POD MAATSCHAPPELIJKE INTEGRATIE
BETER SAMEN LEVEN
SPP INTÉGRATION SOCIALE
MIEUX VIVRE ENSEMBLE

PLATEFORME des DPD des CPAS
(Fédération des CPAS)

ANALYSE des QUESTIONNAIRES BCSS 2021

SCHREMS II

17 MAI 2022

AGENDA

- Questionnaire « Normes Minimales » de la BCSS
    - Analyse des questionnaires rentrés en 2021;
    - Que peut-on tirer de cette analyse? Réflexions / Actions

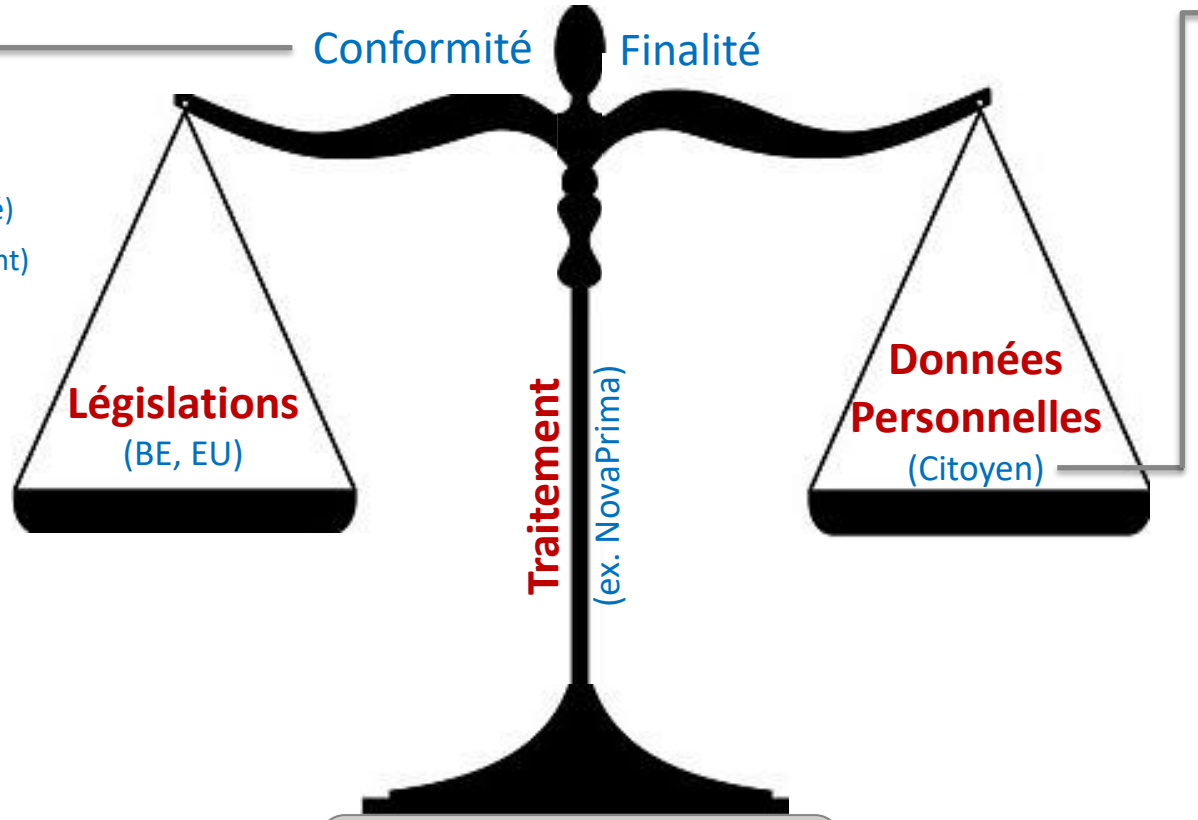
- Conséquences de l'arrêt "Schrems II";
    - Que dit l’arrêt et à quoi le DPD doit-il veiller?
    - Un « cas d’école »

- Divers / Q&R

RGPD – Bref Rappel

Responsable du Traitement
(SPP IS)

OBLIGATIONS:
- DPD
- « Privacy by Design »
- Transparence (Notice de Confidentialité)
- Documentation (Registres de traitement)
- Analyse de risque (DPIA & TIA)
- Contrats (RT-RT, RT-ST)
- Procédures en cas de:
  - Violation de données
  - Demande d'exercice de droits



DROITS:
- Transparence
- Objection
- Consultation
- Correction
- Oubli (effacement)
- Portabilité

Analyse du « Questionnaire MnM » de la BCSS

Les réponses des divers CPAS aux « Questionnaire Normes Minimales » 2021 de la BCSS, bien qu'en progrès significatif par rapport aux années précédentes, présentent néanmoins de nombreux points d'améliorations possibles.

