Rapport – attestation de mise en conformité au RGPD

Société Pass-online.net SCRL
Avenue Albert Einstein 11/A
1348 Ottignies-Louvain-La-Neuve
TVA BE 0859.901.337

OBJET			
CLIENT	DPA		
PRESTATION	Rapport de mise en conformité		
VERSION	2	MODIFICATION	1
DATE	2019 01 14	AUTEUR:	SP
AUTEUR	Me Parsa Saba	DATE	2019 01 09

TABLE DES MATIERES

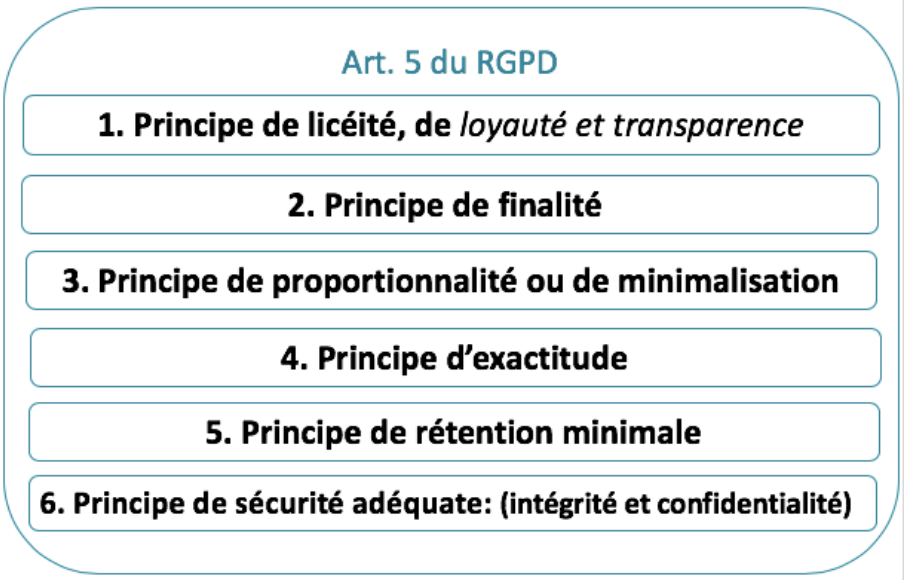
INTRODUCTION

Cette évaluation suivie d'une certification est requise par la société pass-online.net, SCRL, établie avenue Albert Einstein 11/A, à 1348 Ottignies-Louvain-La-Neuve et enregistrée sous le numéro d'entreprise : 0859.901.337. (ci-après l'entreprise)

A. OBLIGATIONS ET PRINCIPES DU RGPD

L'évaluation de la mise en conformité nécessite une analyse complète de l'application dans l'entreprise des principes généraux et des obligations découlant du RGPD.

Les principes généraux du RGPD sont énoncés à l'article 5§1 :



En son article 5§2 le législateur européen énonce le principe d'« accountability », ou la responsabilité comptable ou proactive en ce qu'il énonce ce qui suit :

> « Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté (responsabilité). »

