CONSEIL . AUDIT . FORMATION

PRÉSENTATION

Les exigences relatives au RGPD que les organisations doivent connaître

Jacques ERNOUX
j.ernoux@cplus-consult.be
0496 93 73 43

Cplus sprl
Rue Bâtis de Corère 2B
B – 5336 Courrière (Namur)

YOUR PARTNER FOR PROGRESS

Vision

Votre partenaire de progrès afin de vous accompagner lors de la mise en place de système de management comme outil de gestion au quotidien et vecteur de progrès.

Mission

Mettre en place un système de management performant, adapté, vivant et dynamique, basé sur les enjeux, les parties prenantes (PP), l'analyse des risques et l'amélioration continue

Guider vos projets de manière fonctionnelle jusqu'à son terme avec un budget raisonnable

Apporter notre savoir-faire et notre expérience d'homme de terrain (regard extérieur)

Maintenir à un niveau élevé vos compétences via nos formations continues et nos outils de travail

Respecter les exigences légales et réglementaires liées à votre activitéPrendre en charge la rédaction des documents liés aux différents référentiels (simple, visuel & non redondant)

Valeurs

Efficience : efficace, pratique et simple

Accessibilité : adapté, compréhensible, personnalisé

Fiabilité : flexibilité, confidentialité, expertise

Durabilité : confiance, suivi après mission, relation win-win

CONSEIL . AUDIT . FORMATION

Pourquoi le RGPD ?

CONSEIL . AUDIT . FORMATION

Les évolutions technologiques….

- Vides juridiques dans l'UE
- Les réseaux sociaux (2018)
  - Facebook : 2,07 milliard d'utilisateurs
  - YouTube : 1,50 milliard d'utilisateurs
  - Twitter : 330 millions d'utilisateurs
  - Instagram : 800 millions d'utilisateurs
  - Snapchat : 178 millions d'utilisateurs
  - LinkedIn : 115 millions d'utilisateurs
  - WhatsApp : 1,3 milliard d'utilisateurs actifs
  - Pinterest : 200 millions d'utilisateurs actifs
- Le Big data et arrivée de l'I.A.
- L'internet des objets (IoT plus nombreux que les humains connectés…)
- Les droits des internautes (3,8 milliards de personnes en 2018)

Voir:
https://fr.statista.com/statistiques/571074/nombre-d-utilisateurs-d-internet-dans-le-monde-2005--/
http://www.journaldunet.com/ebusiness/le-net/1071394-nombre-d-internautes-en-france/

LES EXIGENCES RELATIVES AU RGPD QUE LES ORGANISATIONS DOIVENT CONNAÎTRE

2000 : La charte de l'UE exprime clairement dans ses articles 7 et 8 que *la protection des données est un droit fondamental.*

Directive 95/46/CE

2015 : La Cour de justice de l'UE invalide le **Safe Harbour**

ePrivacy : *Encadrer les communications électroniques et la protection de la vie privée*

1998 – 2000 : Le « **Safe Harbour** » est élaboré entre UE et USA

6/7/2016 : *Adoption par l'UE de la directive sur la sécurité des réseaux et des systèmes d'information connue sous l'appellation « **directive NIS** »*

RGPD : Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27/4/2016 *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, et abrogeant la directive 95/46/CE.*

LES EXIGENCES RELATIVES AU RGPD QUE LES ORGANISATIONS DOIVENT CONNAÎTRE

CONSEIL . AUDIT . FORMATION

- Le RGPD est une règlementation « européenne » qui entrera en vigueur en mai 2018. Elle ne nécessite pas de transposition en droit belge contrairement aux « directives ».
- Liens utiles:
  - https://www.privacycommission.be/fr
  - http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=FR

CONSEIL . AUDIT . FORMATION

Les concepts ?

LES EXIGENCES RELATIVES AU RGPD QUE LES ORGANISATIONS DOIVENT CONNAÎTRE

CONSEIL . AUDIT . FORMATION

Le texte réaffirme les principes essentiels de la protection de la vie privée :

- Restriction d'utilisation ;
- Minimisation des données ;
- Précision ;
- Limitation du stockage ;
- Intégrité ;
- Confidentialité.

