NeoSys
votre partenaire informatique

RGPD : comment réussir la mise en conformité de votre SI (2 jours)

Cette formation a pour objectifs d'analyser les enjeux et les principes clefs du RGPD et propose aux entreprises concernées une aide concrète pour :

- Acquérir les connaissances et les compétences nécessaires à la mise en place d'un programme efficace de conformité dans les domaines de la confidentialité et de la sécurité de l'information
- Effectuer un autodiagnostic de leur niveau de conformité au RGPD
- Mesurer les impacts organisationnels de leur mise en conformité en s'appuyant, notamment, sur les retours d'expérience déjà recensés et les difficultés d'application qui en ressortent
- Détailler le plan d'actions à déployer à la fois pour se mettre en conformité avec le RGPD et pour maintenir cette conformité dans le temps

Contenu

Jour n° 1 : principes fondamentaux et juridiques

- TP pour tester si l'auditoire est « RGPD compatible »
- Généralités RGPD
- Aspects légaux &contractuels
- Former & sensibiliser

Jour n°2 : aspects techniques

- Le volet informatique de la RGPD
- La démarche de mise en conformité

Participants

Les responsables de confidentialité, les gestionnaires des risques et les responsables de la conformité légale

Les professionnels de l'IT et de la sécurité de l'information

Documents de références

- Modèles de clauses RGPD pour les contrats, CGU, CGV …
- Modèles de chartes informatiques
- Mise à disposition du référentiels CNIL

Démonstrations

- Démonstration d'un outil spécifiques de diagnostic sécurité du SI incluant la problématique RGPD
- Logiciel PIA / CNIL, d'Etude Impact de la Vie Privée (EIVP)
- MyDPO : solution logicielle en ligne permettant le pilotage complet de la conformité de l'entreprise

Patrick TREMOULET
06.89.49.39.91
p.tremoulet@neosys-info.fr

NeoSys
votre partenaire informatique

RGPD : comment réussir la mise en conformité de votre SI

JOUR n° 1 : principes fondamentaux et juridiques

TP introductif

« Etes-vous RGPD compatible ? »

Le cadre légal et règlementaire

Vue d'ensemble : historique et contexte
Les 6 principaux articles de la loi
Qui est concerné ?
Qui est responsable ? Les sanctions
Le rôle de l'autorité de contrôle

Les définitions et mots-clés

Les grands principes d'un traitement de données
Le registre de traitements
Accountability ou responsabilisation
Privacy by Default
Privacy by Design
Analyse d'impact
Données sensibles, données à risque
Qu'est qu'un transfert de données au sens RGPD

Les principes fondamentaux

Les finalités d'un fichier
La transparence
La pertinence des données
La conservation des données
La sécurité et la confidentialité des données

Les acteurs

Les acteurs internes
Les acteurs externes
La responsabilité des acteurs
Le rôle du Délégué à la Protection de Données (DPO)

Les droits des personnes concernées

Le droit à l'information
L'organisation du recueil de consentement
Le principe de Opt-in et Opt-out
Les droits d'accès, de rectification, d'opposition, à la portabilité …
Focus sur le droit à l'oubli et au déréférencement
Focus sur les directives anticipées

Les impacts contractuels et les relations fournisseurs

Contrats fournisseurs et sous-traitants
CGU (conditions générales d'utilisation)
CGV (conditions générales de vente)
Mailing
Sites commerciaux

Sensibilisation

Application de bonnes pratiques
Formation des équipes opérationnelles informatiques

Procédures et chartes

PSSI : définition d'une Politique de Sécurité du Système d'Information
Garantir la « Privacy by design » (protection de la vie privée dès la conception) et … le « Privacy by default » (protection de la vie privée par défaut)
Utilisation des zones « blocs notes »
Charte informatique utilisateurs
Charte administrateur

Patrick TREMOULET
06.89.49.39.91
p.tremoulet@neosys-info.fr

NeoSys
votre partenaire informatique

RGPD : comment réussir la mise en conformité de votre SI

JOUR n° 2 : aspects techniques

Plan d'actions de mise en conformité du SI

Démarches de certification, gouvernance des données
- Inventaire des données et cartographie du SI
- PIA : procédure d'analyse d'impacts
- Réactivité face à un défaut ou une faille de sécurité

Protection physique
- Les dispositifs anti-intrusion
- Sécurisation des accès aux locaux
- Procédure d'impressions sur les unités déportées (photocopieurs)
- Rangement documents et dossiers papiers
- Procédure de destruction

Sécurité logique
- Pare-feu, antivirus, proxy
- Accès et verrouillage des postes de travail et des applications
- Indentification des informations et serveurs les plus sensibles
- Sécurité des réseaux Wi-Fi (externe, interne)
- Sécurité des flux internes et externes
- Sécurisation accès Internet
- Cloisonnement des réseaux
- Politique de renouvellement matériel

Authentification, mot de passe
- Définir une politique de mots de passe
- Gestion des accès (SSO, TouchID, biométrie)
- Gestion RH, mobilité interne

Sauvegardes
- Définir une politique de sauvegarde et d'archivage
- Gestion d'un PRA / PCA

Messagerie
- Gestion des emails professionnels / professionnelle, protection, chiffrement

Externalisation / infogérance
- Evaluation des risques spécifiques (maîtrise du SI, actions à distance, hébergement mutualisé …)
- Rédaction des exigences applicables aux prestataires (sécurité, réversibilité)

Le Cloud
- Conditions d'hébergement de données
- Utilisation de logiciels en mode Saas

Gestion des terminaux nomades
- Règles d'utilisation des terminaux mobiles
- Connexion en situation de nomadisme
- Utilisation des supports amovibles
- Gestion du BYOD, sécuriser le télétravail

Maintenance
- Evaluation des risques inhérents en amont
- Procédure de prise de main à distance

Journalisation, gestion des logs
- Gestion des dysfonctionnements et des incidents
- Traçabilité des événements, des accès illicites

Démarche de mise en conformité

Pourquoi engager une démarche de mise en conformité
- Asseoir la Gouvernance des données
- Préserver l'image de marque
- Permettre la continuité de l'activité
- Disposer d'un nouvel atout concurrentiel
- Ancrer l'éthique de l'entreprise

Préparation de la conformité RGPD
- Gouvernance/Organisation interne
- Conformité des traitements
- Gestion de risques sur la vie privée
- Gestion des risques liés aux tiers
- Gestion de droits des personnes
- Considérer les cas de transfert des données

Devenir une entreprise « GDPR conforme »
- Evaluer le niveau maturité
- Etablir le niveau de risque
- Disposer d'une feuille de route « sécurité IT »
- Proposition méthode de mise en conformité
- Réfléchir aux processus et traitements
- Déroulement du projet …
- Nommer un DPO, cadrer ses missions
- Réaliser la mise en conformité
- Assurer le suivi de la conformité …
- Prévoir la gestion de crise et … l'assurer
- Gérer une violation de données personnelles ?
- S'assurer contre les risques de fuite de données : les cyber assurances
- « Labelliser » et préserver sa conformité RGPD

Patrick TREMOULET
06.89.49.39.91
p.tremoulet@neosys-info.fr