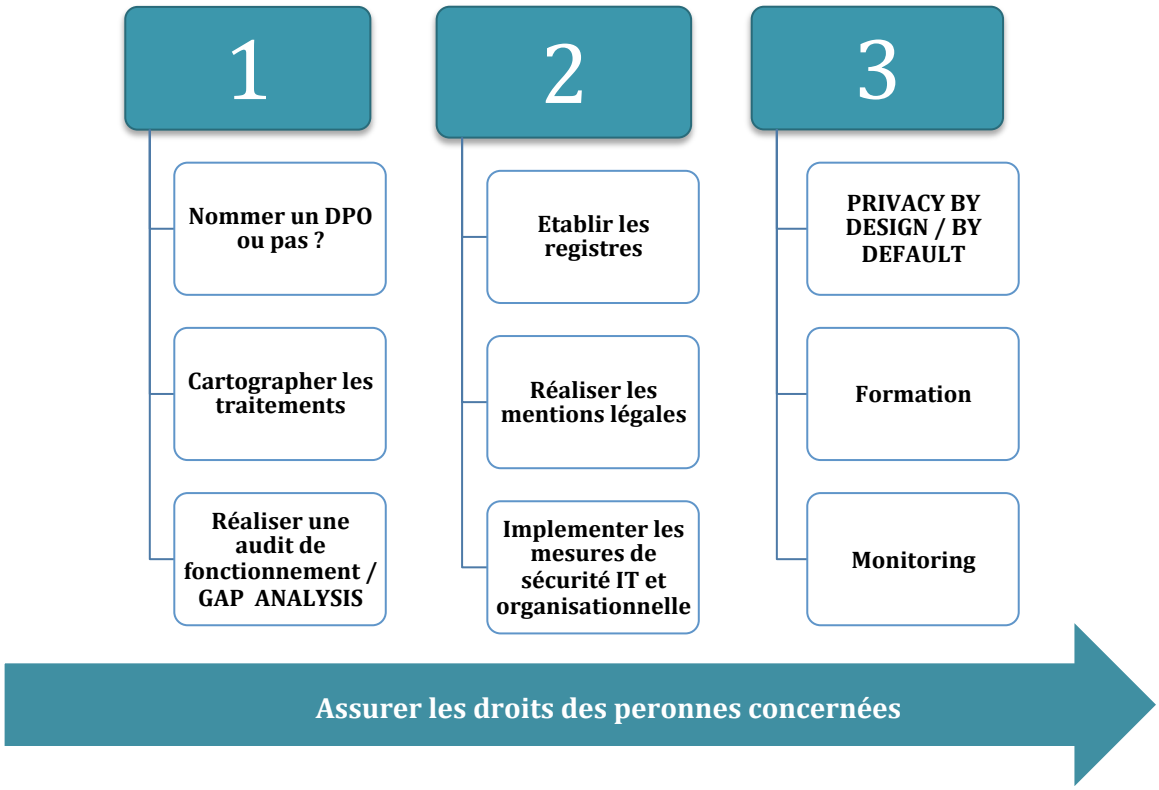
Il s'ensuit la première obligation découlant du RGPD, à savoir, la capacité du responsable du traitement de prouver à tout moment sa mise en conformité.

Pour y parvenir les obligations découlant du RGPD sont notamment les suivantes :

1. La nécessité de désigner un DPO.
2. La gestion des risques par la réalisation d'analyse d'impact, la prise de mesures de sécurité organisationnelles et de mesures de sécurité techniques
3. La tenue de registres en qualité de sous-traitant et de responsable de traitement :
    a. Des traitements
    b. Des violations des bases de données

4. La réalisation des droits des personnes concernées
5. Gestion des sous-traitants et des coresponsables des traitements
6. Gestion des traitements effectués pour compte de tiers
7. Formations

Dans la pratique, nous conseillons le schéma opérationnel suivant :



Il y a aussi lieu de souligner qu'il n'existe pas de modèle de mise en conformité unique.

La mise en conformité est un processus dynamique et personnel à chaque personne physique ou morale. Il induit une mise à jour et un monitoring constant. Ainsi une mise en conformité constatée à un instant « t », peut ne plus être valide à un instant « t' » si par exemple, des changements apparaissent dans les modalités d'exécution du traitement et qu'ils ne sont pas audités et/ou mentionnés, ou encore si l'état de l'art et les évolutions technologiques ne sont pas pris en considération de sorte que les mesures en place sont clairement obsolètes pour assurer un niveau de sécurité adéquat.

Enfin, ce rapport est réalisé sur une base déclarative et suivant les documents transmis par le demandeur et l'examen de son site web.

