Recommandations techniques relatives au respect du Règlement Général sur la Protection des données.

Application des principes de « Privacy by Design » et « Privacy by Default ».

Version 1.0 – 09/11/2018

Le Règlement Général sur la Protection des Données personnelles (RGPD) est entré en application le 25 mai 2018.

Les clauses RGPD, annexées à l'acte d'engagement de l'appel d'offre, déclinent le cadre juridique général en décrivant les responsabilités du responsable de traitement et de ses sous-traitants (au sens large du terme).

Ce document énumère de manière non exhaustive, les recommandations techniques proposées par l'Eurométropole pour remplir les obligations de sécurité nécessaires à la protection des données personnelles.

Ces recommandations techniques devraient être prises en compte systématiquement lorsque l'application réalise des traitements sur des données personnelles. Leur mise en application participe à la conformité des traitements au RGPD notamment sur les aspects des principes de « Privacy by Design » et « Privacy by Default ». Ces deux principes correspondent à l'intégration de la sécurité des données personnelles dès la conception des produits et par défaut.

Les recommandations de ce document portent sur les aspects suivants :

1. DISPOSITIONS GÉNÉRALES DE RESPECT DU RGPD

RGPD-GEN-1 : une application Web doit comporter un espace paramétrable permettant d'indiquer aux personnes concernées par le traitement les mentions d'information obligatoires relatives à la protection des données personnelles. C'est notamment le cas pour les applications destinées à être mise en ligne sur Internet (Saas ou internalisées).

RGPD-GEN-2 : une application Web, destinée à enregistrer des données personnelles d'internautes (citoyen, visiteur, etc.) via un formulaire de l'application, doit comporter un mécanisme permettant de recueillir le consentement de la personne concernée et de conserver la trace de ce consentement. La trace de ce consentement doit être purgée ou « anonymisée » simultanément à la purge ou l'anonymisation des dernières données personnelles stockées pour la personne concernée.

RGPD-GEN-3 : les données personnelles sensibles devraient être cryptées en base ou dans les fichiers dans lesquels elles sont stockées. Le fournisseur doit prévoir les mécanismes d'encryption adéquats par rapport à la sensibilité des données. A défaut, il s'engage à ce que son application supporte des mécanismes d'encryption « externes » à son application (mécanismes d'encryption de la base de données par exemple).

RGPD-GEN-4 : la mise en place de mécanismes techniques permettant d'aider à détecter des violations de données potentielles ou avérées et d'en identifier la nature est recommandée. Cela devrait notamment être le cas lorsque l'application stocke des données sensibles (données de santé, etc.).

2. LA GESTION DES ACCES AUX APPLICATIONS

RGPD-ACC-1 : l'accès d'un utilisateur à une application doit obligatoirement faire l'objet d'une procédure d'authentification.

RGPD-ACC-2 : le paramétrage de l'application doit interdire toute forme d'accès à des interfaces d'administration ou des pages de test pour un utilisateur standard.

RGPD-ACC-3: lorsque l'authentification n'a pas lieu en local sur le serveur ou via le réseau local de l'Eurométropole de Strasbourg (AD, LDAP, base de données), un contrôle de l'identité du serveur doit être réalisé (en utilisant des Certificats numériques d'identité serveur par exemple).

RGPD-ACC-4: les formulaires accessibles via un accès peuvent être utilement pourvus d'un mécanisme de « Captcha » pour éviter une attaque via un programme automatique (brute force

de page de connexion, etc.). Les formulaires dépourvus d'authentification (pages de contact, ou envoi à un ami, par exemple.) devraient l'être systématiquement.

RGPD-ACC-5 : l'application doit effectuer une vérification de l'identité de l'utilisateur pour chaque page accédée et ne pas laisser la possibilité à cet utilisateur de s'octroyer des droits non autorisés par son profil dans l'application (élévation de privilèges).

3. GESTION DES MOTS DE PASSE.

RGPD-MDP- 1 : le mot de passe d'un compte d'accès à une application doit respecter le format défini par la politique de sécurité de l'Eurométropole de Strasbourg (conforme aux recommandations CNIL) :

- 8 caractères,
- au minimum, 3 types de caractères différents,
- interdiction des mots de passe équivalents à l'identifiant ou à des parties du nom complet comptant plus de deux caractères successifs.

