#FOCUSGDPR - 6/2/2020

6e colloque du think tank www.cap-numerique.org

WORKSHOP SOUS-TRAITANTS DE DONNEES

#FocusGDPR – 6/2/2020
Séance plénière

- Oratrices:
  - Alexandra JASPAR : Directrice du centre de connaissances
    - *Alexandra Jaspar est diplomée de l'ULB et de Northwestern University (Chicago). Elle est experte en protection des données à caractère personnel depuis 19 ans. Elle était avocate au cabinet d'avocats Linklaters et ensuite directrice du département Compliance (anti-blanchiment d'argent et vie privée) chez Bpost . Elle est également "Lecturer" à la Solvay Business School (Programme in EU data protection).*
  - Pavlina PENEVA : *Responsable Communication PME à l'Autorité de la protection des données.*
    - *Madame PENEVA est diplômée de l'ULB avec un Master spécialisé en droit européen. Au sein de l'APD elle occupe actuellement le poste de responsable communication pour les PME. Avant Mme PENEVA a travaillé au sein de la Commission européenne, à la direction générale de la recherche et de l'innovation, pendant 6 ans en tant qu'experte juriste en protection des données.*
  - Juline DESCHUYTENEER : *Conseillère juridique à l'Autorité de protection des données*
    - *Après avoir entamé son stage d'avocate au barreau de Bruxelles, Juline Deschuyteneer a rejoint l'Autorité de protection des données où elle exerce en tant que conseiller juridique en protection des données à caractère personnel depuis 6 ans. Elle a obtenu son diplôme en Droit public à l'Université Libre de Bruxelles et a complété sa formation au sein de cette Université en Droit international des Affaires.*
- Contenu :
  1. Compétences, priorités et bilan de l'APD (des 20 premiers mois du RGPD) –
  2. Quels sont les problèmes les plus fréquemment rencontrés dans les PME ? Quelques exemples concrets.
  3. Rappel des acteurs principaux et des obligations majeures (respect des principes de licéité, de transparence et de proportionnalité; registre des activités de traitement) ;
  4. Présentation de la nouvelle recommandation de l'APD relative au marketing direct;
  5. Les actions de l'APD spécifiquement pour les PME.

http://www.cap-numerique.org

#FocusGDPR – 6/2/2020 Ateliers

Atelier « responsable de traitement de données personnelles »

- **Orateurs :**
  - Damien JACOB :
    - *Chargé de cours et de formation en Belgique (EPHEC, HEPL, HEPHC, HEC-LIEGE), au Grand-Duché et en France. Il est également conseiller indépendant (stratégies sur le web, e-Business, e-Commerce).*
    - *Co-animateur pour l'ASBL CAP NUMERIQUE*
  - JULINE DESCHUYTENEER
    - *Conseillère juridique à l'Autorité de protection des données*
  - Pavlina PENEVA
    - *Responsable Communication PME à l'Autorité de la protection des données*

- **Contenu:**
  - **Rappel des obligations incombant au responsable de traitement selon les RGPD.**
    - **Des recommandations seront apportées pour la rédaction de la charte vie privée, ainsi pour la mise en conformité des traitements de données à des fins de marketing (newsletters, tracking publicitaire,…).**
    - **Echange questions / réponses.**
  - **La nouvelle recommandation de l'APD relative au marketing direct**

Atelier « sous-traitant web »

- **Oratrice :**
  - Alexandra JASPAR :
    - Directrice du centre de connaissances

- **Rappel des obligations incombant au sous-traitant selon le RGPD.**
- **Des recommandations seront également apportées pour bien clarifier la relation contractuelle avec le donneur d'ordre (le responsable du traitement) pour la conception des sites (cookies, opt-in,…) et pour correctement assurer le rôle du sous-traitant.**
- **Echange questions / réponses.**

(e-)marketing - Bien appliquer le GDPR

WORKSHOP

SOUS-TRAITANTS DE DONNEES

GBA Gegevensbeschermingsautoriteit

APD Autorité de protection des données

DSB Datenschutzbehörde

DPA Data Protection Authority

Alexandra Jaspar

Autorité de Protection des Données

Directrice

6/2/2020

Responsable du Traitement vs Sous-traitant - rappel

- **Responsable du traitement**

  « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement »

- **Sous-traitant**

  « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement »

- **Sous sous-traitant:**

2. Le sous-traitant ne recrute pas un autre sous-traitant sans l'autorisation écrite préalable, spécifique ou générale, du responsable du traitement. Dans le cas d'une autorisation écrite générale, le sous-traitant informe le responsable du traitement de tout changement prévu concernant l'ajout ou le remplacement d'autres sous- traitants, donnant ainsi au responsable du traitement la possibilité d'émettre des objections à l'encontre de ces changements.