B. BASE LEGALE

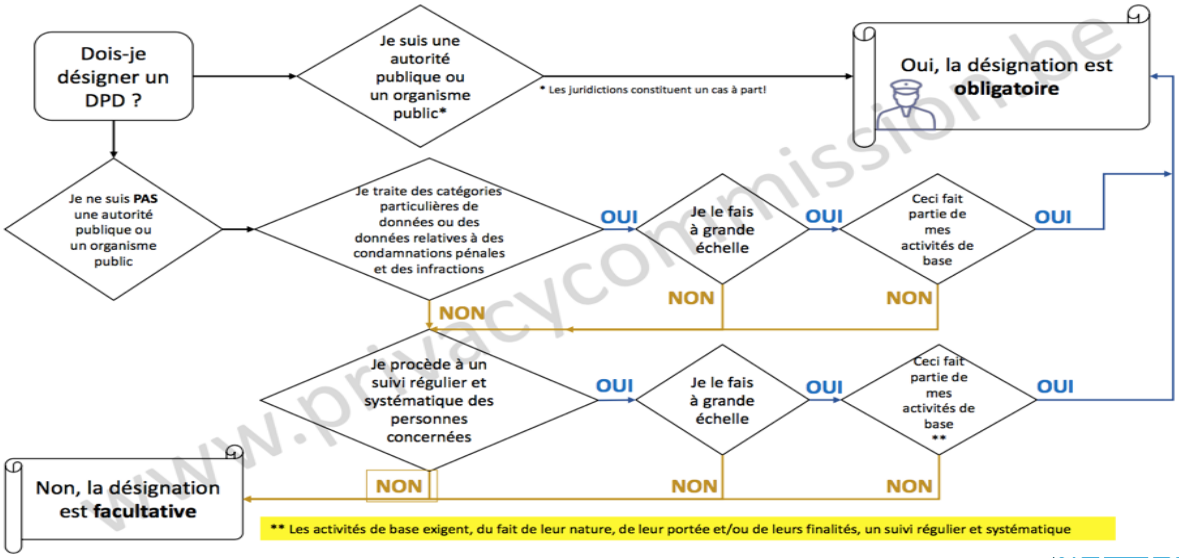
Ce rapport porte sur l'analyse de 9 points de conformités ainsi que les fondements légaux suivants :

Points de contrôle	Bases légales dans le RGPD, notamment :	Remarques
1. La nécessité de désigner un DPO ou pas	Articles 5, 37, 38, 39 et leurs considérants	
1. Les audits : **a. Cartographie** **b. Gap analisys**	Article 5, 6, 9, 10 et leurs considérants	
2. La gestion des risques : **a. Mesures de sécurité organisationnelles** **b. Mesures de sécurité techniques** **c. DPIA**	Article 5, 9, 24, 32, 35, 39 et leurs considérants	
3. Implémentation des mesures **a. Registre des traitements** **b. Documents légaux**	Articles : 5, 13 et 14, 24, 30 et leurs considérants	
4. Procédures quant aux droits des personnes concernées	Article 11 à 22 et leurs considérants	
5. Procédure en cas de violation des données :	Article : 28, 33 et leurs considérants	
6. Gestion des sous-traitants et des coresponsables des traitements	Article 26 et 28 et leurs considérants	
7. Gestion des traitements effectués pour compte de tiers	Article 28 et 30 et leurs considérants	
8. Formation	Article 38 et leurs considérants	

1. Designer un Delegue a la Protection des donnees (ci-apres DPO)

Après avoir analysé la situation particulière de la société au regard des dispositions de l'article 37 du RGPD et suivant le schéma de raisonnement de l'Autorité belge de protection des données (ci-après l'APD) nous arrivons à la conclusion que tant la qualité que les activités de l'entreprise ne rentrent pas dans le champ d'application de cet article, tel que l'énonce le législateur européen :

> « 1. Le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle ;
>
> 2. les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ; ou
> 3. les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 du RGPD et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 du RGPD. »



Il s'ensuit qu'il n'y a pas d'obligation de désignation d'un DPO.

En effet, la société n'est pas une autorité publique. En outre, il ne relève pas de son activité de base ni pour elle, ni pour compte de tiers de traiter des données de catégories particulières ou relatives à des condamnations pénales et des infractions (dites aussi données sensibles).

Enfin, elle ne procède pas à un suivi régulier et systématique des personnes concernées à grande échelle.

Dès lors elle n'est pas tenue de désigner un DPO, elle peut à son choix y procéder.

2. AUDITER : GAP ANALYSIS ET CARTOGRAPHIE

Cette étape permet de recenser toutes les données et d'avoir une vision d'ensemble en répondant au 5 Q, à savoir :

« Où, d'où et vers où… Pourquoi… Comment…Par qui…Combien de temps…

….nos données sont traitées ? »

Cette étape, qui n'est pas obligatoire, permet d'identifier les activités principales de l'entreprise, nécessitant le traitement de données, telles que le recrutement, la gestion de la paye, la formation, la gestion des accès, les statistiques, la gestion des clients prospects, la newsletter, …etc.