Idéalement, un mécanisme de renouvellement périodique devrait être proposé pour s'assurer que les mots de passes sont changés régulièrement. La périodicité doit dans ce cas être paramétrable.

RGPD-MDP-2: l'application doit fournir un moyen de blocage de l'accès en cas de tentatives infructueuses. Idéalement, le blocage doit faire l'objet d'une temporisation après plusieurs échecs, dont la durée augmente exponentiellement dans le temps (supérieure à 1 minute après 5 tentatives échouées) et permette au maximum 25 tentatives par 24 heures. A défaut un blocage complet doit être implémenté. Le nombre de tentatives doit être paramétrable.

RGPD-MDP-3: si les mots de passe sont gérés par l'application (dans une table de base de données par exemple), l'utilisateur devra disposer dans l'application d'une fonctionnalité de changement de son mot de passe. La page demandera l'ancien mot de passe, le nouveau mot de passe et sa confirmation pour que l'utilisateur puisse changer son mot de passe.

RGPD-MDP-4: les applications destinées à être accessibles via internet doivent obligatoirement fournir un mécanisme permettant d'effectuer une demande de renouvellement du mot de passe (mot de passe oublié ou demande d'un nouveau mot de passe en cas de blocage). L'utilisateur doit être redirigé vers une interface lui permettant de saisir son nouveau mot de passe via un lien dans un mail. La validité de la session de renouvellement ne doit pas dépasser 24h et ne pas permettre plus d'un renouvellement.

RGPD-MDP-5: les applications doivent fournir un mécanisme de renouvellement périodique de mot de passe automatisé et sécurisé dont la fréquence doit être paramétrable.

RGPD-MDP-6: l'Eurométropole de Strasbourg doit être en mesure de changer tous les mots de passe de l'application liés aux outils d'infrastructure et d'administration. Si nécessaire, une documentation décrivant la procédure à appliquer devra être fournie. L'application doit permettre le renouvellement de la totalité des mots de passe en cas de compromission ou de suspicion de compromission des accès et d'un mécanisme permettant d'avertir les utilisateurs concernés via un mail ou par un autre moyen simple à mettre en œuvre.

RGPD-MDP-7: l'utilisateur d'une application destinée à être accessible via internet doit être averti de tout changement de mot de passe de son compte d'accès. Cette alerte peut se faire par mail par exemple et en tout état de cause en se basant sur les données d'identification disponibles dans l'application.

RGPD-MDP-8: les applications doivent comporter un mécanisme obligeant l'utilisateur à changer son mot de passe à la première connexion.

RGPD-MDP-9: tout mot de passe qui serait stocké, soit dans des fichiers, soit dans une base de données, doit être crypté. Cela comprend par exemple, les mots de passe de comptes génériques (pool de connexion aux bases de données), les mots de passes applicatifs des utilisateurs, etc.

RGPD-MDP-10: tous les mots de passe par défaut doivent être modifiés lors de la mise en service d'une application, que ce soit en environnement de Test ou en environnement de Production. Une documentation doit être mise à disposition pour identifier tous les outils d'administration ou les éléments d'infrastructure permettant de faire fonctionner l'application (PHP, serveur Web, etc.) et disposant d'un accès avec mot de passe par défaut.

4. MÉCANISME DE PURGES DES DONNÉES.

RGPD-PUR-1: l'application doit comporter des traces de connexion et si possible des actions menées par les utilisateurs. Ces traces doivent bénéficier d'un utilitaire de purge ou d'anonymisation au même titre que les autres données personnelles.

RGPD-PUR-2: l'application doit comporter un utilitaire de purge des données personnelles ou un mécanisme d'anonymisation permettant à l'Eurométropole de Strasbourg de se mettre en conformité avec les indications portées dans le registre des traitements ou dans la demande d'autorisation. Dans l'idéal, le mécanisme peut être déclenché de manière automatique dans l'application. A défaut, le fournisseur développe des scripts permettant de le faire. En dernier recours, le fournisseur produit un document indiquant clairement les manipulations à réaliser pour effectuer les purges ou l'anonymisation des données.

5. MÉCANISMES D'ANONYMISATION DES DONNÉES

RGPD-ANO-1: l'application comporte des outils permettant d'anonymiser les données personnelles. Ces mécanismes permettent des échanges de données dans le cas de maintenances, par exemple, ou encore d'opérations d'évolutions, lorsque la donnée d'origine n'est pas nécessaire. A défaut, des mécanismes de pseudonymisation peuvent être proposés.