Une analyse statistique mène à une réflexion sur les aspects suivants:

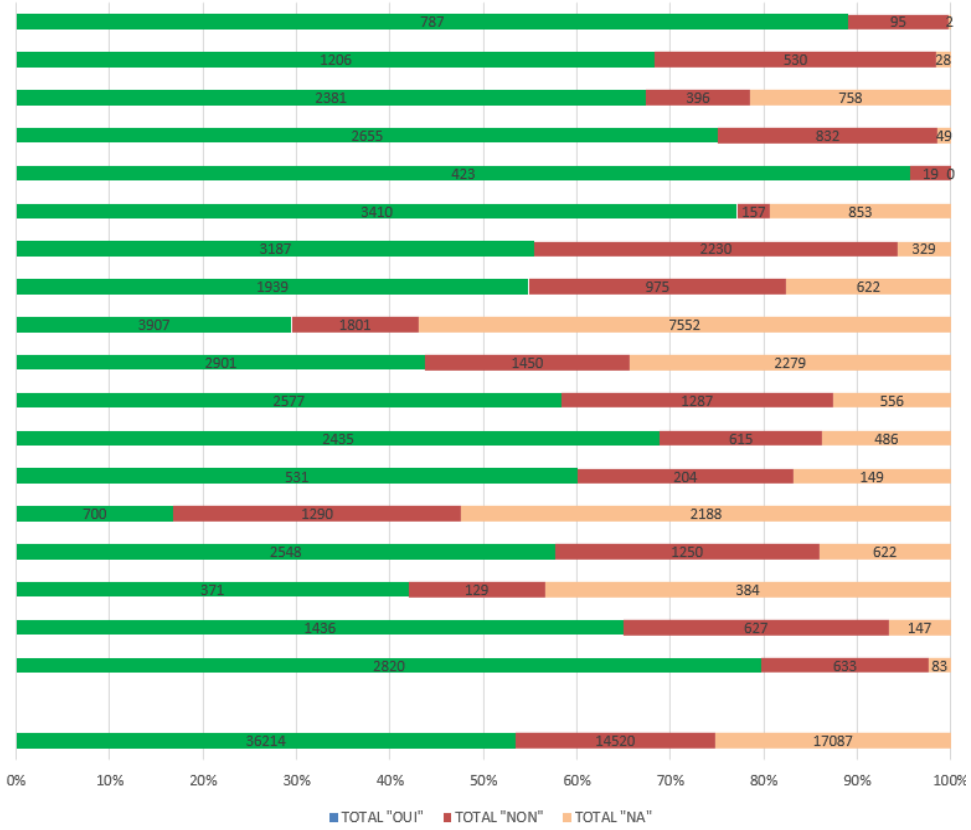
- Taux de répondants
- Pertinence des questions
- Sentiment de ne pas être concerné
- Sentiment d'impuissance dans le rôle de DPD
- Manque de moyens

Analyse du « Questionnaire MnM »: les chiffres

THÈMES:

1	Politique de sécurité de l'information et principes de base
2	Plan de sécurité et la gestion des risques
3	Organisation de la sécurité de l'information
4	Sécurité liée aux collaborateurs
5	Sécurité physique et protection de l'environnement
6	Protection de l'accès logique à systèmes d'information (production, test, development, …)
7	Gestion des ressources de l'entreprise lors du traitement des informations
8	Médias d'enregistrement et appareils mobiles
9	Achat, conception, développement et maintenance de systèmes d'information ICT (applications) : gestion des projets ou programmes
10	Achat, conception, développement et maintenance de systèmes d'information ICT (applications) : transition et support ICT
11	Garantir la continuité et la disponibilité de systèmes d'information de l'institution et ICT
12	Protection de la communication implémentée au moyen des ICT
13	Télétravail et accès en ligne en dehors de l'organisation
14	Mise en place de mesures de chiffrement
15	Relations avec des fournisseurs et travaux avec une tierce partie
16	Systèmes d'information Cloud ICT
17	Respect
18	Gestion des incidents
19	TOUS THÈMES CONFONDUS

OUI / NON / NA par THÈME



Analyse du « Questionnaire MnM »: Constatations/Réflexions

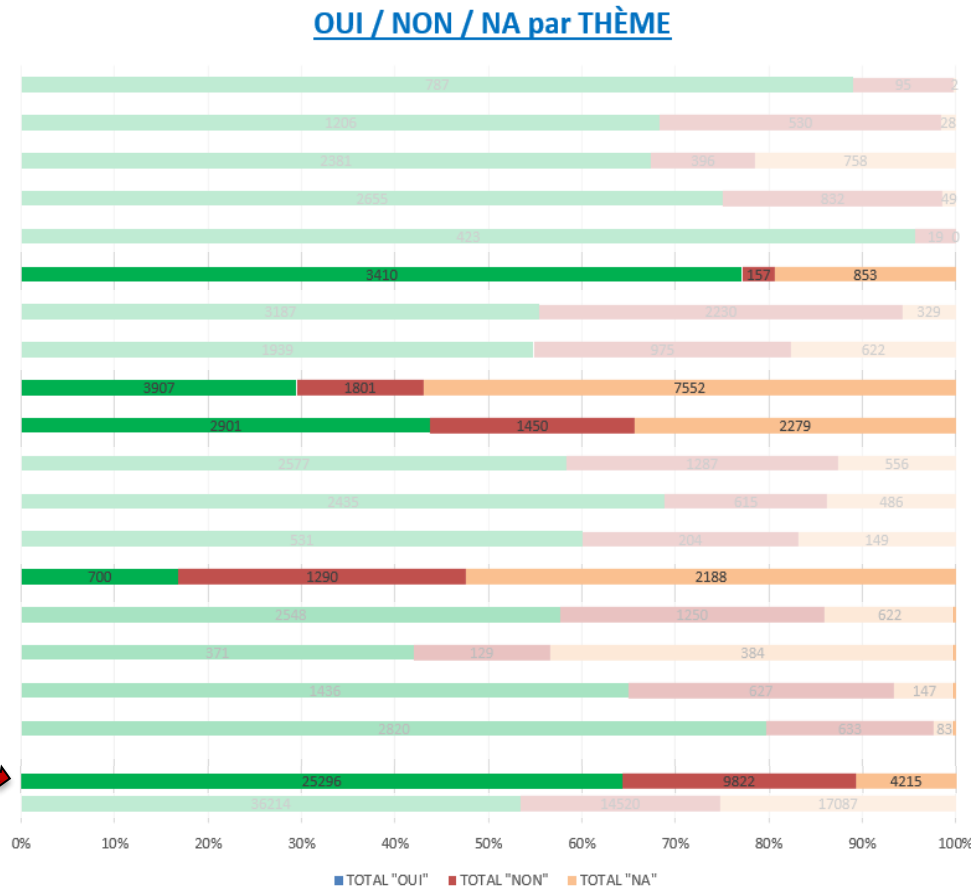
- Caveat: L'analyse n'a pas:
  - porté sur la qualité des explications données en cas de « non » ou « n.a. »
  - ni permis de faire la différence entre répondants NL ou FR
  - ni fait la distinction entre petits et grands CPAS
- Près de ¼ des CPAS (NL & FR confondus) n'ont pas répondu
- Sur l'ensemble des (±68.000) réponses, à peine plus de 50% de « OUI » francs
- Quelques thèmes sortent très clairement de la zone d'influence des DPD de CPAS dépendant de leur fournisseur ICT ou de concepteurs d'applications
- Bien que les sentiments d'impuissance ou de manque de moyens expliquent certaines réponses, on peut s'interroger sur le rôle que les DPD estiment pouvoir ou devoir jouer dans le cadre de leurs mission et responsabilités

