Confidentiel

LED (Lien Entreprises Durables)

« *Conformité RGPD* » V1.0

Juillet-août 2019

| Émetteur(s) :

Christophe NOUHAU – gaellebeaune@posteo.net / christophe.nouhau@proximit.fr

1. Une première réunion a eu lieu le 28/03/2019

Présents : Gaëlle Beaune – Dominique Moreau – Christophe Nouhau

1.1. Etape 1 : Désigner un pilote

⇨ Désigner le responsable des traitements = personne morale (Président de l'association)

Avantage de ne pas être nominatif = rien à changer si changement de président

⇨ Désigner un pilote/référent RGPD = interne (quelqu'un du bureau qui connait un peu RGPD) + éventuellement support externe pour questions ponctuelles

1.2. Etape 2 : Cartographier

⇨ 2.1 - Recenser les différents traitements (comptabilité, évaluations croisées, documents transmis lors de l'adhésion, listes de mails… A lister notamment en partant des informations disponibles chez chaque membre du bureau-Copil)

Documents à produire : Registre des activités de traitement

⇨ Pour chaque traitement de données, se poser les questions Qui, Quoi, Pourquoi, Où, Jusqu'à quand, Comment, et mesures de sécurité

Documents à produire : Fiche de traitement pour chaque activité

1.3. Etape 3 & 4 : Prioriser et gérer les risques

⇨ Identifier les actions à mener en fonction de ce qui ressort des fiches de registre (risques identifiés)

Exemples :

Mails : Utiliser l'adresse mail "distribution@lien-entreprises-durables.fr" pour l'envoi de mail à tous, et créer une liste de diffusion pour le Copil, afin de masquer les adresses mail

Site : Mettre à jour les Mentions Légales en faisant référence au RGPD + créer un document annexe "Politique de confidentialité" + mettre à disposition un moyen de déposer une demande/une modification de mes données (possibilité de créer un mail "rgpd@lien-entreprises-durables.fr")

1.4. Etape 5 : Organiser les processus internes

⇨ Récapituler les vulnérabilités, puis décrire les choses que l'on organise pour les limiter et ce que l'on ferait si un souci se présentait (ex : déclaration CNIL en cas de souci)

Documents à produire : Procédures éventuelles

1.5. Etape 6 : Documenter

- ⇨ Garder les preuves (ex : preuve de sensibilisation du bureau au RGPD, preuve de la réalisation d'un GT RGPD et du lancement d'une démarche de mise en conformité, …)

2. Description des données à caractère personnel manipulées par le LED

Présents : Philippe Mazière – Christophe Nouhau – 19 juillet 2019

Le groupe de travail a déterminé qu'il y avait des données personnelles dans les traitements suivants :

- ⇨ Gestion des échanges avec les membres notamment par messagerie
- ⇨ Gestion des échanges avec la banque
- ⇨ Gestion des adhérents / partenaires via documents numériques listes, gestion des cotisations, statuts de l'association, planning sur CR, gestion Copil, gestion Coplein)
- ⇨ Stockage de certaines informations sur Dropbox
- ⇨ Gestion du site web avec partie privée et publique

3. Et après ?

Points de conformité		**Principe, constat et actions à mettre en place par le LED**
Accountability et registre des activités de traitement (articles 5, 24 et 30 du RGPD)	►	Principe : Afin d'assurer une protection optimale des données personnelles qu'ils traitent de manière continue, les responsables de traitements et les sous-traitants doivent mettre en place des mesures de protection des données appropriées et démontrer cette conformité à tout moment (*accountability*). Parmi ces mesures, le responsable de traitement doit tenir un registre des activités de traitement.
	►	Constat : Bien que certaines bonnes pratiques existent d'ores et déjà au sein de l'association, le LED ne dispose pas à ce jour de documentation relative à la conformité à la règlementation applicable en matière de protection des données (absence de déclarations CNIL, absence de procédure spécifique en matière d'archivage et de suppression des données personnelles pour les données conservées sur les outils informatiques, absence de certaines mentions d'information, etc.).
	►	Actions à mettre en place :

	1.	Rédiger et mettre en œuvre des politiques en matière de protection des données personnelles (voir ci-dessous les préconisations pour chaque point de conformité).
	2.	Créer et compléter un registre des activités de traitement et le mettre régulièrement à jour. Ce registre comporte toutes les informations suivantes : • Le nom et les coordonnées du responsable du traitement (LED) Les finalités du traitement (à effectuer à la prochaine réunion); o La description des catégories de personnes concernées et des catégories de données à caractère personnel ; o Les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, o Dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données ; o Dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles.
	3.	Formaliser une politique interne de protection des données personnelles rappelant les règles applicables (« check-list RGPD »).
	4.	Développer un support de sensibilisation sur les principes du RGPD décrits dans la politique interne et sur la tenue du registre.

Points de conformité		**Principe, constat et actions à mettre en place par le LED**
	►	Principe de licéité: Chaque traitement de données à caractère personnel doit être fondé sur l'intérêt légitime de l'entreprise, le consentement de la personne, l'exécution d'un contrat, ou une obligation légale.
	►	Constat : Les traitements de données personnelles mis en œuvre par le LED sont licites dans la mesure où ils résultent pour la plupart de l'exécution d'un consentement d'adhésion (contrat avec adhérents du LED). Le LED devra simplement prévoir d'intégrer la base juridique de chaque traitement dans chaque mention d'information destinée aux personnes concernées.
	►	Action à mettre en place :
	1.	Prévoir de faire apparaitre les fondements juridiques des traitements (exécution d'un contrat, intérêt légitime, consentement, obligation légale) dans les mentions d'information destinées aux personnes concernées Par exemple avec la notion de signature du

Points de conformité		**Principe, constat et actions à mettre en place par le LED**
		consentement de l'adhérent lors de son adhésion
Principe de minimisation (article 5 du RGPD)	►	Principe de minimisation des données : Les données doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.
	►	Constat : Le LED ne traite pas de données personnelles de manière disproportionnée.
	►	Action à mettre en place :
	1.	Mettre en place un processus permettant d'effectuer une revue régulière des données afin de déterminer si elles sont encore pertinentes ou devenues obsolètes.
	2.	Limiter l'accès aux données personnelles
	3.	Archiver et/ou supprimer les données personnelles qui ne sont plus nécessaires
Durée de conservation (article 5 du RGPD)	►	Principe de limitation de la conservation des données : Les données personnelles doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées. Une fois que la finalité a été atteinte, les données personnelles peuvent être archivées au titre du respect d'une obligation légale ou pendant la durée de prescription légale applicable. Lorsque les données sont archivées, elles doivent être conservées sur un support informatique distinct et à accès très limité. Il convient de prévoir à cet effet une base de données d'archives dédiée ou une séparation logique dans la base de données active, après avoir opéré un tri des données pertinentes à archiver. Lorsque la durée correspondant au respect de l'obligation légale ou la durée de prescription

Information des personnes (article 13 du RGPD)		Tous : Site internet (mentions légales / règles de confidentialité) Salarié : site internet + charte + document à signer Adhérent : contrat Salariés des adhérents : site (y faire référence) + document lors de la visite ?