4. Lorsqu'un sous-traitant recrute un autre sous-traitant pour mener des activités de traitement spécifiques pour le compte du responsable du traitement, les mêmes obligations en matière de protection de données que celles fixées dans le contrat ou un autre acte juridique entre le responsable du traitement et le sous-traitant conformément au paragraphe 3, sont imposées à cet autre sous-traitant par contrat ou au moyen d'un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre, en particulier pour ce qui est de présenter des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement.

Lorsque cet autre sous-traitant ne remplit pas ses obligations en matière de protection des données, le sous-traitant initial demeure pleinement responsable devant le responsable du traitement de l'exécution par l'autre sous-traitant de ses obligations.

Responsable du Traitement vs Sous-traitant – contrat à conclure

3. Le traitement par un sous-traitant est régi par un contrat ou un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre, qui lie le sous-traitant à l'égard du responsable du traitement, définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et les obligations et les droits du responsable du traitement. Ce contrat ou cet autre acte juridique prévoit, notamment, que le sous-traitant:

a) ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement, y compris en ce qui concerne les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel le sous-traitant est soumis; dans ce cas, le sous-traitant informe le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public;

b) veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité;

c) prend toutes les mesures requises en vertu de l'article 32;

d) respecte les conditions visées aux paragraphes 2 et 4 pour recruter un autre sous-traitant;

e) tient compte de la nature du traitement, aide le responsable du traitement, par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits prévus au chapitre III;

f) aide le responsable du traitement à garantir le respect des obligations prévues aux articles 32 à 36, compte tenu de la nature du traitement et des informations à la disposition du sous-traitant;

g)selon le choix du responsable du traitement, supprime toutes les données à caractère personnel ou les renvoie au responsable du traitement au terme de la prestation de services relatifs au traitement, et détruit les copies existantes, à moins que le droit de l'Union ou le droit de l'État membre n'exige la conservation des données à caractère personnel; et

h) met à la disposition du responsable du traitement toutes les informations nécessaires pour apporter la preuve du respect des obligations prévues au présent article et pou permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

En ce qui concerne le point h) du premier alinéa, le sous-traitant informe immédiatement le responsable du traitement si, selon lui, une instruction constitue une violation du présent règlement ou d'autres dispositions du droit de l'Union ou du droit des États membres relatives à la protection des données.

Attention aux modèles-type

Conséquences de cette qualification

NOTAMMENT

- Choix – décisions importantes (vs exécution)
- Définition de la base légale
- Information à fournir + droits à respecter
- Gestion des fuites de données
- Responsabilité & droit de sous (sous) -traiter

Art. 28

1. Lorsqu'un traitement doit être effectué pour le compte d'un responsable du traitement, celui-ci fait uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée.

Exemples

Qui fait quoi? Qui decide quoi?

Loueur de données	Créateur de sites web	Créateur de contenu pour communications de DM/concours	Expert en ciblage publicitaire (ex:media social)	Spécialistes des newsletters
Qui est le RT pour: - Collecte - Enrichissement - Ciblage - Communication	Traite-t-il des données? Pourquoi?	Traite-t-il des données? Pourquoi? Fait-il certaines choix? Lesquels?	Quel choix fait-il? Collecte-t-il les données?	Traite-t-il des données? Pourquoi (juste pour effectuer l'envoi? Fait-il du ciblage?)

Attention aux "disclaimers" et aux intermédiaires

Un exercice parfois compliqué au vu de la multitude des acteurs

Cécile "teste" un concours bidon sur Facebook: "HALLUCINANT" de voir comment ses données personnelles sont siphonnées

Mathieu Tamigniau , publié le 20 décembre 2019 à 06h00 |

RGPD

Depuis trois ans, un Règlement Général de Protection des Données est censé verrouiller la manière dont sont collectées et traitées nos informations personnelles. Si dans la pratique, la plupart des entreprises respectent autant que faire se peut cette "loi", certaines parviennent à la contourner grâce à quelques subterfuges. Notre témoin de 29 ans, active elle-même dans le marketing, a participé à un concours sur Facebook pour gagner en camping-car. Elle n'a rien gagné. En revanche, elle a perdu quelques données personnelles. L'Autorité de Protection de Données fait le point.