Analyse du « Questionnaire MnM »: zoom sur les détails (1 de 3)

Compréhensible et Acceptable pour les (petits) CPAS « héritant » de développements externes

	THÈMES:
1	Politique de sécurité de l'information et principes de base
2	Plan de sécurité et la gestion des risques
3	Organisation de la sécurité de l'information
4	Sécurité liée aux collaborateurs
5	Sécurité physique et protection de l'environnement
6	Protection de l'accès logique à systèmes d'information (production, test, development, …)
7	Gestion des ressources de l'entreprise lors du traitement des informations
8	Médias d'enregistrement et appareils mobiles
9	Achat, conception, développement et maintenance de systèmes d'information ICT (applications) : gestion des projets ou programmes
10	Achat, conception, développement et maintenance de systèmes d'information ICT (applications) : transition et support ICT
11	Garantir la continuité et la disponibilité de systèmes d'information de l'institution et ICT
12	Protection de la communication implémentée au moyen des ICT
13	Télétravail et accès en ligne en dehors de l'organisation
14	Mise en place de mesures de chiffrement
15	Relations avec des fournisseurs et travaux avec une tierce partie
16	Systèmes d'information Cloud ICT
17	Respect
18	Gestion des incidents
19	TOUS THÈMES CONFONDUS

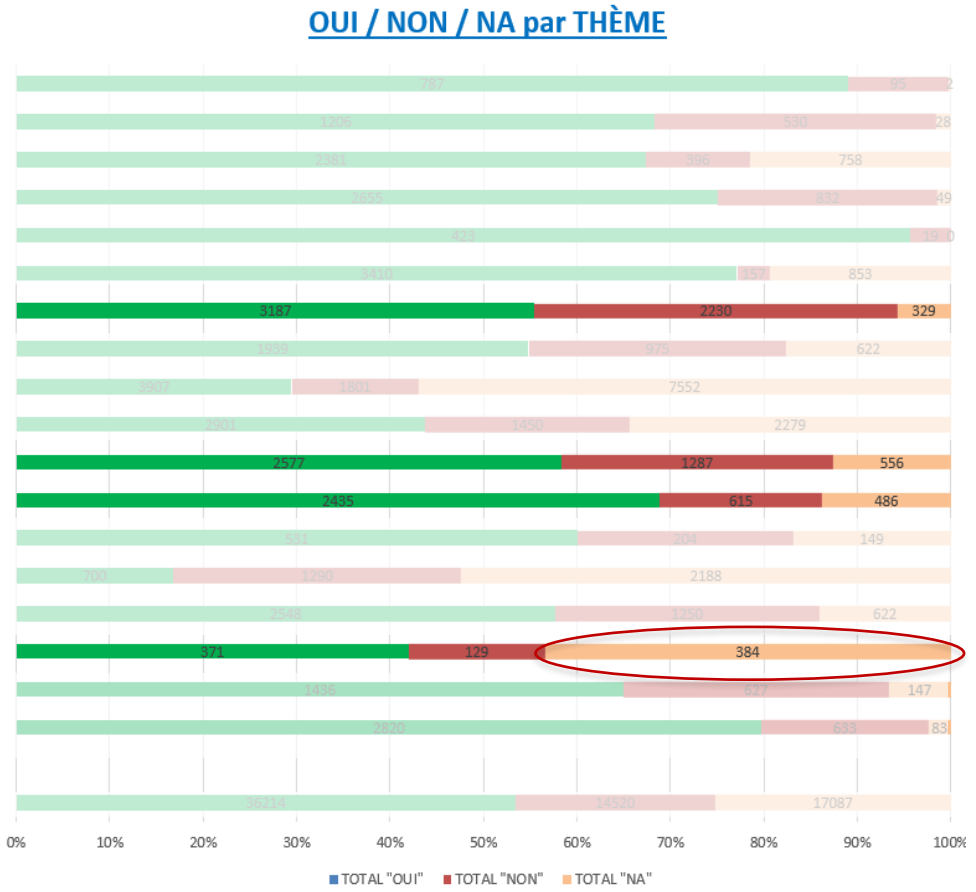
Totaux « O/N/na » adaptés si 6, 9, 10 et 14 exclus



Analyse du « Questionnaire MnM »: zoom sur les détails (2 de 3)

Traduit le sentiment d'impuissance dû à une implication trop faible (importance du rôle mal perçue?)