Cette étape facilite la constitution du registre et interroge sur les données dont l'entreprise a réellement besoin.

C'est aussi l'occasion d'améliorer les pratiques de l'entreprise afin de minimiser les traitements, conformément à l'article 5 du RGPD.

Elle aboutit à :

1 – Un cadastre des traitements, permettant la réalisation du registre des traitements

2 – L'élaboration d'un listing de tâches visant à se conformer au Règlement telles l'élimination de données inutiles, la redéfinition des pouvoirs d'accès aux données par les membres de l'entreprise, création d'automatisme d'effacement ou d'archivage au bout d'une certaine durée des données traitées.

En l'espèce la société a procédé à son audit avec l'outil SMART-GDPR.

L'outil automatise les dispositions du RGPD et procède à un audit avec une large granularité qui se caractérise par plusieurs questionnaires et plus de 1400 questions.

L'entreprise a réalisé, avec l'outil, l'audit du fonctionnement de son activité principale à savoir la création de quizz par son site internet : http://optinplus.eu/quiz , en atteste le rapport d'audit qu'elle a fourni en vue de la réalisation de ce rapport.

Au regard de son activité, il lui avait été conseillé de procéder à l'audit de son traitement RH et de son traitement gestion comptable en vue d'achever son registre de traitement. Elle a réalisé une audit simplifié pour ces deux traitements.

Cette étape n'est pas obligatoire, néanmoins cette dernière est tenue de reprendre dans son registre des traitements l'ensemble des traitements auxquels elle procède.

3. GESTION DES RISQUES ET PRIORISER LES ACTIONS

A la suite de son audit un plan d'action a été recommandé à la société avec plus près de 30 tâches à réaliser en vue d'assurer sa mise en conformité.

L'entreprise annonce avoir procédé aux modifications requises.

Nous rappelons que les données traitées ne sont pas sensibles.

Les données traitées sont les suivantes :

- Données d'identifications : état-civil, identité (nom, prénom), données d'identification (username/password)
- Données de connexion (adresses IP)

A ce stade les mesures suivantes assurent la sécurité adéquate de ces données :

A. MESURES DE SECURITE ORGANISATIONNELLES

L'entreprise prend, notamment, les mesures de sécurité organisationnelles suivantes :

1. Une politique ou des directives internes concernant la confidentialité de données à caractère personnel est mise en place ;
2. Contrôle des accès physique et absence des accès à distance ;
3. L'accès aux matériels sensibles (serveurs, unités de stockage, ordinateurs, etc.) ou de grandes valeurs est protégé ;
4. (A compléter …)

B. DUREE DE CONSERVATION DES DONNEES COLLECTEES

Suivant l'audit des mesures de limitation de la conservation des données ont été mises en place.

L'entreprise a recensé l'ensemble des types de données personnelles utilisées et pour chacune d'entre elle a défini une durée de conservation : limitée dans le temps et en adéquation avec la finalité du traitement et justifiée.

Elle a adopté des mécanismes permettant de vérifier que le traitement est en mesure de détecter la fin de durée de conservation des données et intégrer un processus de suppression des données automatisé ou non une fois leur date de fin de conservation atteinte.

C. MESURES DE SECURITE TECHNIQUES

L'entreprise a réalisé

1. Anonymisation dès cela est possible,
2. Un chiffrement des données documenté via 3 canaux d'encryptage : 1) les disques durs entiers, 2) les bases de données entières et 3 les canaux de communication (https, vpn, etc.).
3. Cryptage matériel SED (Self Encrypted Drive)
4. Hachage des données concernées pour comparaison
5. Control des accès informatiques
    a. une gestion des profils qui sépare les accès selon les tâches et les domaines de responsabilité
    b. une limitation des accès aux données personnelles aux seuls utilisateurs habilités ?

c. une application des principes du moindre privilège avec dont les comptes d'utilisateurs disposant de privilèges élevés sont limités aux seules opérations qui le nécessitent, avec une revue annuelle

6. Gestion des mots de passe.

D. DPIA :

Eu égard à la qualité des données et aux modalités de traitement, aucun DPIA n'est obligatoire.

A ce stade rien ne laisse supposer que l'entreprise a procédé à un DPIA.