Art 25 : Protection des données dès la conception et protection des données par défaut

Compte tenu de l'état des connaissances, des coûts de mise en oeuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en oeuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en oeuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée.

Le responsable du traitement met en oeuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée

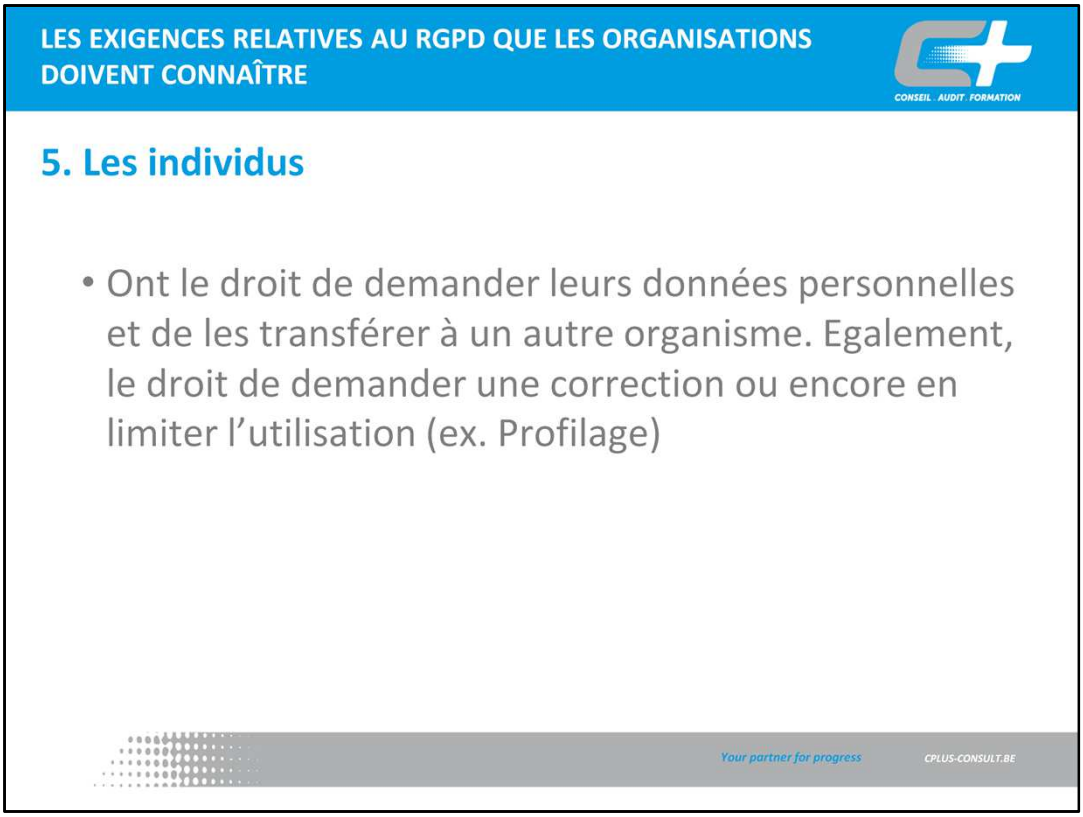
de conservation et à leur accessibilité. En particulier, ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée.

2. Le traitement des données des employés

- Soumis à un examen plus approfondi ;
- Les RH doivent faire partie du processus.

« *Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel.* » (Article 35)

Il rend obligatoire dans certains cas la nomination d'un délégué à la protection des données (DPD ou, en anglais, DPO : Data Protection Officer) pour les organismes privés ou publics dont « les activités de base (…) exigent un suivi régulier et systématique à grande échelle des personnes concernées » ou lorsque « le traitement est effectué par une autorité publique ou un organisme public »
(Article 37)



« Toute information se rapportant à une personne physique identifiée ou identifiable; 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 » (Article 4, §1er RGPD)

« La personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire » (Article 21)