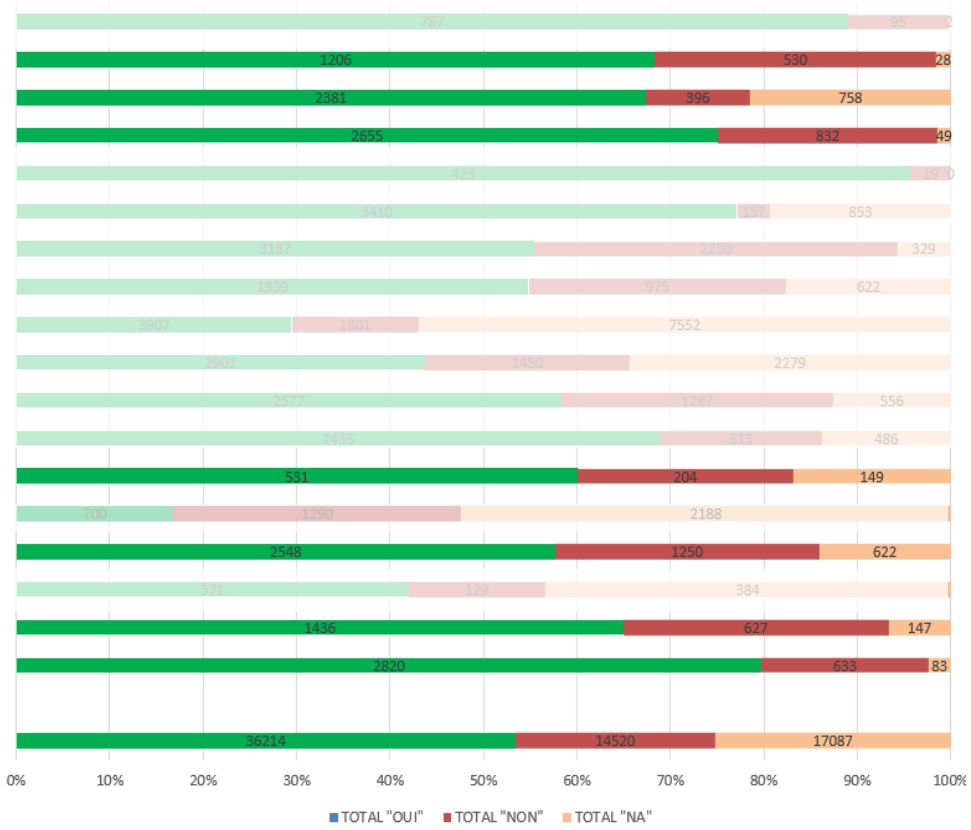
THÈMES:	
1	Politique de sécurité de l'information et principes de base
2	Plan de sécurité et la gestion des risques
3	Organisation de la sécurité de l'information
4	Sécurité liée aux collaborateurs
5	Sécurité physique et protection de l'environnement
6	Protection de l'accès logique à systèmes d'information (production, test, development, …)
7	**Gestion des ressources de l'entreprise lors du traitement des informations**
8	Médias d'enregistrement et appareils mobiles
9	Achat, conception, développement et maintenance de systèmes d'information ICT (applications) : gestion des projets ou programmes
10	Achat, conception, développement et maintenance de systèmes d'information ICT (applications) : transition et support ICT
11	**Garantir la continuité et la disponibilité de systèmes d'information de l'institution et ICT**
12	**Protection de la communication implémentée au moyen des ICT**
13	Télétravail et accès en ligne en dehors de l'organisation
14	Mise en place de mesures de chiffrement
15	Relations avec des fournisseurs et travaux avec une tierce partie
16	**Systèmes d'information Cloud ICT**
17	Respect
18	Gestion des incidents
19	**TOUS THÈMES CONFONDUS**



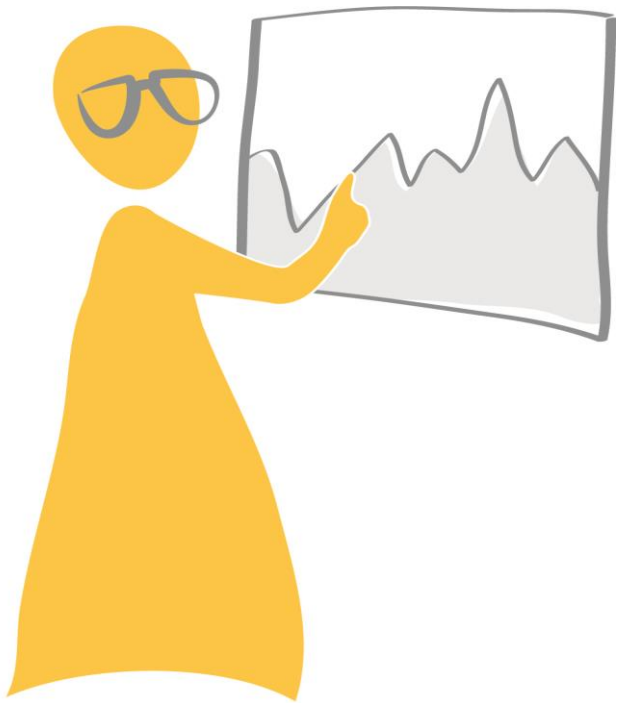
Analyse du « Questionnaire MnM »: zoom sur les détails (3 de 3)

???