L'outil Smart-GDPR le permet.

4. IMPLEMENTATION DES MESURES

A. REGISTRE DES TRAITEMENTS

Conformément à l'article 30 § 1 du RGDP la société tient son registre, par le biais de l'outils Smart-GDPR.

« Chaque responsable du traitement et, le cas échéant, le représentant du responsable du traitement tiennent un registre des activités de traitement effectuées sous leur responsabilité.
Ce registre comporte toutes les informations suivantes:
a) **le nom et les coordonnées du responsable du traitement** et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données;
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, y compris les destinataires dans des pays tiers ou des organisations internationales;
e) **le cas échéant, les transferts de données à caractère personnel** vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa, les documents attestant de l'existence de garanties appropriées;
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** visées à l'article 32, paragraphe 1.»

Seule une entrée est à ce jour disponible sur le registre à savoir : « http://optinplus.eu/quiz »

1. **Finalité** : la gestion des données en vue de la réalisation de l'activité de la société la réalisation de quizz, via le site internet de l'entreprise.
2. **Base de licéité :** intérêt légitime de la société et le consentement
3. **Les mesures de sécurité sont énoncées en amont**
4. **Les mesures et délais pour l'effacement** sont décrits ci-dessus.
5. **Les traitements sur les données sont les suivantes**
    i. Collecte

ii. Envoie d'email
iii. Archivage
iv. Destruction

6. **Remarques suivant l'audit légal du site :**
   a. Charte de confidentialité ou politique de confidentialité du site Internet a été complétée.
   b. S'agissant des l'utilisation de cookies fonctionnels aucun consentement n'est requis en amont. S'agissant des autres cookies analytiques, publicitaire et tiers les mentions doivent être acceptés avant la pose du cookie.[1]
   Le RGPD impose le consentement préalable manifestant la volonté, libre, spécifique, éclairée et univoque de l'internaute.
   En toutes circonstances, une possibilité d'« opt-out » doit-être offerte à l'utilisateur.

B. RESTE A REALISER

1. Les annexes aux registres manquantes à ce stade sont
   a. Convention de sous-traitance ou de coresponsabilité

5. PROCEDURES QUANT AUX DROITS DES PERSONNES CONCERNEES

Suivant l'audit les défaillances relatives à la garantie des droits des personnes concernées ont été soulignées, notamment en matière du droit d'information des personnes concernées.
La société a recensé les méthodes utilisées pour informer les personnes sur son traitement lors du processus de collecte et s'est assurés que l'information est réalisée de manière complète, claire et adaptée au public visé, en fonction de la nature des données et des moyens pratiques choisis.
Conformément aux exigences des articles 13 et 14 du RGPD.
S'agissant des autres droits, la société a mis en place des mécanismes lui permettant facilement l'identification de la personne souhaitant exercer leurs droits, par un formulaire électronique, par courrier électronique et par accès à un compte en ligne.
Aucun coût n'est prévu pour l'exercice d'un droit des personnes.
A ce jour sont mis en place des procédures relatives aux droits suivant sont en place :

1. Droit à l'information relative aux traitements ;
2. Droit d'accès ;
3. Droit de rectification ;
4. Droit à l'effacement ;
5. Droit de s'opposer au traitement
6. Droit à la limitation du traitement ;
7. Droit à la portabilité ;
8. Droit de ne pas faire l'objet d'une décision purement automatisée ;

Un registre des demandes est tenu via l'outil Smart-GDPR

6. PROCEDURE EN CAS DE VIOLATION DES DONNEES

A. CELLULE DE VOLS ET PERTES DE DONNEES.

[1] Conformément aux dispositions de l'article 4, 11° du RGPD un consentement le consentement s'entend de « toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement ; »

Eu égard à la taille de l'entreprise, aucune cellule n'est à ce jour en place ni même nécessaire.
En cas de violation, le gérant est informé de ses obligations et se tient à la disposition des personnes concernées, en atteste son site web.