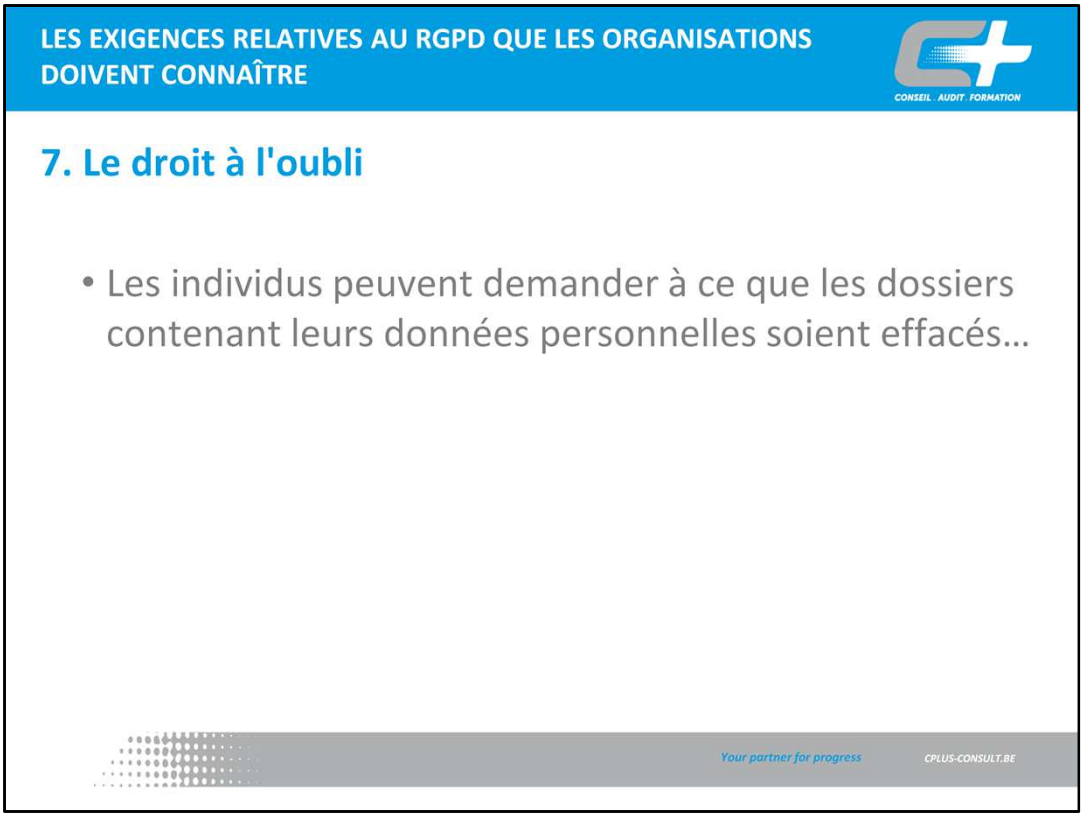
Art 45. Les transferts de données personnelles vers des pays étrangers sont désormais soumis à la vérification des garanties offertes par les lois de ce pays pour préserver un niveau de sécurité équivalent pour les données. Le pays destinataire devra être listé par la Commission européenne.

Art 49. Si le traitement nécessitait de recueillir le consentement de la personne, alors celle-ci devra être informée du transfert de ses données et des risques que présentent l'opération.

« Les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies dans un format structuré, couramment utilisé et lisible par machine, et elles ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle » (Article 20)

6. L'archivage

- Aura une importance de premier ordre pour démontrer la conformité au RGPD.



« La charge de la preuve du consentement pèse sur le responsable du traitement » (Article 7, 1)

Exceptions: exécution d'un contrat accepté par la personne, le traitement découle d'une obligation légale, nécessaire à la sauvegarde des intérêts vitaux de la personne, mission d'intérêt public, personnes mineures, etc

« *La personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données la concernant et le responsable du traitement a l'obligation d'effacer ces données dans les meilleurs délais* » (Article 17)

8. Le responsable de traitement

- Les organismes en charge du traitement des données (responsable de traitement) peuvent maintenant être tenus pour responsables des violations.