THÈMES:	
1	Politique de sécurité de l'information et principes de base
2	Plan de sécurité et la gestion des risques
3	Organisation de la sécurité de l'information
4	Sécurité liée aux collaborateurs
5	Sécurité physique et protection de l'environnement
6	Protection de l'accès logique à systèmes d'information (production, test, development, …)
7	Gestion des ressources de l'entreprise lors du traitement des informations
8	Médias d'enregistrement et appareils mobiles
9	Achat, conception, développement et maintenance de systèmes d'information ICT (applications) : gestion des projets ou programmes
10	Achat, conception, développement et maintenance de systèmes d'information ICT (applications) : transition et support ICT
11	Garantir la continuité et la disponibilité de systèmes d'information de l'institution et ICT
12	Protection de la communication implémentée au moyen des ICT
13	Télétravail et accès en ligne en dehors de l'organisation
14	Mise en place de mesures de chiffrement
15	Relations avec des fournisseurs et travaux avec une tierce partie
16	Systèmes d'information Cloud ICT
17	Respect
18	Gestion des incidents
19	TOUS THÈMES CONFONDUS



Questions / Réflexions / Débat



Schrems, la bombe GDPR!

L'USINED

(Quelle: Pixabay/WilliamCho

AR/VR 5G Intelligence artificielle Mc

2. Februar 2022 - Bei der dynamischen Einbindung von Google Fonts wird die IP-Adresse des Besuchers an Google übermittelt. Dies verletzt laut einem Urteil des Landgerichts München das Persönlichkeitsrecht.

ACCUEIL › CLOUD

Les Cnil européennes lancent une action sur l'utilisation du cloud par le secteur public

22 autorités européennes de protection des données, dont la Cnil, chapeautées par le Comité européen de la protection des données lancent une action sur l'utilisation par le secteur public de services utilisant le cloud. Elles souhaitent s'assurer que ces solutions respectent bien le RGPD.

LE SOIR Alerte info

Meta menace de ne plus proposer Facebook et Instagram en Europe

Meta, la société mère de Facebook, envisage de quitter l'Europe si le groupe n'est plus autorisé à partager les données des utilisateurs européens avec les Etats-Unis.

rtbf.be THÉMATIQUES PLUS

Facebook Says it Will Stop Operating in Eur If Regulators Don't Back Down

European regulators are cracking down on Facebook's ability to transfer data across the Atlantic. Now the tech giant is threatening to pull its services from more than 400 million European users.

MONDE EUROPE

Protection des données personnelles : Meta menace de ne plus proposer Facebook et Instagram en Europe

Schrems, la bombe GDPR!

Verbod Google Analytics dreigt: 'Overdracht data illegaal'

10 februari 2022 15:59
Aangepast: 10 februari 2022 16:54

Websites in de EU moeten mogelijk binnenkort stoppen met het gebruik van Google Analytics om het gedrag van bezoekers te meten. Ook de Franse privacywaakhond CNIL zegt nu dat het gebruik van Analytics de EU-privacywet AVG overtreedt.

Internetrecht door Arnoud Engelfriet

Arnoud Engelfriet is ICT-jurist, gespecialiseerd in internetrecht.Hij werkt als partner bij juridisch adviesbureau ICTRecht. Zijn site Ius mentis heeft meer dan 350 artikelen over internetrecht.

OVER ARNOUD | JURIDISCHE DOCUMENTEN | JURIDISCH ADVIES | WORLD OF

Duitse website veroordeeld voor doorgeven ip-adres bezoeker via Google Fonts

DataNews Rubrieken ▾ Het magazine Voordelen voor abonnees Abonneren

Facebook-moederbedrijf dreigt er opnieuw mee uit Europa te vertrekken

04/02/22 om 21:56 Bijgewerkt om 21:55 Bron : Belga

Facebook-moederbedrijf Meta Platforms overweegt te vertrekken uit Europa als het concern geen data van Europese gebruikers meer mag uitwisselen met de Verenigde Staten. Die boodschap herhaalt het socialemediabedrijf in een document dat het concern heeft ingediend bij de Amerikaanse beurstoezichthouder SEC.

Conséquences de l'arrêt "Schrems II« (1 de 2)

1. Que dit l'arrêt de la CJUE?
   - ❑ Attention à tout transfert de données personnelles vers un pays ne disposant pas d'une décision d'adéquation avec l'U.E. (cela concerne e.a. les USA)
   - ❑ Si existants, ces transferts doivent faire l'objet d'une Analyse d'Impact des Transferts (« TIA ») et de l'établissement de CCT (« Clauses Contractuelles Types ») avec chaque fournisseur concerné;
   - ❑ Les données concernées doivent faire l'objet de mesures fortes les protégeant de leur consultation hors du scope du traitement initial;

2. En quoi un DPD doit-il se sentir concerné?
   - ❑ Évaluer avec pertinence le recours à des solutions « Cloud »
   - ❑ Évaluer l'utilisation de logiciels « made in US » : Office365, Teams, Zoom & C°
     + analyser comment sont implémentés ServiceNow, Sharepoint, Outlook, Skype, …
   - ❑ Sites Web et Webapps: utilisation de cookies, de GoogleAnalytics, GoogleFonts, etc. :

Conséquences de l'arrêt « Schrems II » (2 de 2)