B. REGISTRE DES VIOLATIONS

Un registre des violations est tenu via l'outil Smart-GDPR

7. GESTION DES SOUS-TRAITANTS ET DES CORESPONSABLES DES TRAITEMENTS

En son article 28 le RGPD exige que :

« 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.
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.
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: »

En outre l'article 29 énonce ce qui suit :

> « Lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement. Les responsables conjoints du traitement définissent de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences du présent règlement, notamment en ce qui concerne l'exercice des droits de la personne concernée, et leurs obligations respectives quant à la communication des informations visées aux articles 13 et 14, par voie d'accord entre eux, sauf si, et dans la mesure, où leurs obligations respectives sont définies par le droit de l'Union ou par le droit de l'État membre auquel les responsables du traitement sont soumis. Un point de contact pour les personnes concernées peut être désigné dans l'accord. »

Il s'ensuit que les acteurs traitant les données sont tenus de régler leurs rapports par des conventions garantissant leur mise en conformité.
Nous manquons d'informations à cet égard.

8. GESTION DES TRAITEMENTS EFFECTUES POUR COMPTE DE TIERS

L'article 30 §2 du RGPD énonce ce qui suit :

« 2. Chaque sous-traitant et, le cas échéant, le représentant du sous-traitant tiennent un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement, comprenant :
a) le nom et les coordonnées du ou des sous-traitants et de chaque responsable du traitement pour le compte duquel le sous-traitant agit ainsi que, le cas échéant, les noms et les coordonnées du représentant du responsable du traitement ou du sous-traitant et celles du délégué à la protection des données;
b) les catégories de traitements effectués pour le compte de chaque responsable du traitement;
c) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa, les documents attestant de l'existence de garanties appropriées;
d) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, paragraphe 1. »

La société est tenue de réaliser un registre de sous-traitant lorsqu'elle agit en cette qualité.
La société est outillée pour tenir ses registres tant en qualité de sous-traitant que de responsable de traitements.
L'outil Smart-GDPR permet la tenue simultanée des registres en deux qualités, tant en qualité de sous-traitant que de responsable du traitement.

9. FORMATIONS

A ce stade aucune information utile n'a été transmise, mais cela ne remet pas en doute la mise en conformité de la société, dès lors que le gérant témoigne d'un intérêt à la matière, une connaissance de ses traitements et des mesures utiles et nécessaires à assurer la sécurité adéquate de ces données.

CONCLUSION :

L'entreprise est en cours de mise en conformité. Elle assure à ce stade ses obligations découlant du RGPD.

Elle a :

1- Évalué son besoin de DPO
2- Audité son fonctionnement
3- Réalisé son registre
4- Réalisé ses mentions légales
    a. Elle doit vérifier
        i. Les contrats avec ses sous-traitants et coresponsable
        ii. Les mentions légales dans le cadre de sa relation de travail avec ses employées.
5- Il lui revient à l'avenir de continuer à monitorer son système.

Ces modifications sont en cours, son niveau de maturité au RGPD est excellent. Sa conformité est assuré ou en très bonne voie.

Elle doit monitorer son fonctionnement, pour continuer à assurer sa conformité.

ATTESTATION DE CONTROLE

Par la présente, je soussigne Parsa Saba, avocate et DPO certifiée par l'Université de Maastricht (EDPC), avoir contrôlé les processus de la société pass-online.net, SCRL, établie avenue Albert Einstein 11/A, à 1348 Ottignies-Louvain-La-Neuve et enregistrée sous le numéro d'entreprise : 0859.901.337. (ci-après l'entreprise)

Cette attestation est réalisée sur base déclarative, et suivant l'examen de l'audit réalisé par l'entreprise avec l'outil SMART-GDPR.

J'assure par la présente que l'entreprise assure à ce stade, et tient la preuve des obligations suivantes découlant des dispositions du RGPD :

1- Évaluation de son besoin de DPO,
2- Audit de son fonctionnement,
3- Réalisation de son registre des traitements particulièrement quant à son outil http://optinplus.eu/quiz
4- Réalisation de ses mentions légales, notamment sa charte vie privée

A l'avenir et sans remettre en cause sa conformité actuel au RGPD, il lui revient de :

1. Continuer à monitorer son système et assurer l'avenir les principes de « privacy by design », « privacy by default » ;
2. Former et informer son équipe.

Parsa Saba

Avocate – Lawyer
DPD certifiée – DPO certified

Cabinet d'avocat
ALTALAW – (dép.) GDPR ADVISOR