« Le Règlement, en cas de piratage, généralise l'obligation de signalement à l'ensemble des responsables de traitement, en ce compris leurs sous-traitants, et ce au plus tard 72 heures après la découverte du problème » (Article 33)

10. Le RGPD requiert une coopération plus étroite

- Entre les différentes autorités de contrôle.
- Autorités de contrôle : autorités publiques indépendantes établies par un état membre de l'UE conformément au RGPD.
- En Belgique, c'est la commission de protection de la vie privée

  (https://www.Privacycommission.Be)

11. Simplification administrative

- Le RGPD élimine la fragmentation législative et la complexité administrative existantes.

➢Pour des économies de 2,3 milliards d'euros par an.

http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

12. Les prestataires de services de certification tiers indépendants

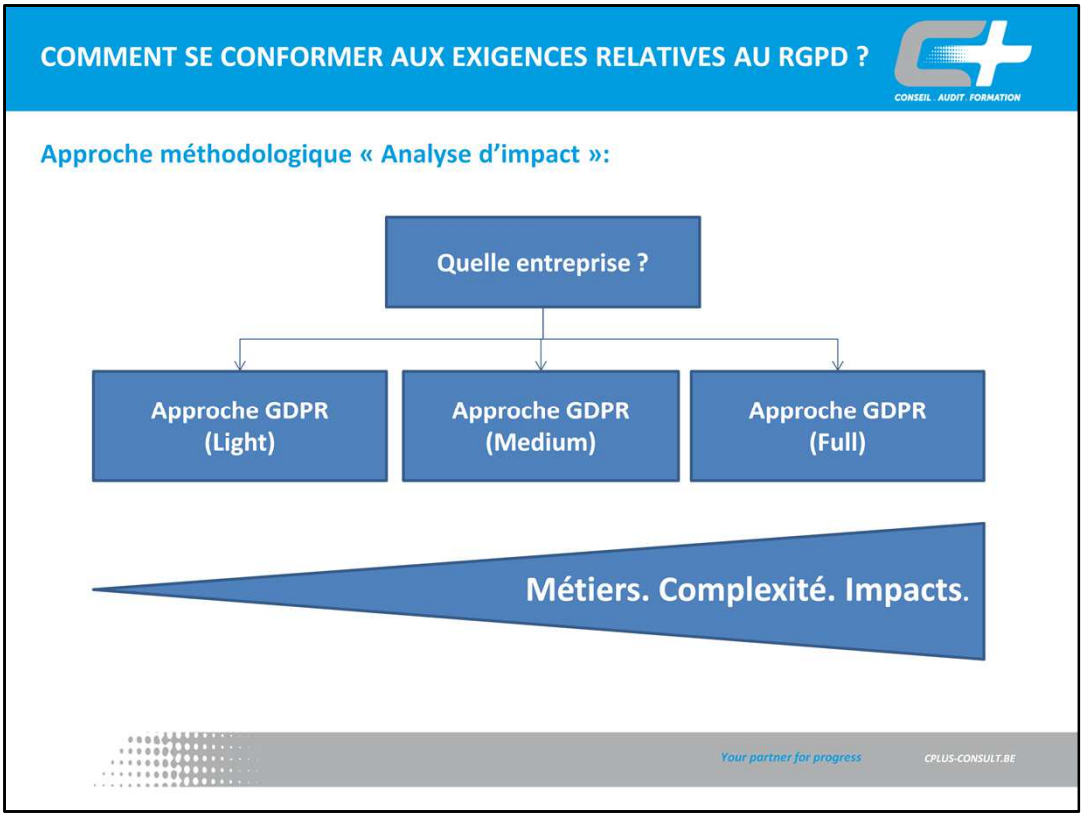
- En vertu des droits d'audit, **des prestataires de services de certification tiers indépendants** devront réaliser des audits réguliers
  - ➢ Pour les organismes en charge du contrôle des données,
  - ➢ Pour ceux en charge du traitement des données.