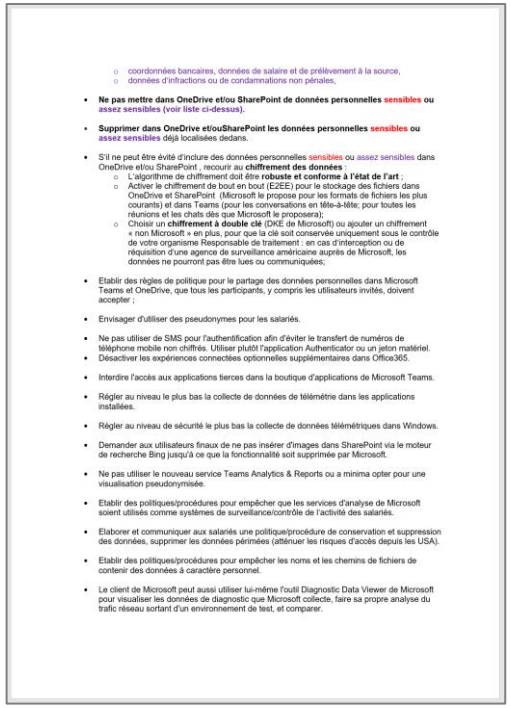
Approche pour se mettre à l'abri de tout reproche

1. **Identifiez précisément les données susceptibles de se voir transférées hors U.E.**
   - par ex. évaluer la nécessité, assurer la minimisation des données, etc. Cela nécessite un exercice de cartographie des données approprié. Y a-t-il des transferts ultérieurs ?
2. **Vérifiez les outils de transfert sur lesquels vous comptez.**
   - Articles 45 à 49 RGPD.
   - seules les décisions d'adéquation de la CE offrent une certitude à 100 %.
3. **Évaluer son efficacité dans le contexte de la législation ou de la pratique du pays tiers.**
   - demander à l'importateur de données de fournir des informations sur la législation et la jurisprudence du pays tiers..
4. **Identifier et adopter des mesures complémentaires en vue d'atteindre une protection équivalente**
   - peuvent être des mesures techniques (par exemple, chiffrement), organisationnelles (par exemple, politiques internes) ou juridiques (par exemple, contrats).
   - ne pas transférer si les mesures complémentaires paraissent insuffisantes.
5. **Prendre des mesures procédurales formelles pour remplir la quatrième étape si nécessaire**
   - contacter l'autorité de contrôle compétente en cas de besoin au titre de l'article 45 ou 46 RGPD
6. **Évaluez régulièrement vos mesures complémentaires.**
   - L'outil de transfert et les éventuelles mesures complémentaires peuvent être amenés à évoluer dans le temps.

Quelle(s) Action(s) envisager ?

Exemples de quelques possibilités… (documents brièvement présentés et annexés à la présentation)

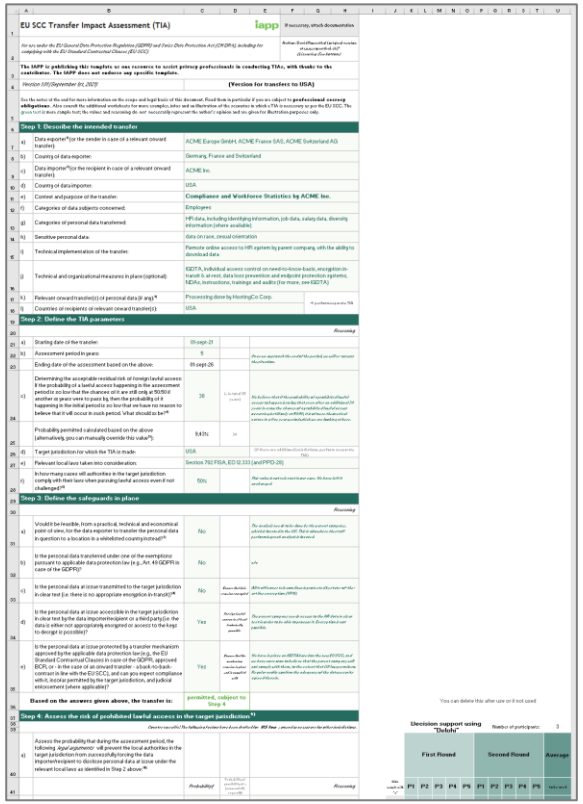
Recommandations_sur_l_utilisation_des_services_Microsoft_365_depuis_l_invalidation_du_traite_UE_USA_Privacy_Shield_V_02a.docx



- coordonnées bancaires, données de salaire et de prélèvement à la source,
- données d'infractions ou de condamnations non pénales,