6. ECHANGES DE DONNEES APPLICATIVES ET TECHNIQUES

Dans certains cas, l'échange de données est nécessaire à la résolution de problèmes ou de bugs applicatifs et peuvent concerner des données à caractère personnel :

RGPD-ECH-1 : tout échange passant par des canaux réputés comme non fiables, comme internet, contenant des données à caractère personnel ou considérées comme confidentielles, doit s'effectuer via des moyens sécurisés. Il n'est, par exemple, pas autorisé d'utiliser un protocole de type FTP ou équivalent, si les données personnelles contenues dans des fichiers ne sont pas cryptées ou anonymisées. Les protocoles SFTP, FTPS ou des plateformes d'échanges pourront être utilisés, dont le stockage est maitrisé et obligatoirement localisé dans l'UE, (sauf dérogation du responsable de traitement suite à l'apport de garanties spécifiques) pourront être utilisées à cet effet.

RGPD-ECH-2 : l'utilisation de plateformes d'échanges, comme Dropbox ou autres plateformes du même type, n'est par défaut pas autorisée, sauf dérogation du responsable de traitement suite à l'apport de garanties spécifiques (données stockées dans l'UE ou pays avec des législations de protection de données adéquates, données cryptées sur la plateforme, etc.)

RGPD-ECH-3 : tout fichier, contenant des données à caractère personnel ou considérées comme confidentielles, destiné à être échangé sur des supports physiques (clé USB, disques USB, CD gravés, etc.), doit être crypté.

7. CONFIDENTIALITÉ ET INTÉGRITÉ DES DONNEES ET RESSOURCES

RGPD-CONF-1 : si l'application utilise les technologies Web, elle doit fonctionner avec le protocole HTTPS et être paramétrée par défaut en https lors de sa mise en œuvre.

RGPD-CONF-2 : sur l'environnement de production, le paramétrage doit masquer les messages d'erreur techniques de l'application, afin d'éviter de mettre en évidence des données ou des informations susceptibles d'être exploitées par une personne mal intentionnée. L'affichage des messages d'erreur technique sera réservé aux environnements de

développement et de test, en phase de mise au point. Sur l'environnement de production, le paramétrage doit masquer les entêtes délivrés par les éléments techniques (serveur Web, OS, etc.), notamment lorsque les applications sont mises en ligne sur Internet. Cette remarque s'entend aussi pour des applications de test ou de pré-production si ces environnements sont exposés sur Internet.

RGPD-CONF-3 : l'application ne doit pas stocker de données confidentielles ou sensibles dans un mécanisme de stockage non sécurisé. Un dispositif de stockage sécurisé doit utiliser un algorithme d'encryption fort et peut intégrer un Sel ou une clé permettant de renforcer la robustesse de l'encryption.

8. VÉRIFICATION DE L'ABSENCE DE FAILLES DE SÉCURITÉ DES APPLICATIONS WEB ET DES ÉLEMENTS D'INFRASTRUCTURE.

RGPD-VUL-1 : les applications Web ne doivent pas être vulnérables à des attaques considérées comme courantes par la CNIL : https://www.cnil.fr/fr/securite-des-sites-web-les-5-problemes-les-plus-souvent-constates

RGPD-VUL-2 : de manière générale, l'application ne doit pas pouvoir être compromise par des attaques connues comme, l'injection de code dans les champs de formulaire (et dans les URL pour les applications Web : injection SQL, XML, commande système…) ou les attaques de type XSS (Cross Site Scripting). Le fournisseur peut se référer aux guides de l'OWASP (Open Web Application Security Project) pour sécuriser ses applications Web.
(https://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project)

RGPD-VUL-3 : il est recommandé de faire effectuer un audit de sécurité par un organisme externe pour détecter d'éventuelles failles de sécurité.

RGPD-VUL-4 : les éléments d'infrastructure ainsi que les systèmes d'exploitation doivent faire l'objet d'une veille pour déterminer s'ils sont soumis à des vulnérabilités connues. Si c'est le cas, un plan d'action doit être mis en place pour effectuer les corrections nécessaires et s'assurer qu'aucune faille critique et/ou exploitable ne subsiste. Ceci est d'autant plus vrai pour les éléments d'infrastructure et systèmes d'exploitation supportant des applications Web.

----------Fin du document ----------