Le Règlement prévoit quant à lui un « droit à un recours effectif » (Articles 78 et 79) et un « droit à réparation » (Article 82)
Il définit des règles de compétences des juridictions se substituant aux règles de droit international privé des États Membres et détermine les amendes qui devront être délivrées par les autorités nationales de contrôle (Article 83)

Responsabilité civile:
Toute personne ayant subi un dommage matériel ou moral a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi
(Article 82§ 1)
Responsabilité pénale:
Augmentation du montant des amendes «administratives»: 10,000,000 EUR ou 2% du chiffre d'affaires annuel global réalisé par l'entreprise, le plus élevé est retenu (Article 83 § 4)

CONSEIL . AUDIT . FORMATION

Comment se conformer au RGPD ?

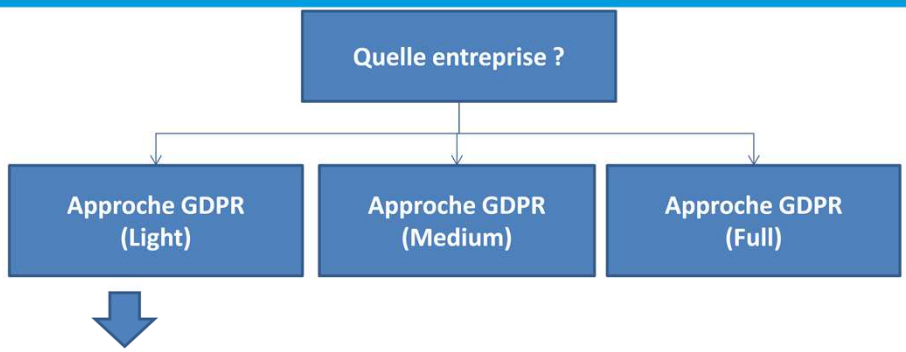


L'analyse d'impact repose sur une approche structurée:

1. Délimiter et décrire le contexte des traitements considérés et ses enjeux;
2. Identifier les mesures existantes ou prévues pour respecter les exigences légales et traiter les risques sur la vie privée de manière proportionnée;
3. Apprécier les risques sur la vie privée pour vérifier qu'ils sont convenablement traités;
4. Prendre la décision de valider la manière dont il est prévu de respecter les principes de protection de la vie privée et de traiter les risques, ou bien réviser les étapes précédentes.
5. Etablir une proposition de « plan d'action ».

COMMENT SE CONFORMER AUX EXIGENCES RELATIVES AU RGPD ?

CONSEIL . AUDIT . FORMATION

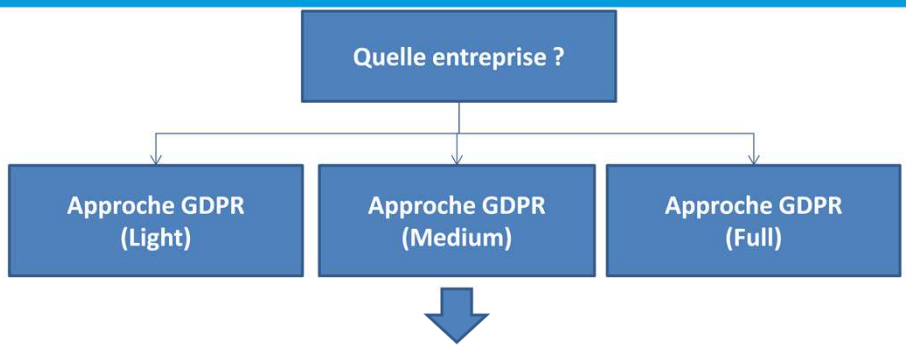


*Nous proposons un **atelier sur mesure d'une journée** (½ sur site et ½ pour finaliser le rapport). Nous travaillons en suivant une liste de vérification des points les plus pertinents pour vous.*

*Nous proposons un **rapport** expliquant a manière dont vous pouvez les gérer.*

COMMENT SE CONFORMER AUX EXIGENCES RELATIVES AU RGPD ?