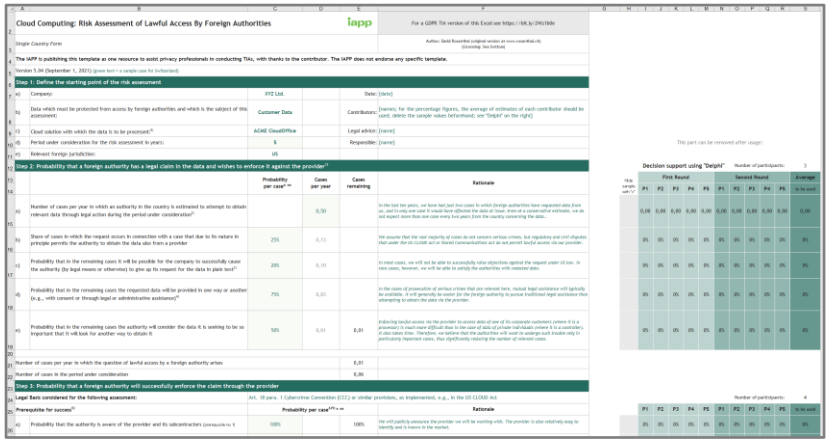
- **Ne pas mettre dans OneDrive et/ou SharePoint de données personnelles sensibles ou assez sensibles (voir liste ci-dessus).**
- **Supprimer dans OneDrive et/ouSharePoint les données personnelles sensibles ou assez sensibles déjà localisées dedans.**
- S'il ne peut être évité d'inclure des données personnelles sensibles ou assez sensibles dans OneDrive et/ou SharePoint , recourir au **chiffrement des données** :
  - L'algorithme de chiffrement doit être **robuste et conforme à l'état de l'art** ;
  - Activer le chiffrement de bout en bout (E2EE) pour le stockage des fichiers dans OneDrive et SharePoint (Microsoft le propose pour les formats de fichiers les plus courants) et dans Teams (pour les conversations en tête-à-tête; pour toutes les réunions et les chats dès que Microsoft le proposera);
  - Choisir un **chiffrement à double clé** (DKE de Microsoft) ou ajouter un chiffrement « non Microsoft » en plus, pour que la clé soit conservée uniquement sous le contrôle de votre organisme Responsable de traitement : en cas d'interception ou de réquisition d'une agence de surveillance américaine auprès de Microsoft, les données ne pourront pas être lues ou communiquées;
- Etablir des règles de politique pour le partage des données personnelles dans Microsoft Teams et OneDrive, que tous les participants, y compris les utilisateurs invités, doivent accepter ;
- Envisager d'utiliser des pseudonymes pour les salariés.
- Ne pas utiliser de SMS pour l'authentification afin d'éviter le transfert de numéros de téléphone mobile non chiffrés. Utiliser plutôt l'application Authenticator ou un jeton matériel.
- Désactiver les expériences connectées optionnelles supplémentaires dans Office365.
- Interdire l'accès aux applications tierces dans la boutique d'applications de Microsoft Teams.
- Régler au niveau le plus bas la collecte de données de télémétrie dans les applications installées.
- Régler au niveau de sécurité le plus bas la collecte de données télémétriques dans Windows.
- Demander aux utilisateurs finaux de ne pas insérer d'images dans SharePoint via le moteur de recherche Bing jusqu'à ce que la fonctionnalité soit supprimée par Microsoft.
- Ne pas utiliser le nouveau service Teams Analytics & Reports ou a minima opter pour une visualisation pseudonymisée.
- Etablir des politiques/procédures pour empêcher que les services d'analyse de Microsoft soient utilisés comme systèmes de surveillance/contrôle de l'activité des salariés.
- Elaborer et communiquer aux salariés une politique/procédure de conservation et suppression des données, supprimer les données périmées (atténuer les risques d'accès depuis les USA).
- Etablir des politiques/procédures pour empêcher les noms et les chemins de fichiers de contenir des données à caractère personnel.
- Le client de Microsoft peut aussi utiliser lui-même l'outil Diagnostic Data Viewer de Microsoft pour visualiser les données de diagnostic que Microsoft collecte, faire sa propre analyse du trafic réseau sortant d'un environnement de test, et comparer.

eu_scc_transfer_impact_assessment.xlsx



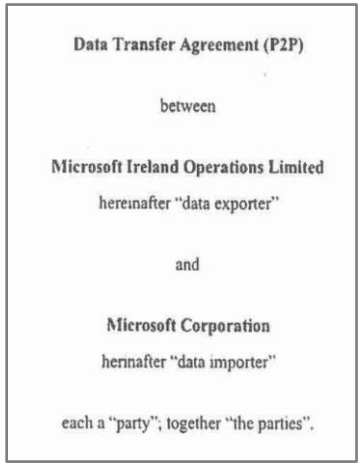
EU SCC Transfer Impact Assessment (TIA)

cloud_computing_risk_assessment_of_lawful_access_by_foregn_authorities.xlsx



Cloud Computing: Risk Assessment of Lawful Access By Foreign Authorities

Microsoft_Standard_Contractual_Clauses_1.pdf



Data Transfer Agreement (P2P)

between

Microsoft Ireland Operations Limited

hereinafter "data exporter"

and

Microsoft Corporation

hereinafter "data importer"

each a "party"; together "the parties".

Vers un « Schrems III » ?

https://noyb.eu/en/privacy-shield-20-first-reaction-max-schrems

"Privacy Shield 2.0"? - First Reaction by Max Schrems

Déclaration:

"Nous avions déjà un accord purement politique en 2015 qui n'avait aucune base légale. D'après ce que vous entendez, nous pourrions jouer au même jeu une troisième fois maintenant.
L'accord était apparemment un symbole que von der Leyen voulait, mais n'a pas le soutien des experts. à Bruxelles, car les États-Unis n'ont pas bougé.
Il est particulièrement épouvantable que les États-Unis aient prétendument utilisé la guerre contre l'Ukraine pour pousser l'UE sur cette question économique.

"Le texte final aura besoin de plus de temps, une fois qu'il arrivera, nous l'analyserons en profondeur, avec nos experts juridiques américains. S'il n'est pas conforme au droit de l'UE, nous ou un autre groupe le contesterons probablement. En fin de compte, le La Cour de justice se prononcera une troisième fois. Nous nous attendons à ce que cela revienne devant la Cour dans les mois suivant une décision finale.«

"Il est regrettable que l'UE et les États-Unis n'aient pas utilisé cette situation pour parvenir à un accord de" non-espionnage ", avec des garanties de base entre des démocraties partageant les mêmes idées.
Les clients et les entreprises font face à plus d'années d'incertitude juridique."

