RGPD ou GDRP

Règlement Général de Protection des Données ou General Data Regulation Protection

Règlement applicable à partir du 25 mai 2018

« obligatoire dans tous ses éléments et directement applicable dans tout État membre »
sous l'égide de la CNIL en France

PARTICULIERS : se protéger, protéger ses contacts
L'ordinateur :

- disposer d'un antivirus antimalware à jour (mises à jour automatiques recommandées)
- disposer d'une alerte en cas d'installation d'un nouveau logiciel, vérifier son origine
- faire régulièrement (automatiquement ou semi) les mises à jour du Système d'Exploitation, des logiciels notamment les navigateurs et les logiciels de messagerie
- nettoyer quotidiennement son ordinateur avant de l'éteindre (ou à chaque démarrage) à l'aide de logiciels tels que CCleaner et/ou Spybot (existent en version gratuite)
- éviter de laisser traîner ses identifiants n'importe où, n'importe quand, accessible à n'importe qui
- disposer d'identifiants différents pour chaque connexion nécessitant une identification
- user éventuellement de pseudos
- choisir un mot de passe pour chacun de ces identifiants.
- Le mot de passe doit être robuste pouvant aller jusqu'à 24 caractères alphanumériques et spéciaux : une phrase facile à retenir (pour son propriétaire) avec chiffres et caractères spéciaux est actuellement recommandée ainsi que d'en changer régulièrement.
- La liste des contacts doit être protégée éventuellement par cryptage du fichier, en ne la laissant pas accessible à n'importe qui, n'importe où, n'importe quand

D'autres précautions sont recommandées telles que de se déconnecter quand la connexion n'est pas nécessaire, préférer une connexion filaire à une connexion Wifi
et désormais plus que jamais : bien lire les contrats à signer pour bénéficier d'un service notamment d'un cloud (suivre l'évolution de COZY CLOUD de la même veine que Mozilla, qui respecte de façon native le RGPD).

Les logiciels
Le logiciel de messagerie : pour la sécurité des données personnelles, Mozilla Thunderbird est recommandé

- Protéger vos données personnelles, c'est « en même temps » protéger celles de vos contacts
- chaque compte de messagerie recueillant les messages sur une adresse donnée, doit être correctement paramétré notamment les POP3 et SMTP qui doivent être en SSL/TLS afin de créer un tunnel d'où ne peuvent sortir les informations qui y transitent
- Il est préférable de placer en copie cachée les adresses d'un message envoyé en nombre (exemple dans le cadre associatif) ou de créer un groupe, de toujours y ajouter la possibilité de demander la suppression de la liste des contacts
- S'il s'agit d'un envoi en nombre auprès, par exemple, de contacts associatifs, il peut être opportun de demander à chacun, en fin de message, si elle/il est d'accord pour faire partie de ce groupe et de lui donner les moyens de l'exprimer afin de ne plus y figurer.
- le webmail (consultation de ses messages en ligne) : voir Le logiciel de navigation (le navigateur)

Le/les navigateurs :

- pour sa sécurité, Mozilla Firefox est recommandé, mais il est vrai que c'est l'IP (de votre ordinateur, de votre connexion Internet) qui permet de vous identifier et de vous suivre instantanément et sans conteste, ainsi une confidentialité renforcée sera obtenue en utilisant Mozilla Tor qui dérive

votre connexion à travers un réseau mondial, jamais avec la même IP ce qui présente quelques inconvénients de langue, de démarche, parfois de mise en page.

- Il est cependant possible de se protéger du « tracking » en vue du « profiling » et donc du vol de miettes de votre identité reconstituables (vos données personnelles et de connexion) en ajoutant des modules ou extensions à votre navigateur Mozilla Firefox, sans trop perdre les avantages de l'Internet. Dont voici un exemple d'assemblage expérimenté – mais attention : avec ces seuls modules – tous « gratuits » avec dons bienvenus :
- paramétrer le navigateur pour toujours naviguer « en privé », ne jamais accepter de cookies tiers, effacer l'historique de navigation et mieux encore ne jamais conserver d'identifiants webmail ou autre
- prendre en compte le badge de sécurité donnant des informations sur le niveau de sécurité du site que vous visitez (https://)
- Ghostery + canvas blocker + https evrywhere + privacy badger + JS on off + Am'I unique ? Ce dernier pour savoir ce que l'on sait de vous par votre navigation!
- Pour connaître tous les dangers pour vos données personnelles (cookies, fingerprinting ...), rendez-vous sur le site de la CNIL cnil.fr et surtout pour connaître vos nouveaux droits

https://www.cnil.fr/fr/comprendre-vos-droits

le droit d'accès, le droit de rectification, le droit d'opposition, le droit de déréférencement, Le droit d'accès aux fichiers de police, de gendarmerie, de renseignement, FICOBA, plus de droits pour vos données : des données à emporter, plus de transparence, protection des mineurs, guichet unique, sanctions renforcées, consécration du droit à l'oubli

ASSOCIATIONS

Les associations comme toute organisation publique ou privée sont soumises à de nouvelles obligations destinées à protéger les données personnelles dont elles disposent dans le cadre de leurs activités
Ces nouvelles obligations, dont la désignation d'un responsable de la protection des données capable de répondre aux questions de la CNIL en cas de contrôle. Ce responsable doit pouvoir dire quelles mesures sont prises pour la protection des données personnelles, à quels traitements ces données sont soumises, si ces traitements sont adaptés aux nécessités de l'association.

Traitement(s) des données personnelles

Toute opération, ou ensemble d'opérations, portant sur de telles données, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement ou interconnexion, verrouillage, effacement ou destruction, ...)

https://www.cnil.fr/fr/definition/traitement-de-donnees-caractere-personnel

notons que tout ce qui a été dit pour les particuliers est valable pour les associations
Le fichier des adhérents, son usage et son utilisation, sa protection contre les fuites, sa mise à jour en validant les informations, y compris en supprimant les personnes qui ne sont plus adhérentes ou membres, en vérifiant régulièrement que tous les contacts par messagerie souhaitent toujours y figurer. L'exprimer clairement dans un document contractuel de synthèse.
Pour ce qui concerne le site web et les services en ligne des associations gérés par Generlab, dès sa conception qui utilise SPIP (Système de Publication pour un Internet Partagé), la protection des données personnelles y est assurée. Certains sites disposent depuis peu d'un analyseur de trafic recommandé par la CNIL (PIWIK MATAMO) dont le paramétrage permet de rendre les IP non identifiables individuellement et de les masquer au bout d'un certain temps.