CONSEIL . AUDIT . FORMATION



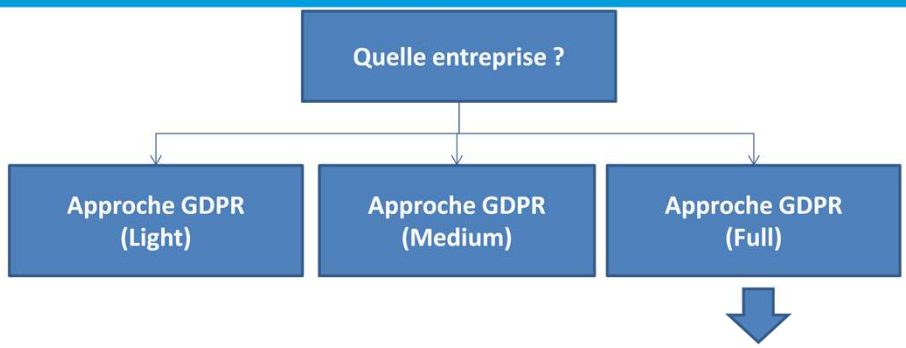
*Atelier sur mesure, plus minutieux, de **deux jours**.*

Nous approfondissons la matière et procédons à une analyse de l'écart. En d'autres termes, nous examinons la situation actuelle et la comparons avec la situation souhaitée.

*Cet inventaire constitue le point de départ par excellence d'un **plan d'action** efficace.*

COMMENT SE CONFORMER AUX EXIGENCES RELATIVES AU RGPD ?

CONSEIL . AUDIT . FORMATION



*Dans un budget d'environ **5 jours**, nous passons à l'étape supérieure et effectuons une analyse de risques intensive pour votre PME, débouchant sur des conseils clairs, sur mesure.*

*Outre le **plan d'action**, nous proposons également une **feuille de route** visant à la conformité de votre organisation au RGPD.*

COMMENT SE CONFORMER AUX EXIGENCES RELATIVES AU RGPD ?

CONSEIL . AUDIT . FORMATION

Principaux documents, procédures, polices à mettre en œuvre

Politique cadre de protection des données personnelles		
	Politique de protection des données personnelles	Article 24(2)
	Politique de confidentialité	Articles 12, 13, 14
	Politique de rétention des données	Articles 5(1)(e), 13(1), 17, 30
	Annexe - Calendrier de conservation des données	Article 30
	Job description du "Data Protection Officer"	Articles 37, 38 et 39

Cartographie des activités de traitement		
	Annexe - Inventaire des activités de traitement	Article 30

Your partner for progress CPLUS-CONSULT.BE

Il s'agit d'un minimum requis…

Principaux documents, procédures, polices à mettre en œuvre

Gestion des droits relatifs aux données		
	Formulaire de consentement du sujet de données	Articles 6(1)(a), 7(1), 9(2)
	Formulaire de retrait du consentement du sujet de données	Article 7, paragraphe 3
	Formulaire de consentement parental. Si applicable…	*Article 8*
	Formulaire de retrait du consentement parental. Si applicable…	*Article 8*
	Analyse d'impact de la protection des données (DPIA)	Article 35

Principaux documents, procédures, polices à mettre en œuvre

Transfer de données à caractère personnel (pays tiers, ou hors UE)		*Si applicable...*
	Annexe 1 - Clauses contractuelles types pour le transfert des DCP aux contrôleurs	Article 46, § 5
	Annexe 2 - Clauses contractuelles types pour le transfert des DCP aux sous-traitants	Article 46, § 5

Tiers de confiance, sous-traitants		
	Accord de traitement des données par les fournisseurs (sous-traitant)	Articles 28, 32 et 82

Principaux documents, procédures, polices à mettre en œuvre

Infractions aux données personnelles		
	Réponse à une violation de données et procédure de notification	Articles 4, §12, 33 et 34
	Registre de violation de données	Article 33, §5
	Formulaire de notification de violation de données à l'autorité	Article 33
	Formulaire de notification de violation de données aux sujets	Article 34

Questions?

Merci de votre attention

Cplus sprl
Rue Bâtis de Corère, 2b
B-5336 Courrière
Tél. : +32 83 61 31 08
info@cplus-consult.be
www.cplus-consult.be

OPTIMISEZ VOTRE ORGANISATION