- Max Schrems, Honorary Chairman of *noyb* and lead litigant in the "Schrems I" and "Schrems II" cases before the CJEU.

Accord entre l'Europe et les États-Unis pour le transfert des données personnelles

Jean-Baptiste A. — 25 Mar. 2022 • 17:02 — 0 — 3

La Commission européenne et les États-Unis ont annoncé avoir trouvé un accord de principe sur un nouveau cadre pour le transfert des données personnelles de l'Union européenne vers les États-Unis. C'est un élément crucial pour l'économie numérique, après l'invalidation du précédent dispositif par la justice européenne.

Nouvel accord entre les États-Unis et l'Europe sur les données

L'annonce, faite à Bruxelles par le président américain Joe Biden et la présidente de la Commission européenne Ursula von der Leyen, intervient après des mois de négociations. Elle fait suite à l'invalidation en juillet 2020 par la justice européenne de l'accord Privacy Shield qui permettait ce transfert, en raison de craintes sur les programmes de surveillance américains.

https://kulturegeek.fr/news-254989/accord-entre-leurope-etats-unis-transfert-donnees-personnelles

En guise de conclusion: un « cas d'école »…

Plutôt thé ou café ? Ascenseur ou escalier ?

Certes, on s'est habitués à travailler ensemble sans se voir. Mais peut-être vous souvenez-vous quand même des petites habitudes de vos collègues. Et eux, pensez-vous qu'ils se souviennent des vôtres ?

Nous vous invitons à **remplir ce petit** questionnaire sur vous et à **envoyer une photo de vous** au groupe Culture et Cohésion sociale pour le **jeudi 10 février**. Précision utile : aucune question n'est obligatoire, vous pouvez ne répondre qu'à celles qui vous inspirent ou vous correspondent le mieux.

Un nouveau questionnaire sera ensuite diffusé à l'ensemble des collègues afin que les uns deviennent les habitudes des autres. L'occasion, assurément, de se remémorer le « bon vieux temps » à la Finto !

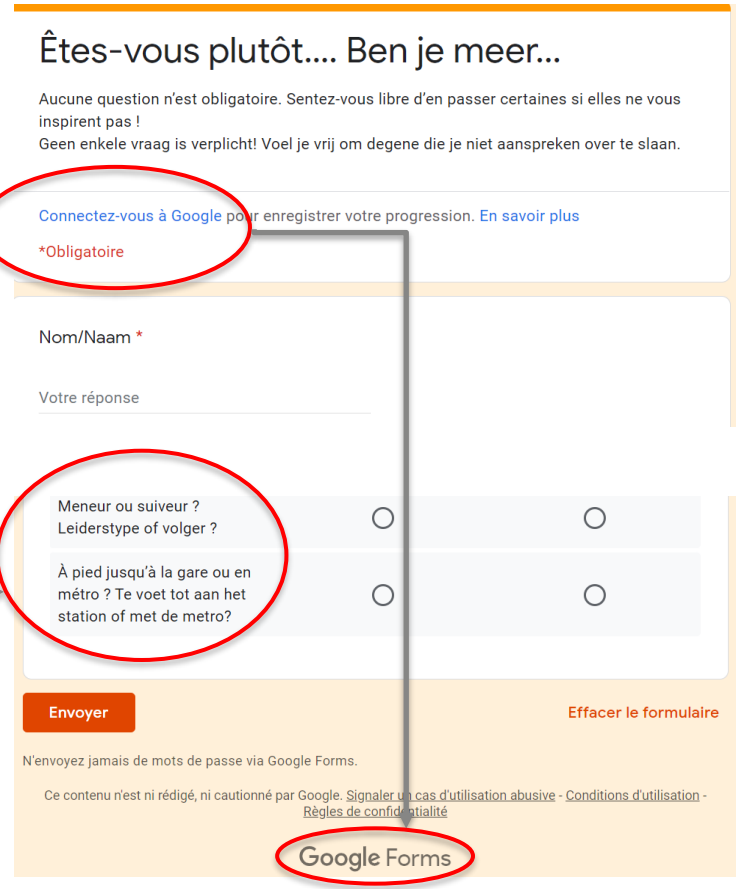
Voir **SCHREMS II** concernant l'utilisation de solutions transférant des données personnelles à des tiers extérieurs

DONNÉES BIOMÉTRIQUES

et

PROFILAGE

considérés comme données sensibles par le RGPD



Principe de TRANSPARENCE:
Pourquoi, licéité, qui pourra consulter, droits, contacts, … ?
→ référer à une (mini-)notice de confidentialité

CONSENTEMENT à traiter ces données

SPP Intégration sociale, Lutte contre la Pauvreté, Economie sociale et Politique des Grandes Villes

Centre administratif Botanique
Finance Tower
Boulevard du Jardin Botanique 50 boîte 165
1000 Bruxelles

POD MAATSCHAPPELIJKE INTEGRATIE
BETER SAMEN LEVEN
SPP INTÉGRATION SOCIALE
MIEUX VIVRE ENSEMBLE

Contactez-nous

lundi au vendredi de 8h30 à 12h30 et de 13h à 16h30 (vendredi jusque 16h) via

+32 2 508 85 86 ou… +32 508 8430
question@mi-is.be mi.dpo@mi-is.be
www.mi-is.be

Suivez-nous

Questions – Échanges de Points de Vue