait trop de pauses

Une entreprise souhaite utiliser la vidéosurveillance mise en place pour limiter les vols, et pour laquelle elle a obtenue l'autorisation de la CNPD, afin de surveiller les pauses des salariés.

Quelques conseils pratiques: des exemples concrets

Exemple 4 : Utilisation de la vidéosurveillance autorisée pour éviter les vols dans un magasin pour démontrer que le salarié fait trop de pauses

- La finalité est la protection des biens de l'entreprise
- L'autorisation de vidéosurveillance a été obtenue pour cette finalité
- Détournement de la finalité : non autorisée

Quelques conseils pratiques: des exemples concrets

Exemple 5 : Log informatique retraçant certaines activités

- ❑ Log système donnant des informations sur la connexion
- ❑ Log de sécurité
- ❑ Log applicatif permettant de retracer les modifications

Quelques conseils pratiques: des exemples concrets

Exemple 5 : Log informatique retraçant certaines activités

Le traitement définit les modalités :

- Utilisation en cas d'incident pour comprendre et résoudre le problème➔ en principe autorisé
- Analyse de la performance des salariés ➔ surveillance sur le lieu de travail : autorisation préalable
- Analyse du comportement des consommateurs ➔ surveillance selon l'article 10 : autorisation pour profilage

Quelques conseils pratiques: des exemples concrets

Exemple 6 : Retracer les données relatives à l'utilisation privée des services de téléphonie fixe pour les besoins de la refacturation

Une entreprise souhaite refacturer à ses employés les appels téléphoniques d'ordre privé.

→ délibération du 11/01/2008

Datagest

Quelques conseils pratiques: des exemples concrets

Exemple 6 : Retracer les données relatives à l'utilisation privée des services de téléphonie fixe pour les besoins de la refacturation

→ Demande refusée:

Les utilisations excessives voire abusives du téléphone, que ce soit à des fins privées ou non, ne portent pas atteinte à l'intégrité de l'installation téléphonique ni à aucun autre bien de l'entreprise, de sorte que le point 2 du paragraphe 1er de l'article L.261-1 du Code du Travail ne trouve pas application. « Protection des biens » et « Protection des intérêts commerciaux, économiques ou financiers » de l'entreprise sont deux notions qui ne sauraient être assimilées.

Datagest

Comment appréhender concrètement l'enjeu de la protection des données personnelles?

1	Notions importantes: définitions, législation et principes fondamentaux
2	Les obligations légales: droits et devoirs des parties prenantes
3	Les évolutions prévisibles: la portée du futur règlement européen
4	Quelques conseils pratiques: des exemples concrets
5	**Accompagnement de Datagest pour la protection des données**

Datagest

Comment Datagest peut vous aider dans le rôle de chargé de la protection des données

Les missions possibles

- ❑ Chargé de la protection des données et tenue du registre (en remplacement des notifications)
- ❑ Assistance à la préparation des demandes d'autorisation
- ❑ Intermédiaire entre le responsable de traitement et les personnes concernées
- ❑ Préparation de la conformité au futur règlement

Datagest

Comment Datagest peut vous aider dans le rôle de chargé de la protection des données

Avantages de la désignation d'un chargé de la protection des données

- ❑ Externalisation de vos obligations administratives
- ❑ Meilleure sécurité juridique
- ❑ Simplification des relations avec la CNPD
- ❑ Signe fort d'adhérence au principe de la protection des données

Datagest

Comment Datagest peut vous aider dans le rôle de chargé de la protection des données

Modalités pratiques

- Désignation formelle
- Accord de la CNPD
- Inventaire des traitements
- Inventaire des notifications et autorisations existantes
- Mise en conformité
- Revue annuelle / revue en cas de changements
- Assistance en cas de demandes

Datagest

Informations complémentaires

- Commission Nationale pour la Protection des Données
  www.cnpd.lu

- Association pour la Protection des Données au Luxembourg
  www.apdl.lu

- Contact:
  - Romain Sabel - romain.sabel@datagest.lu
  - Nicolas Vaisse - nicolas.vaisse@datagest.lu

Datagest

Questions…