Conclusion - conseil

- **Définissez les roles/statuts de tous les acteurs – avant quoi que ce soit**
- **Concluez les contrats requis (ou conseillés)**
  - RT-ST: oui
  - RT conjoints: oui
  - RT-RT: conseillé
  - RT-ST – SST: oui
- **Informez votre personnel de votre role/statut et obligations**
- **Veillez à respecter le contenu de ces contrats**
  - utilisation ds données uniquement aux fins prévues
  - mise en oeuvre des mesures de sécurité et droits d'accès
  - délais de notification d'une violation de données
  - etc
- **Contrôlez vos sous-traitants et choisissez les bien**
  - s'ils livrent des données: garantie (provenance et consentement + preuve)
  - s'ils livrent du contenu (ex: information, collecte de consentements): vérifiez-le
- **Si vos tâches ne requièrent pas le traitement de données, ne les collectez pas**
- **Creez des services privacy-friendly (& by design) pour vos clients:**

Supports d'information

Principe de transparance – obligation du RT

En pratique: "Charte vie privée", "Privacy policy" etc

Utilisez un langage clair

Proposez un canevas conforme à l'article 28 du RGPD, reprenant donc au moins:

- l'identité et les coordonnées du responsable du traitement et, le cas échéant, du représentant du responsable du traitement
- le cas échéant, les coordonnées du délégué à la protection des données;
- les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement;
- lorsque le traitement est fondé sur l'article 6, paragraphe 1, point f), les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers;
- les destinataires ou les catégories de destinataires des données à caractère personnel, s'ils existent; et
- le fait que le responsable du traitement a l'intention d'effectuer un transfert de données à caractère personnel vers un pays tiers;
- la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée;
- l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, la rectification ou l'effacement de celles-ci, ou une limitation du traitement relatif à la personne concernée, ou du droit de s'opposer au traitement et du droit à la portabilité des données;
- lorsque le traitement est fondé sur l'article 6, paragraphe 1, point a), ou sur l'article 9, paragraphe 2, point a), l'existence du droit de retirer son consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci;
- le droit d'introduire une réclamation auprès d'une autorité de contrôle;
- des informations sur la question de savoir si l'exigence de fourniture de données à caractère personnel a un caractère réglementaire ou contractuel ou si elle conditionne la conclusion d'un contrat et si la personne concernée est tenue de fournir les données à caractère personnel, ainsi que sur les conséquences éventuelles de la non-fourniture de ces données;
- l'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 22, paragraphes 1 et 4, et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.
- lorsqu'il a l'intention d'effectuer un traitement ultérieur des données à caractère personnel pour une finalité autre que celle pour laquelle les données à caractère personnel ont été collectées, le responsable du traitement fournit au préalable à la personne concernée des informations au sujet de cette autre finalité et toute autre information pertinente visée au paragraphe 2.

Cookies – mécanisme de collecte de consentement

Obligation du RT (placement et utilisation des données)

Proposez un mécanisme conforme au RGPD:

- **Récolte du consentement du visiteur**
- Avant tout placement d'un cookie
- Sauf pour le placement de cookies absolument indispensables pour le fonctionnement du site (essentiels/fonctionnels vs analytiques)
- **Granulaire: pour chaque type de cookies (pas "en bloc" ex "Tout accepter")**
- Les cookies doivent etre décrits (nom, données collectées et finalités) par catégories – de manière claire
- **Une démarche active est nécessaire** (pas de "refus" ou "désactivation" ni de "en savoir plus") – la poursuite de la navigation ne donne pas lieu à un consentement
- Pas de renvoi vers les sites des tiers (cookies de tiers)
- Le visiteur ne doit pas etre incidé à consentir malgré lui
- **Aucun service, bien ou avanatge ne peut lui etre refusé s'il n'accepte pas (ex: accès au site)**

Le petit guide du développeur:

La CNIL publie un guide destiné aux développeurs afin de les aider à mettre leurs travaux en conformité au RGPD.

Le guide, publié en licence libre, contient 16 fiches thématiques et a vocation à être enrichi par les acteurs du développement web ou applicatif.

La CNIL publie un guide RGPD pour les développeurs

cnil.fr

https://www.cnil.fr/fr/guide-rgpd-du-developpeur

Questions ?

Cap Numérique

- Inciter la société et les entreprises wallonnes à tirer **profit de tous les avantages offerts par les outils numériques** de la manière la plus adéquate possible ;
- Veiller au **développement** et à la **propagation** des enseignements dans le domaine du numérique ;
- Elargir et **entretenir les liens entre les entreprises et les diplômés** des sections socio-économiques de l'enseignement supérieur abordant le domaine du numérique.

Prochains colloques :

www.cap-numerique.org

#FOCUSGDPR - 6/2/2020

6e colloque du think tank www.cap-numerique.org